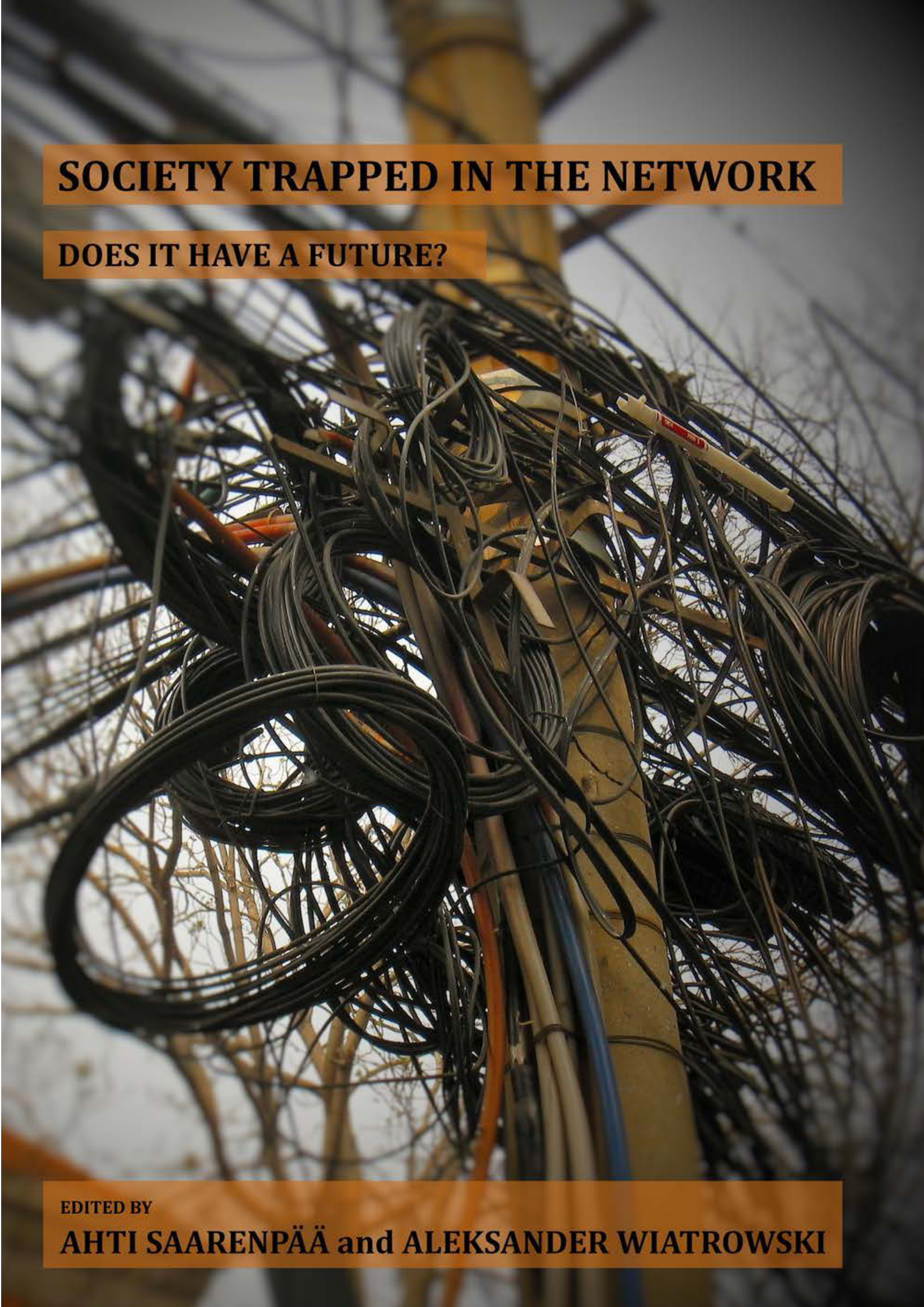


SOCIETY TRAPPED IN THE NETWORK

DOES IT HAVE A FUTURE?

EDITED BY
AHTI SAARENPÄÄ and ALEKSANDER WIATROWSKI

Society Trapped in the Network
Does it have a Future?

Edited by Ahti Saarenpää and Aleksander Wiatrowski

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

ROVANIEMI 2016

This book is one of the results of the project Network Society as a Paradigm for Legal and Societal Thinking (NETSO) conducted at University of Lapland, Faculty of Law, Institute for Law and Informatics.

Layout and editing Ahti Saarenpää and Aleksander Wiatrowski
Cover design Aleksander Wiatrowski

ISBN 978–952–484–916–6
ISBN pdf 978–952–484–917–3

University of Lapland Printing Centre
Rovaniemi 2016

SUMMARY OF CONTENT

CONTENT

NETSO RESEARCH PROJECT 2010–2013

Name of the responsible leader:	**Ahti Saarenpää, University of Lapland**
Title of the research project:	**Network Society as a Paradigm for Legal and Societal Thinking (NETSO)**
Site of research:	**University of Lapland, Institute for Law and Informatics**

The NETSO project aims to generate basic knowledge of the theoretical foundations and context of the network society development and to discover the subsequent changes in the legal, communicational and societal aspects of the process. The project deals especially with the foundational thinking behind the fashionable talk about ubiquitous information society. This will be linked to the modern constitutional rights.

NETSO aims at discovering the changes in the network society, particularly in light of legal and sociological research, with several thematic foci. The research questions depicting the main themes can be listed as a number of How's:

1. How has information society as a concept evolved internationally and in Finland, both in scientific thinking and political discourses?

2. How is the nature of legal regulation changing in the network society, while strengthening the role of constitutional rights and the rule of law state? What is the role of watchdog organizations in this development?

3. How is individual privacy protected in the network society and in the information administration?

4. How is the role of a consumer changing in the network society?

5. How is e–governance changing everyday life and citizenship? Which are the new risks?

6. How is the nature of IT business changing in the network society?

7. How does the paradigm of network society challenge the conventional disciplines of law, sociology, media, art, computer and information systems, with new interdisciplinary approaches?

INTRODUCTION

The world is changing. This observation, simple and indisputable as it may seem, is easily overlooked in law and the social sciences. Laws and provisions may change but we often fail to see the implications of such change for society and or consider possible links unproblematical. And even when the conceptual world changes, the new concept is often welcomed unquestioningly, with open arms. A prime example is "the Information Society".

It was this relationship between society and law that formed the focus of *Netso*, an international project that ran from 2011 to 2015, funded principally by the Academy of Finland. The present publication and the recently published *Lawyers in the Media Society*, a collaborative Finnish–Polish effort, present some of our observations. The project has also published *KnowRi§ht 2012* book. These contributions, the doctoral thesis of *Johanna Tornberg* and *Juhani Korja* as well as my general presentation of Legal Informatics, *Oikeusinformatiikka* – updated in conjunction with the project and appearing in the work *Oikeus tänään* – have presented essentially unequivocal evidence that "Information Society" – as a concept and a term – has outlived its usefulness. If we look at communication and law in the world around us today, it is time we spoke of the Network Society.

Likewise, it is time we bid good–bye to e–government, although it is a concept of comparatively recent vintage. Six particular reasons have prompted this conclusion, each based on developments showing that we now live in what may be considered a legal network society.

E–government as a concept reflects a bygone era. It was coined when society has just taken the first steps in the transition from what was routine progress in office automation to more extensive use of IT in government. The focus at the time was on more effective use of a *tool* that could make the work of government easier. Today, the situation is markedly different. The everyday use of computers is a natural aspect of government. Government operates in an environment *defined by information systems* and *information networks*. The era of tools and the tool mentality is over.

In the 1990s, the temporal backdrop to the concept of e–government, we were still living in the *Information Society.* That is an era now past; the transition to the *Network Society* we live in today was just beginning. The World Wide Web was something new that represented a wealth of new opportunities. Today, in the modern Network Society, we are critically reliant on information networks and their use in government and elsewhere. Use takes diverse forms, from the creation of documents to communication, and from initiating matters electronically to using the wide variety of *electronic accounts* that individuals and organizations set up.

The third central change we have to consider is the development of the modern *constitutional state*. Throughout the world countries have entered – or are at least stating to – the era of the constitutional state. It is a state, which places far more weight on *human* and *fundamental rights* – the rights of the individual – than its predecessors did, and makes those rights essential elements in all systems planning at the governmental level. New Public Management, which held sway earlier and viewed people as clients whose needs were dwarfed by considerations of efficiency in government, has now yielded or will gradually have to. Government in its various forms – government IT services included – must now respect human rights to the full.

The fourth crucial development is the change in the status of *information* in society. When people talked about the Information Society, what they had in mind was the quantitative growth in information processing and information as well as the impacts these developments would have on society. Today, views stressing the increased importance of information have their basis in an interest in our *right to know* and the *right to knowledge* this entails. The new constitutional state has a significant informational dimension.

The fifth reason is the transition that is underway to a *digital working environment* across the board – citizens, organizations and the public sector. This change makes it possible to design *interoperable systems* in which the path information takes can be optimized in technical as well as legal terms with a view to respecting the rights of the individual. The long reign of static paper documents, when nearly everything was reduced in form and content to what would fit in a single paper document, is more and more behind us.

Lastly, the sixth crucial change to mention is that we now take information security much more seriously than before. We must sit up and take notice of the fact that information security is a central condition for the realization of our fundamental rights both in general and in government. It is with this in mind that I have called information security a *meta right* as where fundamental rights are concerned. Rigorous information security is a guarantee that the fundamental rights we exercise when using networks are properly safeguarded.

Once again. The world is changing. The legal framework of Network Society is changing. And government must be changing too. In this connection good lawyers must be digital lawyers. This is our NETSO message to all lawyers.

Tämä teos on alkuperäisen Netsohankkeen tavoin ensi sijassa englanninkielinen. Mukana on myös hankkeeseen eri tavoin osallistuneiden tutkijoiden suomenkielisiä kirjoituksia. Tässä julkaisussa aihe ratkaisee, ei kieli. Erityisesti kiinnitämme huomiota siihen, että Juhana Riekkisen laaja selvitys tietosuojavaltuutetun asemasta ja toiminnasta julkaistaan kokonaisuudessaan suomeksi. Kun olemme siirtymässä uuden eurooppalaisen tietosuoja–asetuksen aikakaudelle, tuo perusteellinen selvitys tarjoaa nähdäksemme hyvän pohjan viranomaistoiminnan kehittämiselle muuttuvassa oikeudellisessa toimintaympäristössä.

Ahti Saarenpää, Rovaniemi 2016

WHERE ARE WE HEADED? LAW, THE FUTURE OF COMPUTER MEDIA, AND HERMANN FRIEDMANN

Mauri Ylä–Kotola

Rector, University of Lapland, Prof. Dr. at Finnish Academy of Fine Arts,
mauri.yla–kotola@ulapland.fi

In this article, I look at certain stages in the history of computer media as those developments bear on legal philosophical inquiry. First, I will examine the computer, media, and law, then proceed to the philosophy of Hermann Friedmann (1873–1957) and, lastly, draw on my observations to answer the question of what kind of future we are heading towards. The perspective I adopt here is that of a philosopher and media scientist, not that of a legal scholar. What I hope to articulate is a vision, not a legal study, although some of the ideas I present might have a contribution to make to systematic legal philosophy.

1. Computer, media, and legal studies

The academic field that concerns itself with the problematics of computers and law is called legal informatics. In 1992 the Council of Europe recommended that an institute of legal informatics be established in every member state. In that same year, on the initiative of Professor Ahti Saarenpää, the Institute for Legal Informatics was set up in the Faculty of Law at the University of Lapland.[1]

The application of information technology in legal culture in general, and in the legal sciences particularly, goes back to the 1940s in the United States. The academic debate in the field originated with jurimetrics, which then expanded to become a broader study of the relationship between law and technology. Issues in legal informatics were addressed under two orientations: (1) computer law and (2) computers and law. The first looked at legal questions relating to information technology and its use, the second at legal information and its processing on computers.[2]

Ahti Saarenpää describes modern legal informatics as a field whose general frames of reference are the regulation of information and IT in the Information Society and their use of in legal life. The field can be subdivided into four areas: legal information processing, legal

[1] Saarenpää 1998: 218.
[2] Saarenpää 1998:211.

information, information law, and IT law. Information law is concerned with issues such as privacy and public access, telecommunications, electronic trade, information security, and copyright of information network products.[3]

One to be distinguished within IT is computer media technology. Computer media refer to the forms of the new media, such as information networks, multimedia, virtual reality, digital television, virtual space, smartphones and ubiquitous computing.

One of the principal insights that media research has contributed is the notion that the world of film, television and computers is more than a world outside us. It is a world that very much shapes how we perceive and understand things. According to Marshall McLuhan's well–known observation, media are extensions of the senses. Their proximity prevents us from understanding and comprehending them directly. In this respect, the development of media also affects legal culture, as well as legal practices and legal thinking as a whole. Given how computer media are used, the scope of media, or communications, law and information law overlap to some extent as well.

The application of the law in everyday life is based, ideally at least, on the notion that legal values which are defined democratically through the political decision–making process are shaped through legal expertise into a system of laws, which are then applied to individual cases. The broader philosophical question here is what has happened in reality, that is, what are the facts in a given case.

In classical times, a realistic view of a person's relationship to reality proceeded from the assumption that one could obtain objective information through direct observation. From the time of Immanuel Kant, if not before, it has been understood that there is no such thing as direct observation; rather, even at the retina, reality is shaped by the knowledge structures of the mind.

The concept "data environment" denotes the human being's sensory environment. One requirement for applying legal information is knowledge of empirical reality, the sensory environment, the facts of a case. Evidence refers to reality *an sich*, which as such is unattainable but which can be reconstructed using pieces of evidence. Evidence is part of the data or sensory environment, which is always a sensed, experienced and lived environment. Indeed, both the natural environment and the digital data environment are just as much in our heads as outside of them. What really happens does not happen in the world *an sich* but in a phenomenological world of experience.

[3] Saarenpää 1998:212–213.

The etymology of the term "data environment" is the Latin word "datum", which literally denotes something given, in particular in the sense of sensory data. In the modern conception of the term, sensory data is not given but actively constructed by the individual. The concept of the digital environment derives from the notion that in our era, characterized by a culture of simulation, nature has been replaced by technonature as the individual's principal sensory environment. This being the case, the data environment is increasingly one produced by technology, in other words, digitally.

Digital data environments are sometimes called "information environments". "Digital data environment" is the more descriptive term, however, as the focus is the sensory rather than the informative nature of the IT environment. Similarly, it makes more sense to speak of a Society of Digital Data than an Information or Knowledge Society. The scope of information networks goes beyond mere information: they convey every bit as many corporeal sensory experiences. As digital television and the net converge, sensory experiences will figure more prominently.[4]

Where today natural language and textuality occupy a central role in email and information network communication, the networks of the future will feature a more salient presence for moving pictures and visuality, as well as sound and space. This development will pose challenges for legal informatics as well. While coining and invoking a term such as "legal datalogy" would certainly be contrived, it is important that we note the difference between the terms "information" and "data". We will soon see legal iconography joining legal linguistics as one of the sister sciences of legal informatics. Where legal linguistics studies language, legal iconology studies images. Iconography is a model for interpretation that has been derived from iconography. It strives to interpret the inner meaning and content of an image, the worldview that the image conveys. The model of iconology developed by Erwin Panofsky (1892–1968) has three levels: the primary, or natural, level, iconographic analysis and iconological interpretation. We can view iconological interpretation in law as adhering to Panofsky's model, with deeper interpretation producing deeper knowledge.[5]

In post–industrial society, the types of environment are nature, the built environment and the media environment. Law can also be approached in terms of these distinctions. Characteristic of nature is that it has not been created by people; distinctive of the built environment and the media environment are that they are manufactured or artificial. The first two are material in nature, whereas in the media environment the material and immaterial are

[4] Ylä–Kotola & Arai 2000: 11.
[5] Panofsky 1972: 5–9.

fused. In post–industrial society, the scope of environmental law overlaps that of information law.

In terms of environmental law, audiovisual media culture can be conceived as technonature in which information technology becomes associated with nature and the built environments of our daily life, which are not thought of as being technical in nature. These associations give rise to novel social and interactional spaces. The ideas of Henri Lefebvre on the production of space and the linguistics of the city – built on the concepts of *parole* and *langue* – require a new interpretation if we are to successfully analyse virtual cities and media environments. Among the salient features of media environments are their multidimensionality and the way in which they create multiple copies and versions of the same contents in different environments. In particular, the proliferation in the near future of immersive and sensorimotor 3D user interfaces in both homes and workplaces will mean that media will take on the character of environments more so than images.

2. The philosophy of Hermann Friedmann

Adolph Hermann Friedmann was born on 30 March 1873 in what is today the Polish town of Bialystok (also Belostok or Blavystock), near the Lithuanian border. He died in Heidelberg in the Federal Republic of Germany on 25 May 1957. Friedmann was a Finnish citizen from 1906 to his death. Bialystok was the city where he spent his childhood and Riga where he received his education. Hermann Friedmann's father, a Jewish banker named Isidor Friedmann became the Governor of the Bank of Latvia after the First World War.

Friedmann studied at the classical lyceum in Riga, that is, the government gymnasium, from 1883 to 1990. He went on to study law at the University of Tartu, the city at the time featured a vibrant student life with its many German undergraduate and was called the "Athens of Emajoki", the river on which the city is located. The language of instruction at the university was German from the beginning of the 1800s until the 1890s, prior to its becoming russified. Where his chosen field, law, was concerned, from his days in Tartu Friedmann mentions in his memoires Mikail Djakonow, who studied the history of Russian law, Guljajew, an expert on Roman Law, Pustorolew, an expert in criminal law, and Krasnoshon, a scholar in Orthodox Canon Law. Friedmann delved into Russo–German legal history until the end of the fourteenth century under the tutelage of Djakonow. In Friedmann's memoires, law in Tartu comes across as being a heavily russified national science.[6]

[6] Friedmann 1950: 106–107.

Friedmann moved to Heidelberg in 1896. In the city's highly regarded university his teachers included constitutional law theoretician Georg Jellinek (1851–1911) and Ernst Immanuel Bekker (1827–1916). Jellinek, an Austrian, had been a professor in Basel since 1889 and was awarded a chair in Heidelberg in 1891. It was Bekker in particular who had a strong influence on Friedmann. Friedmann's first two published studies were in the field of law. One, published by R. Reich Buchhandlung in Basel in 1900, was a 42–page legal philosophical work titled *Die unkörperliche Sache: Zur Systematik des Privatrechts* and dedicated to his "dear parents". The second, published in the same year, was an extensive article in a Swiss law journal titled "Der Anspruch auf Realerfüllung in schweizerischen Rechte". The latter article is still cited today by Swiss legal scholars.[7]

In his first legal philosophical work, *Die unkörperliche Sache: Zur Systematik des Privatrechts* (1900), Friedmann's point of departure was Roman Law. Professor Ernst Immanuel Bekker, not only a specialist in Roman Law but an accomplished scholar in philosophy and the natural sciences, encouraged Friedmann to study immaterial matters such as electricity, light, heat and sound. Accordingly, Friedmann's work is in inquiry into immaterial law (*Immaterialgüterrecht*), although the scope and meaning of the concept in his study differed somewhat from what they are today.

Friedmann's aim was to present a universal systematics of private law as it pertained to immaterial things. His work represents the conceptual jurisprudence typical of his day. The subheading of the work, *Zur Systematik des Privatrechts*, brings out the distinction between private and public law. Carl Friedrich Gerber (1823–1891), an early representative of conceptual jurisprudence, emphasized the distinct nature of the conceptual systems of public law and private law. A second renowned scholar in the field, Bernhard Windscheid (1817–1892) – whom Friedmann cites in passing in his work – regarded the system of legal concepts as a system of objective law. A legal concept was described as having a core, or *Wesen*, regardless of its being used in varying ways in different legal orders. The system of legal concepts served as a description of objective legal relationships. Having a systematics to appeal to makes the notion of objective law possible. Terms must nevertheless be clarified in order to go beyond their varying forms and illuminate the objective essence of the law. The connection between conceptual jurisprudence and philosophical objective idealism is clear. In his later, mature philosophical thinking, Friedmann detached himself from conceptual jurisprudence.

[7] Works where it is cited include *Schweizerisches Obligationsrecht*, a work by Law Eugen Bucher, professor of law at the University of Bern, and *Die nachträgliche Leistungserschwerung*, a doctoral thesis submitted at Gallen University by Corrado Rampini. (Bucher 1988: 327, Rampini 2002: 68).

Friedmann's legal philosophical study of immaterial things is based quite straightforwardly on Roman Law as set out in the works of Gaius, Cicero, Cato, Palladius, Horace, Ovid, Quintilian, Juvenal, Martial, Seneca, Pomponius, Livy, and Quintus Mucius Scaevola, among others. Friedmann does not engage in a debate with later legal practice, for example German legal practice. This methodological choice is typical of his time and here one can see the influence of Friedrich Karl von Savigny. Savigny took the view that the "vine" of hermeneutic interpretation that had grown around Roman Law had to be excised. In Savigny's opinion Roman Law did not have multiple interpretations, that is, an original interpretation and new ones arising from the new circumstances prevailing at given times; rather, legal relations constituted an objective system, a geometry of sorts, which is what Roman Law represented.

Friedmann's work shows his profound knowledge of Roman Law but also reveals a solid grounding in nineteenth–century legal philosophy – although the article lacks an account of actual contemporary cases and court decisions relating to immaterial things. Among the experts on the history of Roman Law, Friedmann cites Leopold Joseph Neustetl (1798–1825), professor of Roman Law at Breslau University, Canon Law scholar Georg Philip Eduard Huschke (1801–1886), historian Joachim Marquardt (1812–1882), Rudolf Stammler (1856–1938), who, following Kant's example, sought the *a priori* forms of law, Eugene Huber (1849–1923), who studied the Roman roots of Swiss law, philologist and legal scholar Lothar Anton Alfred Pernice (1841–1901) and Otto Karlowa (1836–1904), who studied the reception of Roman Law in Germany. The work also refers to the Swiss lawyer and politician Johann Caspar Bluntschl (1808–1881), Rudolf von Ihering (1818–1892), a pioneer in the field of law who, crucially, examined conceptual jurisprudence in historical perspective, and historian Otto von Gierkeen (1841–1921). The book cites a number of natural scientists and philosophers as well, among the former Emil du Bois–Reymondiin (1818–1896) and the latter, Karl Steffensen (1816–1888), a conservative professor from Basel University whom history remembers for his critique of the philosophy of his colleague Friedrich Nietzsche.

In his autobiography, Friedmann provides some background to *Die unkörperliche Sache*. One case he handled while working in Basel as a lawyer gave him the impetus to delve into Roman Law using original Latin legal records. He recalls that when he did so he noticed that Roman Law drew a distinction between two categories of things: (1) things which can be touched (res quae tangi possunt) and (2) things which can only be sensed as mental observations (cernere animo).[8] Observation is profoundly related to the connection between tangibility and

[8] Friedmann 1950: 128.

conceptualizing, which led Friedmann to investigate in greater depth the philosophy of the sense of touch (haptic perception) and the sense of sight (optic perception). In *Die unkörperliche Sache*, the distinctions drawn in Roman Law are viewed as being at their core a geometry of objective reality. The book describes an objective system of legal relations pertaining to immaterial things, a system equally applicable in the present day and Roman times.

Friedmann's later, strictly legally oriented writings ended up being comparatively modest. He moved to Basel, was involved in founding a scientific journal on racial hygiene in Germany, and published studies in the fields of physics and evolutionary biology. A work published in 1904, *Die Konvergenz der Organismen*, drew the attention of an influential American scientist, one of President Herbert Hoover's teachers, Vernon Lyman Kellogg (1867–1937). In his work *Darwinism to–day: a discussion of present–day scientific criticism of the Darwinian selection theories, together with a brief account of the principal other proposed auxiliary and alternative theories of species–forming* (1907), Kellogg created a synopsis of different views on the theory of evolution. The introduction to the book is headed "The Death–bed of Darwinism" and contains a chapter "Friedmann's theory to replace evolution with divergence". According to Kellogg, in a little book titled *Die Konvergenz der Organismen* one could find a singular attempt to formulate a scientific theory to explain the living world we know and to replace the theory of evolution. In Kellogg's estimation, the author of the book assumed that the diversity of life forms was the original state of affairs and that the similarities between them are the result of convergence. Kellogg noted that the theory in this respect is the opposite of evolution, according to which the diversity of life sprung from initial identity and homogeneity.[9]

In the early 1900s, the theory of evolution emphasized an explanatory model based on homology, which posits a common structure derived from a common ancestry. If two organisms have similar structures, they are assumed to descend from a common ancestor. As the ancestor of two organisms has had the structure in question, it has not had to develop in both organisms separately. The similar structures observed in different species have been interpreted as evidence of a genetic affinity. Friedmann's convergence theory held that where a similar structure exists in two different organisms this might have developed separately, independently of one another, there then being no need to assume a common ancestor. The reason why two separate developments would produce the same structural form was explained by the fact that

[9] Kellogg 1907: 8–9.

the form proved optimal for its task. Similar needs resulted in the development of similar forms for different organisms.

After living in Berlin for a short time, Friedmann spent the years 1905–1906 in the Baltic countries and St. Petersburg. In 1906 he moved to Finland. Why did Friedmann, student of the renowned Jellinek, not apply for a post as teacher in the Faculty of Law at the University of Helsinki? Friedmann himself mentions that there was no position open for a teacher of Roman Law. An additional reason might have been the general orientation of legal studies in Helsinki, which his friend Johannes Öhquist described as follows with reference to the 1880s: "The teaching of law at the University of Helsinki is wholly geared to producing civil servants. Academic research is a mere stepchild to this endeavour. The only subjects which involved pure scientific inquiry – legal philosophy and the history of the legal system –, were considered so secondary in value that students completed the courses in the form of what was known as a preliminary degree. Virtually no time was spent dealing with fundamental issues (except perhaps in legal philosophy, but even then at a very elementary level). The principal studies focus on current law, which students must know – to the letter. The university produces skilful and knowledgeable civil servants, ones scarcely aware that there is a science of law that concerns itself with theory, principles, worldviews and philosophy."[10]

On 17 June 1909, Hermann Friedmann was accepted as a member of the German Evangelical Lutheran congregation as one had moved to Finland from abroad. The state archives have a letter Friedmann wrote to Senator Leo Mechelin (1839–1914) telling him everything from his studies in constitutional law to his great respect for the senator and asking that he might be given an audience with the senator. Friedmann probably knew Mechelin's name because in Heidelberg he had read his *Das Staatsrecht des Grossfürstentums Finnland*, in which Mechelin had presented his ideas on Finland as a constitutional state distinct from Russia. In Finland, Friedmann worked as an advisor to the governor general and later as a business lawyer, among other capacities. One of his most extensive cases was as attorney for Finnish shipowners in a dispute seeking compensation for ships hired by Britain during the First World War, some of which were lost. The case was heard in, among other instances, the League of Nations and British courts. Friedmann received the most publicity in the 1920s as attorney for Allan Törnudd and Margit Niininen in a murder trial.

Friedmann came to be respected by figures such as J.K. Paasikivi, Rudolf Holsti, Rafael Erich and G.A. Gripenberg. Edwin Linkomies and Eino Kaila submitted that he be given the

[10] Öhquist 2006: 98.

title of professor, which the President of the Republic then granted to him in 1931. In 1934 Friedmann moved to London; as a Jew, he lost his status in the German community in Finland when the Nazis came to power, although he had private reasons and commercial interests that prompted the move to London as well. After the war, Friedmann was named an honorary professor at the University of Heidelberg; he was given some of the highest awards of the Federal Republic of Germany and he became chairman of the PEN Club of Germany, a literary association.

Today one could say that Hermann Friedmann is essentially a forgotten philosopher both in Finland and internationally. Yet, his theoretical system, idealistic morphology, attracted extensive attention in Central Europe in the 1920s and 1930s. In modern terms, Friedmann's contribution could be described as a semiotics of the world of forms. "World of forms" is the main concept of morphological idealism, which Friedmann developed later in his life as a more mature philosopher. Through rational reconstruction the world of forms could be defined as a sensory environment. Individuals construct a conception of reality using the structures of their minds and the tools which they make use of in their daily lives. A person often describes reality using language, but images and sounds play an important role in thinking. And when we see something, we interpret what we see using the memories in our minds, with the perception being filtered and shaped by the structures of memories and expectations, or schemata. Semiotics studies the functional, constantly changing system of mental representations, such as images and sounds, and investigates how we use this system in conceptualizing reality. This is not a textbook definition of the science but describes it well. Semiotics is a science of sign systems, the science of an *a priori* sign system and how the other sign systems of the phenomena in the world around us are constructed in active perception. In this context, Hermann Friedmann can be said to have constructed a scientific theory of the semiotics of the world of forms.

Friedmann developed a science of his own, the science of form, drawing on the morphological theory of evolution, Goethean natural science, sensory psychology, modern physics and Pythagorean music theory. Methodologically, Friedmann's science bridged the dichotomy between the natural and culture sciences. Friedmann's basic premise was that all knowledge was based on sensory observation but that observation itself was not unproblematical or direct. He emphasized that different senses dominate in different cultures and historical contexts and these then form the basis for forms of knowledge structured in keeping with a different sensory logic. People's knowledge of the world is constructed through sensory logics. Accordingly, the nature of various historical schools of thought or, to use a

modern term, scientific paradigms, is determined by the dominant sense and logic of observation at any given time.

The fundamental notion in Friedman's idealistic morphology that the sensory world and the forms of perception are a culturally and biologically conditioned system is a general theory which can accommodate the media culture of our own day. It resembles Marshall McLuhan's ideas whereby the medium shapes perception and thinking, but is more complex and deeper as a theory. According to Friedmann, the cultural situation as a whole determines which of the senses is given prominence. This in turn creates the sensory culture and its characteristic ways of perception and presentation, that is, the ways in which an object is observed and in which it is presented. We can think that different cultures have different ways to discriminate, name, describe, classify and value sensory perceptions and the experiences associated with them. A stronger interpretation would maintain that the way a sensory perception itself is constructed is culturally determined. The history of how the senses have been conceptualized is an account of how the distinctions, hierarchies and distinctive characteristics of the senses have changed.

The archives of the Finnish Philosophical Society contain minutes of a meeting held in the building known as the Old Student House on 6th May 1926. The record shows that 20 people attended the meeting, which was chaired by Professor Arvi Grotenfelt. The second item in the minutes notes that Doctor Hermann Friedmann gave a presentation in German on the fundamental idea in his *Die Welt der Formen* with special reference to the concept of reality.

According to the secretary to the meeting, J. E. Salomaa, Friedmann proceeded from Kant's distinction between sense and understanding. He characterized the former as receptive and the latter as spontaneous. Friedmann also presented this distinction but in a different to that Kant had used. According to Friedmann these is no general sensibility but rather many sensibilities. In his view, the sense of touch is entirely receptive, which is not the case with the sense of sight. A blow to the eye does not result in light, but rather a haptic sensation. Sight to Friedmann could be described in terms of the concept of spontaneity as this related to understanding in Kant's terms.

Friedmann maintained that an optical experience occurred at three levels, described by the German *erblicke*, *sehe* and *schaue*; equivalent terms are found in Greek. According to Friedmann such distinctions could not be made in the haptic realm, although the sensory psychology of blind persons had not been sufficiently studied at the time. He contended that persons blind since birth were unable to learn a certain type of geometry: they could only learn tactile geometry, not optical, which is based on perspective. A blind person reads by using the

forefinger of his or her right and left hands. Friedmann maintained that this reading involves first synthesis and then analysis.

Kant himself did not draw a categorical distinction between the sensible and the intelligible. In the history of philosophy, the materialists and idealists have also foregrounded the connection between the two in different ways. The conceptions are often unclear, as Friedmann notes. In his view, every sense has its own logic, its own concepts. The concepts of tactile and optical geometry differ: there is metric and projective geometry – two areas of logic and sensibility.

The optical realm has different causal relations than the haptic. According to Friedmann, determination and realization in biology coincide in the haptic realm but differ in the optical. One can imagine the haptic realm without the optical but not the optical without the haptic. Kant himself demonstrated that objective reality always includes a conceptualizing subject.

3. Where are we headed?

Douglas Engelbart (1925–) is a pioneer in the development of information technology. Among other accomplishments, he developed the mouse and created the foundation for word–processing software. In addition, early on he anticipated many of the features and functionalities of the modern computer, such as linking, hypermedia publishing, computer–aided conferencing and context–sensitive help.

Marshall McLuhan took the view that media augment the senses. Increased effectiveness, or augmentation, is also a key theme in Engelbart's work. By "augmentation" Engelbart means the change that can be achieved through collaboration between and individual and a machine. By dint of their culture, people have many encoded skills, which allow them to cope in the world. Working with machines, in this case engaging computer–assisted activity, extends this network of skills. Engelbart's point of departure is the augmentation of a person's physical and mental capabilities such that he or she can solve complex problems more effectively, more quickly and better. Engelbart predicts that in the future the computer will augment almost everyone's activities.[11] As an academic field, legal informatics seeks to apply technology in order to augment the practices of legal life.

According to Friedmann, in human history our data environment has changed depending on what sense our culture has favoured at any given time. The sensory culture has determined the medium which people have used, that is, the means for augmenting human activity.

[11] Ylä–Kotola and Arai 2000: 27.

In classical times, there was a focus on rhythmically articulated, or muse–inspired, speech. The Middle Ages saw a shift towards abstract, written expression based on verbal analogies, symbols and allegories. In the late Middle Ages, Friedmann saw an emphasis on mysticism and non–verbal expression, until in the modern era Newton's physics reduced reality to the movement of solid bodies in space and thereby gave rise to an emphasis on the sense of motion. The defining criterion for science became accuracy. In Friedmann's view, the new science of the future would be based on the sense of sight – optics – and that the model for it would be Goethe's morphology, later interpretations of which predicted that people would develop a new sense that combines all the others.

The consequences of Friedmann's theory can be seen in the area of legal culture in different eras. In ancient Greece and Rome much was made of masterful performances by virtuoso speakers – sophists and orators, who spoke with singing voices that carried well. In the Middle Ages, the use of parables become a method by which the Church Fathers could derive new social norms from the Bible and continuous revelation. The search for analogies was also a tool in the daily application of the law.

Thanks to modern science, law, too, began to emphasize the opposition to metaphysics that had arisen during the Enlightenment, which had been interpreted in different ways in legal positivism and legal realism. The central concern of legal positivism is that the law in force has been enacted in a formally correct manner, no matter how unfair the content of the law might be. German conceptual jurisprudence made a categorical distinction between the societal impacts of law and its content. Using logical inference, every legal phenomenon could be assigned its proper place in the legal system, with this then used to derive a solution to the problem at hand. In nineteenth–century England the analytical school undertook to define the existing law as precisely as possible in the spirit of Newton's physics and paid a great deal of attention to how legal language was used. Metaphysics was rejected from a different perspective in nineteenth–century legal realism, which stressed that law is only that which is obeyed in practice. Judicial realism viewed law as the system of norms which figures in the practical work of judges.

Although the young Friedmann represented conceptual jurisprudence in his first publications, his later work could be described as an inquiry in the field of haptics, as it lacked self–evaluation: a punch in the eye was a haptic sensory experience, whereas an optical experience was always a perception constructed by the perceiver. The science Friedmann aspired to, one based largely on symbols, sought to combine facts and values through a

normativity which had developed precisely as a result of the evolution of the language of the senses. Here Friedmann's later views represented a morphological natural law of sorts.

Where are we headed next? What will be the sensory culture of the future, how will it be reflected in the media, and how will this then be reflected in legal culture? One answer is digitalization. Digitality emerged as one of the key concepts of the 1990s to emphasize the change, dramatic shift and revolution in media culture. Being digital refers to the transition from what was, on the one hand, an analogue and, on the other, an electromechanical world to the digital age of computers. The notion of "being digital", as well as that of a transition "from atoms to bits", was coined by director of MIT's MediaLab Nicholas Negroponte.[12]

Digitalization means the breaking down of information into bits, which makes possible its storage, organization and manipulation. Most salient is the ability to render data that occurs in disparate forms in a uniform format. To Negroponte, being digital was more than this, however. It meant detaching information from the material world, from paper and books, and rendering it in a digital world, one deemed to be immaterial. In law, the practical impacts of digitalization are reflected in developments such as legal cybernetics and legal databases, of which the former studies the potential for automatic decision–making using algorithms and artificial intelligence applications. The possibilities of achieving global legal practice are immensely greater with the availability of cases on networks.

Future developments in computer media can be grouped in terms of four phases, which as historical phenomena are partially concurrent: (a) networking, integrating and duplicating media; (b) utopias of interactivity and hypertextuality; (c) a transition from an audiovisual to a sensorimotor media culture; and (d) the integration of media technology with the human body.[13] All four phases can be examined in terms of Herman Friedmann's semiotics of the world of forms. All also have implications for legal culture and law.

Clearly, the four phases overlap to an extent temporally and thematically. For example, sensorimotor media systems that react to movements of the body are also interactive. The different phases and their distinctive features give rise to various types of digital data environments. Here you can distinguish FilmComp, SpaceComp and CyberComp. The first is characterized by a live, illusory visuality on a two–dimensional surface, the second by integration of the media technology into the space around the user and the third by the media representations being constructed directly in the mind. Spatiality and the perception that the data environment surrounds the user are emphasized in the second type, Mark Weiser's views

[12] Ylä–Kotola and Arai 2000: 30.
[13] Ylä–Kotola and Arai 2000: 32.

on UbiCom (ubiquitous computing, in which digital technology is embedded in the environment, can be considered the precursor of SpaceComp, but his thinking actually puts more emphasis on the networking of different media than on the fundamental notion of SpaceComp whereby the user actively affects his or her data environment through bodily movements registered by sensors. [14]

Characteristic of the Internet and of the digital television of tomorrow are increased and diverse program offerings. This development will bring with it more intuitive and easier to use interfaces. With the increased supply, we will see a heightened need to tailor media to one's own preferences using, for example, an agent powered by artificial intelligence or a television guide. The expanding offerings in the area of popular culture will bring about a restructuring of the means of reception and affect the nature of the personalized reception made possible by tailoring incoming material. Our sensory environment will create new forms of perception, ones we unaware of today. One of the issues which legal informatics has to address is copyright in the case of works of art that people have tailored and shaped to suit their own tastes.

In his article "The Computer for the 21st Century!", Mark Weiser criticizes the difficulty of using computers. We have to learn technical aspects of IT that are unnecessary for completing the task at hand. Weiser points out that the most effective technologies are those which one does not even notice. They are woven into the fabric of our daily life such that they are indistinguishable from it. Written information is not confined to books, magazines and newspapers but is also conveyed by street signs, notice boards and even graffiti. He notes that even sweets are wrapped in paper with writing on it. The established presence of information that is bound up with literacy commands hardly any special attention on our part. It is difficult to imagine modern life otherwise. Contrasting with such products of literacy technology, silicon–based information technology is far from being part of the environment, Weiser claims.[15]

Weiser takes the view that despite data pens and laptops, the idea of the personal computer has failed; it is still a utopian notion. With today's equipment, it is very unlikely that we can make information technology an invisible part of our environment. The applications for today's personal computers are but the first steps in the overall development. Computers will be linked to one another and vanish into the background.[16]

[14] Ylä–Kotola and Arai 2000: 32.
[15] Ylä–Kotola and Arai 2000: 34.
[16] Ylä–Kotola and Arai 2000: 34.

The notion of a hundred computers in one room might seem frightening. However, just like cables in the walls these computers will be out of sight, not distracting. As Weiser maintains, people will simply use them, unaware of them, in order to complete the tasks at hand. Weiser goes on to point out that, the effectiveness of invisible computer technology does not lie in a single device but in the interaction between devices. Hundreds of processors and displays form more than a graphic user interface; they make for an effective working environment in which things get done.[17]

A digital data environment in which a single room might have hundreds of invisible computers is a new technonatural environment for human beings. Success in a given environment is governed by the laws of evolution. As evolutionary developments in a species require long periods of time, the planning we do has to take into consideration the constraints of evolutionary theory. The fundamental thesis of Friedmann's theory of convergent evolution was intended to counter the view that if two organisms had the same structure, they were necessarily descended from a common ancestor, as Darwin assumed. Friedmann's theory of convergence maintains that a similar structural form can develop twice in different organisms independent of one another, with no need for a common parent. The reason why two separate courses of development produces the same form would be that the structure is optimal for the task at hand. In other words, for different organisms' similar needs would lead to the development of similar forms. When people's work and free time are spent in ubiquitous computing rooms with hundreds of digital sensors and interfaces, the design of the rooms should be based on convergent information technology solutions that are optimal for the tasks at hand. There would be lessons to learn from nature in this design.

In the realm of legal culture, UBiComp technology is most closely associate with crime prevention through all–encompassing surveillance and recording. At the same time, privacy becomes a more acute problem, as society takes on Orwellian features. Ubitechnology is totalitarianism's best friend, whereas the open society has often been based on flexibility and an Americanist ploy.

Particularly during the breakthrough of multimedia and information networks in the 1990s, one heard a great deal about interactivity. There is a true content with interactivity in computer media at least to the extent that playfulness is becoming an integral part of media. This incorporates movements of the body and the eyes rather than just the eyes: the media experience becomes sensorimotor one. The combination of movement with watching and

[17] Ylä–Kotola and Arai 2000: 36–37.

hearing in games changes the stable data environment of television in a radical way. The hand plays a key role in computer games.

The integration of human beings and technology in cyborg utopias in both bio– and nanotechnologies will diminish the differences between human, animal and machine. Friedmann's Goethe–inspired discussion of the new sensibility of the individual of the future contributes a new perspective on this issue, a second perspective is that articulated by of Georg Henrik von Wright, who in his *Tiede ja ihmisjärki* cites Einstein: **"The tragedy of modern man** lies – generally speaking – in this: he has created living conditions for himself for which, because of his **phylogenetic** development, he is not adequate", continuing. "Is this tragedy destined for permanence? If so, the end can hardly be anything else than the self–destruction of the human species."[18] The design of changes living conditions – the data environment of the future – is thus a matter of survival for the human race. The normative guidance for this design through appropriate legislation could be a challenge for the future of democracy, capitalism and law alike.

[18] von Wright 1987: 76.

KNOWLEDGE, INFORMATION, AND INDIVIDUALS[1]

Wolfgang Mincke

Professor emeritus, Dr. Dr. Dr. *honoris causa* of University of Lapland, wmincke@web.de

"Why waste time learning, when ignorance is instantaneous?"
(Calvin)

1. What is knowledge?

What is knowledge good for? Why is it necessary?

To know the way from town A to town B is good for not going a long way round and to save time and gasoline. To know poems by heart is good for boasting – and annoying other people. Knowledge apparently is good for solving cross words!

It must have been about this line that in the end of the sixties the idea gained ground that knowledge of facts was not as important as traditionally had been thought. Instead, the focus should be on procedural knowledge, methodological knowledge.

This school of thought has been rather successful, perhaps not that much successful in furthering education but in discarding knowledge of facts: In school, learning by heart was despised. No more capitals of states, no more year dates in history, no more poems by heart. There arises one question: What is a method or procedure about if you have no knowledge of facts, if you do not know the facts the procedure is to manage, what is the method or a skill to explain?

Without knowledge of facts, you are fully committed to a method and bound to it. To make a choice between methods, you have to evaluate the findings, the results of competing methods. Which is the better among different methods? Apparently, the one that better explains the facts, and the one that brings about reasonable results. Without knowledge of facts, you cannot make this evaluation! This should be a severe warning of all ideologically founded concepts of education. This explains why typically regimes based on an ideology and which propagate this ideology firstly have to restrict the access to knowledge. It is the knowledge of facts that opens the possibility to think of alternatives. However, what is a reasonable result?

[1] Also published [in:] Saarenpää, Sztobryn (eds.), Lawyers in the Media Society. The Legal Challenges of the Media Society, Rovaniemi 2016

Or, in other words: What can we accept as knowledge? Or, what do we know? Socrates answered: Nothing. I only know that I know nothing. This sounds like coquetry, but it has a good philosophical motivation. Popper has taught us that there are no assured truths, we can trust only in falsification. A more practical answer has the Finnish philosopher Niiniluoto: Knowledge is assured believes, assured, ascertained cognition. (*Tieto on hyvin perusteltu tosi uskomus*.)[2]

How does one assure believes, ascertain cognition, control the content of a statement?

- google it...
- look it up in Wikipedia...
- look it up in an encyclopedia....
- ask friends you believe to be cleverer than you are…
- ask an expert.

It is natural humbleness, when one believes others more than his own judgment – but this is not the self–contained, autonomous person we see as the goal of education and erudition and that we accept as a competent partner in argumentation, a person with an own judgment. How does such a self–contained, autonomous person evaluate what is reasonable?

Suppose: A friend has gone to Florence, in July. You get a message from him by E–Mail: Here it is terribly hot, 35°C! What to do with such a message? You will contrast it and check it with what you know. There are three main possibilities:

1. The message confirms what you already know.
2. The message tells you something new but is consistent with what you know.
3. The message contradicts what you know.

2. The informational interpretation

The three possibilities can be phrased in terms of informational content:

1. The message is not informative. Your knowledge remains as it was. You knew that Florence is in Italy; 35° is not unusual in Florence in July.
2. You might not have known where Florence is and what the weather there is like in summer. Now you know that much at least: It is pretty warm there in July. The message is informative; it adds something to your knowledge.
3. You might have thought Florence is a place far up North in Norway. Now you know: This cannot be true. The third possibility is the most interesting case: the

[2] N. Ilkka, Informaatio, *Tieto ja Yhteiskunta (Information, Knowledge, and Society)*, Helsinki 1989, p.57.

message says: There is something wrong with your knowledge. You have to change your world view. This is the maximum information you can get from message. Such a message gives reason to become sceptic: Is it true at all?

Here we encounter something interesting: When we speak about "no information" (and that is minimum information) and maximum information – apparently there is something like an amount of information, a quantity that will vary in the cases between the extremes, at least in the sense of less and more information.

Apparently, information – in the sense "what is informative" – depends not so much on the message itself but mainly on the previous knowledge of the receiver of a message, on his expectations:

For an ignorant – a person who knows very little or nothing – everything is informative.

For average people like us what is informative depends on what we know, on our world view, on our expectation. For an all knowing person, an omniscient (if such a person exists) nothing is informative.

The ignorant is not very interesting, nor is the omniscient. We are interested in people like us, who have a world view, some knowledge about the world. We know where Florence is and have an idea, a certain expectation what the weather is like in summer in Florence.

But: The information the receiver gets from a message does not only depend on his knowledge but to a high degree on his competence to evaluate the information of the message: And this competence depends on his knowledge and on his capability to process the message, to track the effects of a message in his knowledge.

In the silly example of weather in Florence in July again: Imagine the message is not "it is terribly hot here" but: Last night here fell snow!

The ignorant might conclude that Florence must be somewhere near the North Pole or deep down in South America. And he might think: "Aha, weather is much better here!" The best he will get from the message would be a wrong world view.

An average person, who has an idea where Florence is and what weather can be expected in July, would think: That is sensational. I would never have thought that. That is impossible! And he would now imagine how traffic breaks down in the town and other consequences of snowfall.

Now think of a meteorologist. He has not only factual knowledge about weather in Florence, but he knows why it is hot in July in Florence. Snow in July is not only very unexpected, a sensation, but it contradicts his knowledge. He knows that weather in the seasons

has to do with the inclination of the earth axis and would consider, whether something might have happened to this inclination.

It is apparent that an average person gets more information from the message than an ignorant and that the expert gets more information than the average person. With a conventional opinion one would think that the information of a message has to do with expectations, with the probability of the message. This is and remains true. But this does not fully explain the difference between the meteorologist and the layman in weather science. For both, when asked, the probability of snow in July in Florence would be zero, it is impossible in the world as they know it.

But apparently the message has more significance for the meteorologist than for meteorological layman. We could conclude: The amount of information does not only depend on the probability of an event, on our expectations. The more somebody already knows and the better his ability is to reason and his logical ability (this is the capability to track the consequences of a message in a world view), the more information he can get from a message.

3. Quantification

This more or less information means apparently that different persons get different amounts of information from a message. And this brings us to the problem, how to determine the amount of information.

If the amount of information a person gets from a message is mainly not in the message itself but depends on his previous knowledge and on his logical competence, it seems futile to look for an amount of information that could be determined objectively. Knowledge differs from person to person.

But an objective amount of information is just, what Rudolf Carnap and Yehoshua Bar–Hillel, two philosophers, where after in an article they published in 1952[3]. In this article they explored a measure of information. Their starting point was not real human knowledge and their logic was very simple: They took a very simple model consisting of three individuals and two properties. These made up their whole universe (our knowledge) to test a measure of quantification of information. If you want a more concrete situation: imagine an astronomer interested in three planets of a foreign star (the three individuals). And he is eager to get information whether there is water on them and whether there is life (the two properties). His "universe" (in this scientific project) is closed to these states of the planets under review.

[3] R. Carnap, Y. Bar–Hillel, *An outline of the theory of Semantic information*. Research Laboratory of Electronic, Massachusetts Institute of Technology, Report No. 247, 1952.

How many answers can he get? There are 64 possible answers: none, one, two or all three of the planets have water or life or both, thus from none of them has water (w) or life (l) – to all of them have water and life. This is a combinatorial calculation with the formula $(2^2)^3 = 2^6=64$. Or, to be more elaborate: There are 4 possibilities for C (w+l, w–l, –w+l, –w–l). The same 4 possibilities exist for B, so we get 4 * 4, and again for A exist the same 4 possibilities, making 4*4*4 = 64 possibilities.

Carnap/Bar Hillel concluded: The maximum information one can get in such a universe is, when the two properties are determined for all three individuals (when our astronomer knows of all three planets whether there is or is not water or life). There remains a single possibility and 63 possibilities are excluded, and this is the maximum information our astronomer can sensibly hope for. The more possibilities are excluded – the more information you get. And this can be calculated and thus quantified in such a simple model. When the astronomer gets to know there is water on planet A, 32 possibilities are excluded. If additionally, he gets to know that there is life on planet B, then 48 possibilities are excluded. Generally: The more possibilities are excluded the bigger is the informational content of the message – or: The amount of information is equal to the amount of excluded possibilities.

Of course, the model Carnap and Bar Hillel have used is far from realistic. They assume a receiver who has complete knowledge and perfect logical skill. For real life situations it is absurdly small (or it may fit for exceptional situations astronomers might be in). In real life we have to do with an indefinite if not infinite number of individuals (where "individual" means not only persons but everything that qualifies for an item to make statements about) and a number alike of properties such items may have. One could begin to doubt, whether it is sensible at all to ponder over the amount of information of messages.

But, of course, we speak about information of messages and sentences of all kind. And we do this very sensibly. Indeed, we do not try to quantify such information, but we compare the informational content of messages, as we have done here, and we state that it is very well possible to speak about more or less information. How is this possible?

We know the answer already: Our situation is not the one, Carnap and Bar Hillel have taken as basis for their analysis. When evaluating the information of a message we do not start from scratch, with no previous knowledge, where everything is possible with the same grade of probability. This led into the problem of immense numbers.

On the contrary: We have a world view. And this world view is a very, very small cutout of these zillions of possibilities. This world view, our own "universe", can be understood as decisions made among the immense number of possibilities. And these decisions are made

possible by our knowledge of facts, which we accept as well founded, or by our assured believes, as Niiniluoto says, and which make up our knowledge. We have established ideas how properties are distributed among things and persons. These are the basis of what we expect and what surprises us as new and informative. The universe has shrunk to something manageable, though it may be very large still.

A very important difference between the universe, Carnap and Bar–Hillel have taken as basis in their study and the real universe, we live in, is that their universe is complete, closed. All possible states are known. This was a condition for quantification. Such exact quantification is not possible in an open system. Our universe, our world view is open. We are conscious thereof that we never have complete knowledge of the world. We have to accommodate our knowledge permanently learning new facts enlarging our knowledge or correcting our beliefs, changing our universe. This makes exact quantification of the informational content of any incoming message impossible.

What remains of Carnap and Bar–Hillel's project of quantification of information is the possibility of a rough estimation, an estimation of the informational value of an incoming message. But even such a rough estimation will often be sufficient to compare the informational content of different messages.

And what we still can accept is that a measure of information is the amount of excluded possibilities by a message. The more a message restricts what we have thought to be possible, the more it contradicts our previous knowledge, the more of our previous knowledge a message suggests to be wrong, the larger is its informational content. In an open system, of course, we cannot restrict information to excluded possibilities. We have to take into account messages that do not contradict our knowledge but just enlarge it. Here the question of quantification gets a new turn. Following the model of Carnap and Bar–Hillel one could now think of a list of possible additions to our knowledge, but we have seen that in the real world this leads to unmanageable numbers at least, if the idea is not mad from the outset. Again we will be limited to rough estimations of the amount of information of a message, at most.

4. Logic and information

Something very important that has to be explained for the property "informative" or simply to the property "new": We refer to something as new and informative, if we have not known it before, when we have not had it in our consciousness. This is enough for communication in everyday life. But there are generally two different kinds of "newness", which are not distinguished in everyday life:

Something may be new, because it adds something hitherto really foreign to our knowledge. It adds something to our knowledge and we have to check whether our knowledge thereby only has been enriched, or whether it contradicts our previous knowledge so that we have to correct it.

The other way something is new to us, is when it is only subjectively new for us, though it could have been concluded from the knowledge we already had. It is only new to us, because we did not realize this as a consequence from what we already knew. This is what Kant calls analytic judgments:

...a great, perhaps the greatest, part of the business of our reason consists in analysis of the concepts which we already have of objects. This analysis supplies us with a considerable body of knowledge, which, while nothing but explanation or elucidation of what has already been thought in our concepts, though in a confused manner, is yet prized as being, at least as regards its form, new insight. But so far as the matter or content is concerned, there has been no extension of our previously possessed concepts, but only an analysis of them.[4]

The same idea can be found with Descartes:

But, on examination, I found that, as for logic, its syllogisms and the majority of its other precepts are of avail rather in the communication of what we already know… than in the investigation of the unknown.[5]

Or in plain words: Logic is good in explaining what one already knows or could have known, it does not help to learn anything new that cannot be inferred from previous knowledge. But it says something about knowledge: that a distinction has to be made between inferable knowledge and really new knowledge.

---

[4] I. Kant's Critique of Pure Reason, Translated by N.K. Smith, London 1929, p. 47; Kritik der reinen Vernunft, p. 51: *Ein großer Theil und vielleicht der größte von dem Geschäfte unserer Vernunft besteht in Zergliederungen der Begriffe, die wir schon von Gegenständen haben. Dieses liefert uns eine Menge von Erkenntnissen, die, ob sie gleich nicht weiter als Aufklärungen oder Erläuterungen desjenigen sind, was in unseren Begriffen (wiewohl noch auf verworrene Art) schon gedacht worden, doch wenigstens der Form nach neuen Einsichten gleich geschätzt werden, wiewohl sie der Materie oder dem Inhalte nach die Begriffe, die wir haben nicht erweitern, sondern nur auseinander setzen.*

[5] …Discourse on the Method of Rightly Conducting One's Reason and of Seeking Truth, http://www.literature.org/authors/descartes–rene/reason–discourse/chapter–02.html…

Kant and Descartes do not speak in terms of information. But they can be interpreted informationally: Everything that can be deduced logically from existing knowledge (or any analytic judgment as Kant would say) seems only to be informative because it removes subjective ignorance or doubts. Objectively such inferable knowledge is not informative; the facts where from to infer have been known and the rules of logic have been known.

To sum up: The basis of information as understanding what happens in the world are knowledge and the ability to process this knowledge, thus: logic. The ideal would be a person with complete knowledge and perfect logical skill. These are the conditions Carnap and Bar–Hillel have assumed in their model and this is what they have termed the "semantic information" of a message.

We have to live with imperfection in knowledge and logical skill. Both are given to individuals in varying degrees. This is the reason for perhaps the worst inequality in all societies, even worse than the inequality between rich and poor.

5. Societal importance of information

Since long time society has reacted to inequality of knowledge: schooling, even compulsory schooling, from kindergarten to postdoctoral studies. There is no doubt that the acquisition of knowledge can be furthered. It might be questioned whether logical skill can be taught to the same extent – though it is surely possible up to a certain degree. (One might have a suspicion here that teaching methods is just a substitute for teaching logical skill, though methods can be seen as selection and predetermination of logical possibilities.)

If our world view depends on knowledge and logical skill, and if it is mainly knowledge that can effectively be furthered in society, it is a consequence that access to knowledge is the main means to diminish inequality and further equality in society.

Knowledge is not only good for erudition. Knowledge is the basis of all decisions we make. This is commonplace in economics, where better information offers better chances. Economists could even be seen as pioneers of equality of knowledge, when economic theory classically has assumed consumers as perfectly informed persons, and in a special case, when it is striven to preserve equality by sanctioning the use of insider information. But knowledge plays a main role in all spheres of human life. Knowledge is the basis of an authentic world view. And nobody should be excluded from an authentic world view.

Access to knowledge is so important that one might wonder that it does not have an own article in constitutions. Mostly the access to knowledge and information is derived from the regulation of freedom of expression, the argumentation here above could suggest finding the

core of it already in the principle of equality. The clearest wording can be found in the European Convention on Human Rights, where the second sentence of art.10 para. 1 reads: “This right (sc.: to freedom of expression) shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.”

Indeed, when one begins to think about it, a right to knowledge seems unruly as a concept. Could a right to knowledge mean that you have a right to know everything that is known somewhere in the world? Or that you are under a duty to make public everything you know, because of the right of others? Neither seems sensible. Though, there might be an ethical obligation: Imagine somebody who has discovered a cure against a certain disease. Isn't he under a moral duty to make this knowledge known to the public? Or, are scientists obliged to make known all their insights – at least when they hold an office?

Indeed, on the European level a right of access to information has been awarded by the Directive on Environmental Information[6], by the Regulation on Access to Documents[7] and various freedom of information legislation in different countries. This legislation is important enough, though it is limited in its scope to documents and information held by public authorities. This is much too narrow.

More important perhaps for general knowledge is information not held by public authorities, but general information public authorities aim to influence or to suppress. There is no need to tell examples, history is full of them. We are permanently witnessing still suppression of information in many states. This suppression is not only an assault upon a specific right; it is an assault upon the personality as a whole: It should have become clear that everybody has the right to develop an authentic view of the world and this presupposes access to all available information. There arise questions beyond the known problems of protection of personal data and problems of public security. With another facet of the problem one could ask, whether it is admissible to let media influence people with questionable information.

But who is to decide what is authentic? Many would like to take that position, we should beware of them. The best we can arrive at is an attitude that is open for competition of opinions and leaving the decision which to follow to us. As a rule one could state that nobody may interfere with our cognitive abilities. This would be not more than a generalization of the formulation the Convention on Human Rights has used in its art. 10. The concept of semantic information does not contribute much to the formulation of such a rule. But it helps to see and underlines the importance of such a rule.

[6] Directive 2003/4/EC.
[7] Regulation 1049/2001.

Though the concept of semantic information is important enough as a means for the understanding of an elementary condition of human life, its importance is by far not exhausted thereby. Some examples might illustrate that.

6. Meaning of sentences

What is the meaning of a sentence? This question seems trivial, but it is not. There is a lot of discussion about the meaning of words and concepts. Since the Middle Ages nominalists, conceptualists, and realists have disputed about the meaning of concepts. In modern times, we have heard about the difference of extension and intension of a word, with the widely known example of morning star and evening star having the same extension, the planet Venus, but different intension. Much less popular is the discussion about the meaning of sentences, of statements, though there is a proliferate abundance of theories.[8] Semantic information can perhaps give a relative simple clue to approach the problem.

We will use in a very loose manner the model of a universe as Carnap and Bar–Hillel have proposed it, where propositions have to be tested against a universe of possibilities. Thereby one might get a rather simple answer to the question, what a sentence means. We imagine our own individual knowledge as the universe, where the meaning of a sentence is considered. The sentence will have a certain significance by being in accord or consistent with what we know and excluding other possibilities as inconsistent with the statement. One might be tempted to see the meaning of the sentence as pointing to or as a reference to the whole bulk of consistent possibilities in our knowledge, but that would not be very illuminative. Especially, as an everyday experience, we know that we ourselves do not immediately oversee all our consistent knowledge (and in this "knowledge" might even hide inconsistencies).

A better proposal than to look at the consistent possibilities as the denotation of a statement perhaps would be to understand the meaning of a sentence as an instruction to draw the line between possibilities consistent with the statement and excluded possibilities. It might be simple to draw that line in a systematically ordered knowledge like the universe Carnap/Bar–Hillel use. In our chaotic knowledge the division into possible and excluded possibilities cannot be designated by a line. This character as an instruction explains, why the meaning of a statement does not have to be instantaneously clear. It may take time to consider its effects in one's universe.

[8] Cf. Wikipedia s.v. Meaning (philosophy of language).

It is a consequence of this model of meaning that meaning has a subjective background. The individual universe decides what is in accord with one's knowledge and thus subjectively true. This explains why “snow in Florence” may have a very different meaning for different individuals, depending on their previous knowledge or expertise. On the other hand, this difference should not be exaggerated. One can take for granted that to the greatest extent our knowledge is homogeneous, shaped by homogeneous everyday experience. It is this homogeneity that makes communication possible. This might vary in different cultures and different environments. We can assume that in comparison with this homogeneous knowledge it is a very small layer on top of it where knowledge is formed by individual experience or expertise.

7. Understanding

It is a very short step from meaning to understanding. What does it mean that somebody understands a message? In ordinary talk, this seems unproblematic. Somebody has the intention to present something he has in mind, and if the receiver can reproduce this in his mind, he understands the message. But, one should doubt that this is ever exactly possible.

Understanding can be described as grasping the meaning of a statement, the process of unravelling its information. Meaning can be looked at as something objective. A statement has a meaning, whether the work of testing it for consistency with individual knowledge has been done or not. Above it has already been pointed thereto that we are not instantaneously conscious of our whole knowledge even ourselves, we do not have a place outside ourselves to get our knowledge before us and to look at it. This makes understanding subjective, individual. And here not only the individuality of knowledge decides but the second element comes into play, the skill to check a statement for information. This is the logical ability to see, whether the informational content of a message can be derived from previous knowledge, whether it extends this knowledge or whether it is in conflict with such knowledge. And this ability apparently varies from individual to individual.

Of course, there are everyday situations of understanding where we have an immediate understanding, when commonplace knowledge that can be presupposed from everybody is concerned. In such situations, one can count thereon that a message is understood immediately. But even such texts may comprise surprises. But generally the process of understanding is not an instantaneous event, often it is a process where the content of a message with its consequences becomes conscious only successively and after long pondering. Everybody in science has had this experience.

It is a somehow very astonishing fact that texts that are thousand or more years old can be spoken about, revealing new insights and showing actuality. This can have to do with implications these texts have always had, but which are revealed only now. But a more usual reason is perhaps that our knowledge, our experience, our expectations have changed, changing or expanding the information of the text, giving such texts a new meaning and thereby demand a new understanding.

8. Music

We can loosen the model of semantic information even farther and speculate about phenomena that are not bound to language. Why do many people have difficulties with so–called modern classical music? The usual explanation is that we are accustomed to a certain kind of tonality, some even maintain that this is innate. Classical music is based on the tonic, the dominant, and the subdominant. In this setting we experience musical tension or friction and relief or possibly simple dullness, too. This musical setting can be seen as equivalent with a universe of knowledge, making up one's expectations. Without such a universe we have no expectation, we have no norm, no criteria, we do not know what to exclude. Shortly: Such music has no information for the conservative listener. This does not exclude that non–tonical music has an own setting, an own universe. We find different settings in Arabic music or in the pentatonic music of the Far East. Or compositors might invent own settings which – without explanation – can only be opened up from the composition itself. This explains perhaps why performing musicians seem to have a better access to modern music. They have to deal with their music much more intensive than pure consumers do and may find a new order and information beyond harmonics.

9. Science

Above we have stated that it is impossible completely to render knowledge understood in real life; the immense number of possible states is an unsurmountable obstacle. Therefore, the information of a message will better be understood not as a confined picture of situations but as an instruction to delimit what is in accordance with the message and what is excluded by the message. In the outcome, personal knowledge and logical skill will decide how much and what information somebody draws from the message. This is the case in normal life situations.

This is not enough in any field that thinks itself suitable for a scientific approach. What we expect from science is clear answers. Any science must create and uphold a view of its field that makes it possible to unravel the information of a proposition concerning its realm. And this

view has to be intersubjective, not bound to a personal knowledge (though of course the command of this knowledge may greatly vary even among experts). This does not exclude that scientists have very own ideas and subjective judgments. But there has to be a level to discuss and to judge the value and qualification of deviating opinions.

The discussion which criteria a field must fulfill to get the status as a science has a long history. A first and necessary criterion seems to be the endeavour to find a means to make the information of assertions in a field of knowledge traceable (though it is perhaps not sufficient, in the sense that every such endeavour in any field has to be seen as science). Then all sciences are informational sciences. This makes the difference between scientists and engineers.

To make the information of assertions traceable might begin simply by collecting and fixing the established knowledge of a field. This could start with an encyclopedic collection. A next step could be to bring this collection into some thematic order. But a developed science will have seen the need to ease the disclosure of information of propositions. An established means to facilitate this is the presentation of knowledge in a systematic manner. This does not only help to find relevant knowledge. A successful system will have a logical structure and thus facilitate to keep the knowledge consistent.

What we expect from any science is that it gives the possibility to evaluate whether a proposition is in accord with existing knowledge, whether it adds something new to existing knowledge or whether it contradicts it. The evaluation, whether the proposition under review is in accordance with existing knowledge, if done in a formally correct manner, is commonly named a proof. It is here where logic comes in: A proposition is proven to be scientifically valid if it can be derived logically from established, accepted sentences in that science. We all know this from mathematics in school, when for instance Pythagoras' theorem has been proven. The usual way is to deduce a proposition from more elementary accepted more general sentences.

On the contrary, the failure of a logical proof might demonstrate, that a proposition contradicts generally accepted knowledge. Very often this indicates that the proposition under review is simply wrong. But it can signify, that parts of the hitherto accepted knowledge are to be abandoned. A famous example for this was the case in astronomy, when Copernicus found out that Earth circles around the Sun.

A third possibility is that the proposition neither can be proven, nor does it contradict existing knowledge, either. We exclude here overly speculative or nonsensical propositions. The possibility of a new insight is always given, because in all scientific systems we have to do with open systems that demand additions and completion. An impressive example of this was the formulation of the periodic system of elements by Mendeleev. This system did not change

knowledge of the hitherto known elements, it brought them into an order and opened the door to further insights. Thereby even the existence of elements which were not known yet could be predicted.

To give this an informational interpretation and applying the basic cases of semantic information: If a proposition can be derived in the system, if it can be proven valid, the proposition does objectively not extend our knowledge. The sentences wherefrom the proposition was deduced were known, the rules of logic used in the deduction were known. Therefore, the proposition tells nothing new. Only the deduction itself had been undone. Somebody with perfect knowledge and perfect logical skill would have known this before: So this sentence has no objective information.

If the sentence cannot be derived, because it tells something new, the knowledge base of a science is extended. This case did not arise in the model of Carnap/Bar–Hillel. Their knowledge base was closed, there was no new knowledge. But in an open system new, added knowledge has apparently information. This information is not only that an item is added to the knowledge base. Think of Mendeleev's periodic table again: It not only brings the elements into an order, it opens up insights into the nature of elements: their number of protons, their electron configuration, their chemical properties etc. It will not be clear at once, what the amount of information of such discoveries or inventions is. Often connections with other parts of the established knowledge will become apparent only gradually, by and by. In the end, historians will argue over the importance of discoveries (and then they argue over the amount of their information).

If the sentence contradicts established knowledge (and the sentence is true), this can mean a revolution in science. At least parts of it are wrong. The established knowledge has to be revised. In the closed model of Carnap and Bar–Hillel, a single contradiction makes the whole system worthless. Logicians can show that in a system with a contradiction any sentence can be proven to be true. So, Carnap and Bar–Hillel found in contradictions the maximum of possible information.

But we can still use their thesis that the amount of information of a proposition, sentence or message is the bigger, the more knowledge is excluded by that proposition. This seems to be counterintuitive for many, perhaps because one is inclined to find information in the meaning of the sentence as pointing or referring to something positive rather, than as pointing to excluded cases. But think of Kepler who found out that the planets do not go round the sun in a circular orbit but in an ellipsis. Whose discovery had more information? Though Kepler's discovery has opened the way to many new insights, I think that Copernicus' discovery had more information

just by overturning a whole world view. Keplers discovery was a correction of Copernicus rather. And this seems to be the preferred opinion of historians, when they speak about the Copernican Revolution.

10. Legal information

This all is of eminent importance for the science of jurisprudence. If it is the task of any science to render its established knowledge in a communicable and reproducible form law is an exemplary model as a science. Since the days of Menes in Egypt or Hammurabi of Babylon it has been the endeavour of lawyers to render their material in an ordered form. Jurisprudence has come a long way from more or less ordered lists of rules to modern more or less systematic codifications.

From the outset all codifications can be seen as not only guiding jurisdiction but as delimiting arbitrariness as well. And so they continued to do up to the elaborate codifications of our days. In all developed legal systems lawyers are bound by their respective legal order; this holds for all professions employing law: judges, advocates, commercial lawyers, administrative lawyers, etc. And this is what we expect from their reasoning: that they show that their decision, pleading, advice is derived from valid law.

In this function as a confirmation that a decision is consistent with the valid legal order legal reasoning corresponds to or even equates to proofs in other professions. However one arrived at a result, this result preliminary has to be seen as a hypothesis that has to be tested for consistency with the established rules of the respective science. Ideally, the justification of a decision has to demonstrate that it was arrived at without change or modification of existing rules or invention of new rules. In a sense, this means that the result has no information. Of course, the result and the reasoning behind it might be (subjectively) informative for somebody because actually he has not verified this reasoning himself or because he was not able to do so. But for a legal expert with perfect knowledge of the legal order and perfect logical skill the result would have been clear from the outset: for him the result says nothing new, it has no information. The decision renders just what the legal order contains for this case.

It is perfectly clear that such unambiguous results are by far not always to be expected, such results even might be seen as exceptions. Such cases have been termed figuratively as “soft cases”. What keeps lawyers busy are so–called “hard cases”, where a clear–cut result does not show up unambiguously. The reasons for this are manifold: Difficulties begin with subsumption. The law uses categorizing concepts: the facts of a case must be brought under such categories. But, whether an item belongs to one category or another or whether it will

demand a new category cannot be decided by logic. It is mostly common sense that leads subsumption and there is usually broad room for disagreement.

This is where interpretation comes in. Surely, for advocates and other practicing lawyers there will always be the tendency to steer interpretation of a rule into a direction that serves best the aim he has in mind. He will see that his interpretation supports the claim of his client or his superior. Then usually there will clash two interpretations of two representatives of two disagreeing parties.

Things become even worse, when a rule does not only offer room for interpretation but when it becomes apparent that there is no rule for the problem in question, when the legal order seems to be incomplete, when there is a lacuna in the law. Lawyers will argue similarly as in interpretation to fill in the lacuna.

What characterizes all hard cases is that lawyers not only apply law but they work on the legal order, clarifying, modifying, completing it. Now, undeniably what they do has informational value, it maintains something clarifying, modifying or completing the legal order, something new that is not – yet – established legal knowledge. This same holds for judges interpreting or completing the law in their decisions. Legislation is by definition informative (if it is not only reformulating existing law).

Legal science has traditionally offered tools for the situation that a clear rule is missing: For interpretation, different methods are offered: grammatical interpretation, historical interpretation, systematic interpretation, teleological interpretation, etc. For situations of lack of an appropriate rule: Try to find a norm top down from an established rule, *a maiore ad minus*, or try it bottom up, *a minore ad maius*, or find somewhere a regulation that is comparable and apply the idea of this rule analogously, or argue that any other interpretation would lead to absurd results. Further, law has stated general principles, governing legal regulations: that contractual parties have to act in good faith, that goods are transferable, that rights can only relate to specific goods, and many more.

Such rules might seem useful but they have a crucial flaw: There is no "meta–rule", when to use which method of interpretation, the rules of interpretation defy logical treatment. But this should be no more a surprise after what has been set out above about the relation between logic and information: Objective information begins where logic ends, informative in the objective sense is only what cannot be deduced logically.

What are these rules of interpretation then good for, what is their sense? For an answer, one has to start from the outset again that lawyers are generally bound to the established legal order. Informationally this can be understood as a command that they have to avoid inroads

into the established order or that they have to minimize information, understood objectively as changes of existing law. Even if the law is not clear or if the law needs completion, this does not give lawyers arbitrary power to emend or complete the law. They have to find a solution that is as near as possible to existing law. In this task the rules of interpretation give advice: Try an argumentation top down from an established rule, or try it bottom up from another rule, or find a comparable regulation and look by which method you arrive at a solution for your case that minimizes the inroad into existing law and keep care that your proposal does not conflict with general principles of the legal order. And this means: Keep the information of your solution as low as possible.

This sounds very conservative and indeed it is this far – but it has not necessarily to be. Clearly it might make law unattractive for revolutionists or demolitionists, but it does not hinder development and progress in law. Rules of interpretation, general principles are not categorical commands, they can be understood as standards indicating where specific argumentation is required. What we may demand from any argumentation that goes beyond established law is that it either shows that it only adjusts the existing law or indicates and justifies where it modifies or even overrules established law. This means that any decision owes us its informational content.

DOES LEGAL INFORMATICS HAVE A METHOD IN THE NEW NETWORK SOCIETY?

Ahti Saarenpää

Professor emeritus, Institute for Law and Informatics, Faculty of Law, University of Lapland, Docent, Faculty of law, University of Helsinki, Vice Chair, Finnish Data Protection Board, Finland, ahtis1@gmail.com

1. Some thoughts on legal method

When we think back on the history – or histories – of *legal informatics*, we find quite a number of the developmental phase's characteristic of a new scientific discipline. I will take up this observation in more detail later. After new phenomena have been observed, the next step is to demonstrate their importance. It is at this point, more than any other that one must come to terms with the ways in which the scientific community works. Later comes the stage when the concern is maintaining the continuing importance of the field.

Science by its very nature is very much a search for something new. However, the scientific community in the field of law is a very *conservative* one. It is a community characterised by a resistance to change and a reliance on *regulation*. Any question that cannot be linked to provisions in the written law or to case–law easily fails to attract the interest and energies of scholars. Where social scientists have been said to devour text, the typical legal academic has more of an appetite for provisions. It is hard to eat something that is not there. Accordingly, preserving the old often takes precedence over looking for the new. Indeed, as Professor *Manfred Rehbinder* many years ago has perceptively pointed out, it is easier to write the hundred and first work on something old than the first on something new.

Law, like many other sciences, is accustomed to relying on a taxonomy, or as we say in Nordic countries*, systematics*, in its work. The family of different legal sciences is an extensive one. For example, *Juridisk Nettviser*, the significant Norwegian portal for legal materials, uses a taxonomy which at the end of 2014 mentioned 66 different legal sciences. But this is only part of the truth. The spectrum of legal fields, just counting important ones, is far broader. In fact, the two fields besides legal informatics which I am particularly interested in at the moment – law of *personality* and *elder law* – are nowhere to be found as such on the *Nettviser* list. I have been teaching courses in both subjects many years at the University of Lapland. And I am certainly not the only one around studying and teaching these topics. These internationally

well–known fields should of course have their place in the taxonomy of the discipline. However, different taxonomies naturally have their particular domestic backgrounds connected to the local legal culture.

Taxonomies of a discipline no doubt play their most crucial role in universities and research departments that use well–established classifications, that is, where the academic chairs are divided by field. Indeed, when appointed to his chair, Danish professor of legal informatics *Peter Blume* made a telling reference in his inaugural speech to *subject imperialism*. This occurs in two forms. In the one, given that university chairs are typically divided by subject – largely the case in the Nordic countries – it is difficult to get a chair designated for a new subject. In the other, when recruiting researchers for positions where the particular subject(s) to be taught are not specified, competence in a new subject – or one perceived as such – may actually be an obstacle to getting a position. Due to *tacit knowledge* we a not so open–minded.

The classifications which institutions embrace and work with make them slow and reluctant to accept anything truly new. Any taxonomy will open up and close perspectives and doors. In this light, the original 1992 recommendation of the *Council of Europe* that institutes of legal informatics should be set up was a perceptive insight. The institutes offer a foothold for a dynamic taxonomy – dynamic systematics – and the opportunities for collaboration that this brings. Thanks are in order here partly to Swedish professor *Peter Seipel*. He was one of the key people involved in preparing the recommendation.

When working within the general taxonomy of his or her discipline, a lawyer is guided by what are known as *general doctrines.* Concepts, principles and theories are the key tools of our trade. As Finnish professor of legal theory *Hannu Tolonen* so aptly put it, these tools tell us what is or what can be right and wrong. A good lawyer has a good toolbox at his or her disposal for recognising legal phenomena and problems. The less able practitioner is satisfied with the traditional, somewhat amateurish, reflection on *what is fair and just* – although this, too, is occasionally a helpful approach.

It is no secret that general doctrines are very much bound to the particular field in which they are used. This is in fact one of the hallmarks of our professional specialisation. The tools and skills for using them are adapted to the needs at hand. The result is field–specific or even narrower specialisation. At the end of the day, expertise becomes associated with an individual in a progression of skills from ordinary professional to expert and, further, to authority in the field. The well–known *Dreyfus* five steps model of skill acquisition is not enough. We must also remember the role of expert authorities at the end of the path of skills. It is a long path – and often a conservative one too.

Several years ago, a book on private law was published in Finland whose author presented his ideas on the leading legal principles in certain fields of law. Legal informatics was included – accompanied by a question mark. This view was at once correct and wrong. It was correct to the extent that legal informatics cannot of course have only one leading legal principle on the level of practical jurisprudence. For example, we are dealing with two rather different concerns when we reflect on the principles of legal information retrieval and analyse the interoperability of information systems. The diverse interests of the field make legal informatics something quite different than, for example, property law or child law.

The author was quite wrong, however, if we bear in mind that, no field of law today can fail to count *respect for human rights* as one of its guiding legal principles. It is the leading principle that shapes our legal culture, in particular our theory of law in Europe. We strive for an optimal legal culture and this culture is based on human rights. Naturally, Legal Informatics is also bound to this principle, regardless of whether its focus happens to be legal information retrieval or, say, *information* law. Respect for human rights is the leading principle of general doctrines. One implication of this is that no field or group of researchers – no matter how it might emphasise its singularity – can claim human rights as its own; this fact falls naturally under the general obligation of science to adhere to the truth.

Although we do not always realise it, it is a short step from principles to methods. The ability to use principles as tools for *knowledge management* is part of our set of methodological skills. In fact, it is – and must be – a crucial part. Principles play a key role on the 'path to somewhere' – *methodos*. The old discussion in legal theory of the possibly binding nature of principles in making legal decisions gives far too narrow a picture of the importance of principles in legal life. This is not to say the discussion would be unimportant; it is just far too limited in scope where legal information management is concerned.

A lawyer's method is the element that distinguishes – or should distinguish – him or her from those practicing other professions. Professions are shaped by the method their members use, the duties they undertake and the education they receive. Law as such is open to anyone as an object of research; other professions are naturally welcome to study it. But it is the skill of the professionals in the field that primarily determines what law looks like and what it should look like. I will have something to say later on how cooperation between professions nowadays affects this.

Although the method used in a profession is one of its cornerstones, conceptions vary as to what a method entails. In 1997 we published a book in Finland called *Minun metodini – My Method*. Conceived and edited by Doctor *Juha Häyhä*, today a justice on the Finnish Supreme

Court, the work, which comprised contributions from 17 professors of law, puzzled readers and contributors alike. The philosophers' stone remained a mystery, undiscovered. It turned out that some of the authors actually had no method to speak of. They just wrote and somehow got ideas. Of course, education plays and must play a part here, too, but…

For my own part, I have, like the late Swiss professor *Alois Troller*, spoken of the *basic method* in law. As lawyers, as a profession, we share a whole range of methodological elements. These distinguish us from those engaged in other professions. I myself have divided these elements into categories on three bases: *knowledge, skill* and *procedure*.

My list of elements begins with a personal skill in legal information retrieval based on a sound familiarity with the scholarship in the field. It ends with the requirement of justified doubt, which of course is common to all sciences. Both of these elements have particular significance in the field of law. A lawyer who does not know how to look for legal information is not really a lawyer, or at least not a good one. Sorry.

Indeed, Professor *Peter Blume's* interesting methodology successfully illuminates the practical importance for any lawyer of information retrieval skills and the legal informational environment. His methodological point of departure lies in legal information retrieval. Moreover, a lawyer who does not instinctively challenge previous approaches and previous knowledge or – as all too often happens – waits for leading Supreme Court cases may, with this poverty of method, be a liability as a practitioner and researcher and to others.

But do these skills taken together constitute a method? In our *Netso* discussions, German professor *Wolfgang Mincke* has pointed out that the method of legal informatics would in fact be *information*. This idea may at first blush be quite confusing. Do we have a confounding of content and method here? Is information not a taxonomic criterion for delimiting the field and thus something other than a method?

This is certainly one way of looking at things. For example, in Nordic perspective family and inheritance law and property law are taxonomically different matters, but in methodological terms, on the level of legal dogmatics, they have been – and indeed are – closely linked. Yet, this view causes one to overlook something crucial. A method is more than a technical tool. It is a description as well. The focus of the research at hand will always influence the method. And, citing Professor *Hannu Tolonen* again, given that general doctrines tell us what is correct, our methodological choices will inevitably be bound to our research topic. What we have here are not random choices, however. The methods in a particular field are linked in a family of sorts.

If and when we say that the method of legal informatics is information, we must first take a closer look at the history of the field. The journey from realising the legal implications of data processing to operating in the multifaceted domain that is legal informatics today has been a long one. Although Swedish professor *Peter Seipel* pointed out long ago, that legal informatics is not a science that concerns itself with technological tools, for many years and in great measure work in the area was done partly in the spirit of the so called *technological imperative*. It was often overlooked that risks merited serious study. Likewise, it took a long time to wake up to the existence and importance of *information law* as one real part of our modern legal informatics.

Now that we are speaking of information as a method, we must include the examination of risks. Our society has changed; our technology has changed. Information as such can no longer be seen merely as raw material to which certain rights attach or may attach. If we choose to take *citizens' rights* seriously, we must see information as a crucial building block of society today, and of the method of legal informatics. As *Wolfgang Mincke* has also written: "One of the great achievements of societal development since mediaeval times has been the change of knowledge from an arcane good for privileged groups to a good of common property, accessible for the general population." Thanks' *Wolfgang*.

To go back to professor *Mincke's* methodological idea, he does specify what he meant: "A sufficiently comprehensive systematic law does not need a special legal method. One task of legal informatics is to reveal the informational content of legal propositions – this is the main task of any scientific endeavour; structurally, legal science is not different in this respect." This is also true. We do need a method, but not always a special *"tailored"* method.

But when speaking about legal informatics we must keep in mind the important connection to *society*. In fact, we also have long–standing traditions in legal informatics: one where information and information processing are the cornerstones of research and another, wider one, where society is the key element. Yet, it is easy to lose the connection between information and society. This applies in particular to so–called *one–act men*, whose expertise is narrow in scope; they often lack general skills and thus work in a methodological void.

Here I would like to point out what Professor *Herbert Burkert* has written. In the memory book of Professor *Jon Bing,* he also took into discussion the method of information law. The idea of Burkert is quite short and sound. We must be able to see and seek the role of information in the network society. There is no need to discuss so much about information law as discipline only.

It is essential to point out that a question that perhaps baffled us at first has now, after careful scrutiny, been answered and that the answer has or at least could have implications for research in the field. Where a method is viewed solely as a technique – or even as a technology – that one need not explain or reflect on, the essential importance of scientific self–understanding in research has been forgotten. Referring to theses written with this mind–set as research sends out the wrong signal about the role of research work as a demonstration of learning – or, in fact, of legal sophistication.

As I have noted earlier, every new scientific discipline – and traditional ones as well – should always be able to justify why it is needed and where it belongs in the scientific scheme of things. With this in mind, it is now appropriate to go on and examine closer the factors that today allow us to speak of legal informatics as an independent and significant field of law in the *Network Society*.

2. Legal informatics as a science of changes

If we think of how scientific disciplines develop, we can unhesitatingly describe legal informatics as a legal science that concerns itself first and foremost with significant *changes.* In fact, it is an exceptionally interesting member of the legal sciences in at least five ways. It is the most important of the legal sciences when it comes to delving into changes in the state, society and technology and at the same time – and crucially – taking a critical stand on those developments.

Firstly, legal informatics has been and today still is frequently referred to as a (1) quite new science. It is also regularly mentioned as concerning itself with (2) the change in society from the earliest Service Society to the Information Society. In the context of our *Netso* project, we have sought to demonstrate that society has already changed to become what we call the *Network Society.* The third distinguishing characteristic of legal informatics is (3) the significant impact it has on the changing legal culture that forms the frame of reference for legal life. It is the legal culture that guides the work of the legal profession. The fourth hallmark I could cite has to do with (4) the breadth of general scientific education it represents. The field has a range of significant and essential ties to other sciences, in particular the information sciences. It is an essential, collaborative field. The fifth characteristic of note is (5) the fundamentally international nature of legal informatics, an orientation more significant than in the case of many other fields.

Each of these features merits some elaboration – however brief – at this point. If we fail to keep them in mind, it might be difficult to understand the position and functions of legal

informatics in what is already a very extensive family of legal sciences. We can no longer speak merely of the impacts which the development of IT has quite had often on national and international legislation and regulation. This is not, of course, to overlook the fact that these are numerous and increasing in number. We are living in an era of new regulation where IT and its use are concerned. This regulation should not be regarded only from the technical or statistical point of view. It is, in a word, deeply societal.

2.1 Legal informatics as a (comparatively) new science

Legal informatics, often described as a new science despite it's already over sixty–year history as an internationally robust and modern legal science has changed the traditional structural logic of the discipline of law and continues to do so. The stages in the history of legal informatics go essentially hand in hand with changes in technology and society and as a science, it is changing the discipline of law itself.

But – and this is a crucial point – unlike most modern sciences, legal informatics is not narrow in scope and driven by a need to focus on ever–narrower specific issues; far from it. It is in fact a science that has bridged very many of the fences thrown up between fields in our very statically structured discipline. I think a few illustrative examples are in order here.

In temporal perspective, it is a good idea to start from the relation between legal informatics and *copyright*. Issues relating to the legal protection of software planners and authors came to the attention of legal informatics back in the 1960s. They were gradually recognised and accepted everywhere primarily as copyright issues. The alternative interpretation was that software was patentable. This position still prompts debate and enjoys some currency, but today the point of departure internationally is that the authors of conventional software applications are entitled to copyright protection.

The author of a computer program receives copyright protection if the program meets what is known as the threshold of originality. Determining whether this is the case requires in practice a basic knowledge of IT. Accordingly, researchers in legal informatics were the first to take a deeper interest in the topic. This connection does continue. Professor *Jon Bing* once conspicuously pointed out that there has been an *unholy marriage* between legal informatics and copyright law.

Later, but only very slowly, researchers on traditional copyright began (or had to begin) paying closer attention to the numerous copyright–related problems of interpretation connected with the use of IT and information networks as well as to the new regulation in the area. Linking on networks is a good example in this regard. It is one of the basic elements of the information

infrastructure in the Network Society. In practice, the use of the Internet is very much based on linking.

Linking as a copyright issue came to the fore in Finland for the first time when it was taken up in a doctoral thesis in legal informatics written by Lecturer *Brita Herler at the University of Vaasa.* I had the privilege of being the opponent at the public defence. In 2014 the Court of Justice of the European Union handed down a decision (Case C–466/12) in which it drew the same conclusions as Brita Herler had back in 2001. Unfortunately, the thesis, written in Swedish and defended in the Faculty of Economics, is not even always mentioned in the later legal literature on copyright in Finland. This is a regrettable example of the often closed nature that law has traditionally had as a discipline.

In the Network Society, copyright has become an increasingly prominent topic in societal debate. The issues *Herler* took up are now established topics in at least two fields – intellectual property and legal informatics – where they are studied separately and jointly; and they are discussed well beyond these fields. What at one time was a very narrow field of legal expertise has undergone – or is undergoing – a significant make–over. Copyright law is increasingly becoming law that every lawyer should know quite well. And, of course, piracy in its various forms has emerged as a serious copying and access problem in our network society.

E–commerce, which has special features, has also long been a topic of interest for researchers in legal informatics. It is only in recent years that it has attracted greater attention in the law of obligations, commercial law and tax law, an interest prompted by the increased use of open information networks in every life. Traditional mail order selling has increasingly been replaced by various forms of online sales, and the regulation relating to this has been revised in Europe. Today, this topic, too, has become an essential focus of interest for a number of fields of law. And it has sparked an interest in law in certain other disciplines, particularly Business Administration. For example, online marketing as an aspect of e–commerce makes interdisciplinary collaboration nothing short of essential. And one of the main reasons to update data protection legislation has been to strengthen the economies within the Internal Market. When trying to fulfil this goal, e–commerce and personal data protection should go hand in hand.

In terms of the systematics of law, personal data protection comes under the *law of personality*, which in turn falls under civil law. Indeed, personal data protection is unquestionably a core area within the modern law of personality. At issue are our identity and its protection when our personal data are processed. But, as we know, the legislation providing protection for personal data has been and still is one of the longer–standing areas of legal

research pursued in legal informatics and modern information law.

But, while we are on the subject, let us not forget public law. After all personal data protection is the essential interface for its principles of publicity and openness. For example, according to the Act on Openness in Government Activities, every user of a computer terminal in public administration in Finland should be familiar with the importance of privacy, personal data protection and openness in his or her use of government information systems. What is more, the shift to the era of open data, and the practical implications of the principle of openness this entails, will only increase the scope and salience of personal data protection as one of the key areas of competence needed by practicing lawyers and information systems planners in Europe.

However, it is precisely in legal informatics, in addition to the law of personality, where the core practical expertise in personal data protection can be said to lie, and clearly will remain for the most part. The development of technology and its use produce a steady stream of problems in the regulation and interpretation of the legislation providing for protection of personal data. It is partly for this reason that the European Commission submitted its proposal for a General Data Protection Regulation to the European Parliament, in January 2012. The previous directive is to be replaced by a regulation, which is better adapted to the Network Society and is more binding than a directive. And we must of course remember the European Charter too. Protection of personal data is now one of our written fundamental rights. Every single time when we process personal data, we are processing a fundamental right.

The development of IT in public administration has brought to light the relation between legal informatics and administrative law. Traditional administrative law has been a field whose research has been characterised by a focus on procedures and the regulation of different areas of government administration. Even the very first stage in computerising government brought legal informatics into the picture. The first wave of German legal informatics, in the early 1970s, directed considerable attention to the use of IT as a tool in government. Later, the topic spawned important doctoral theses in Sweden and Norway – *Magnusson–Sjöberg* and *Schartum* – as well.

In today's Network Society, one of the principal focuses of legal informatics is the *legal planning* (design) of government information systems. Government is dependent on those systems, and so are citizens and public bodies to an increasing extent. Conventional research in administrative law has yet to take much of an interest in this development. Information systems in administration are too often seen as practical tools only.

We should also not forget criminal law in this context. The development of IT is also

reflected in the essential changes that have had to be made in criminal sanctions to include situations where earlier legislation failed to cover the new methods by which crimes are committed in the digital environment. For example, payment device fraud committed using systems for monetary transactions represents the new regulation that falls squarely within the scope of research in legal informatics. Naturally, where the sanctions are concerned, these forms of fraud merit examining in the field of criminal law.

In a similar development, information network crime has been given a place among the crimes for which sanctions have been enacted in the Finnish Criminal Code too This issue and the international and national legislation to combat cybercrimes are long–standing interests of legal informatics more so than of other areas of law. Not even the practicing lawyer can get by any longer without knowledge of the international conventions in this area.

It is thanks to these conventions that at the beginning of May 2014 Finland finally woke up to the importance of the identity theft on the societal level. The Ministry of Justice, which astoundingly had previously opposed enacting legislation, has now decided to propose that identity thefts be criminalised. Its previous negative position clearly stemmed from its inability to recognise and react to a change taking place in society. In the Network Society, identity theft is a grave violation of an individual's right to self–determination. The new Finnish regulation is coming in force at the beginning of September 2015.

Similarly, we need to note that the investigation of various information and information network crimes has required new procedural rules for investigation and surveillance. An example is the new Coercive Measures Act that came into force in Finland in 2014. Then again, it had to be amended even before it came into force because of shortcomings in the drafting: its treatment of information and communications technology was poor and it largely ignored the perspective of legal informatics.

These small, disparate examples provide an insightful overview of the multidisciplinary scope of the research interests in legal informatics. Legal informatics, a relative newcomer as a science, is thus not narrow in scope – as such fields tend to be – but rather, in traditional terms, more of a comparatively new multidisciplinary science. For precisely this reason, it is a more difficult area of law in practice than conventional scientific fields.

The roots of legal informatics lie ultimately and primarily in the area of legal theory. As the state and society change, the role of legal informatics as one of the general legal sciences is set to increase, and markedly. Then again, in the new constitutional state, with its characteristic juridification, legal informatics is called upon in increasing measure to address questions of regulation and interpretation that reach into many areas of law that fall within its traditional

systematics. If legal informatics did not work this way, the socially crucial relation between law and IT would not get anywhere near the attention it merits, with specific, important details being lost in the process as well. Here we see legal informatics performing its function as a field that serves other fields in the discipline of law and as an observatory that picks up on new developments.

Here, we can justifiably speak of the introduction of a *dynamic systematics* as one of the more visible changes that has affected modern law. The traditional *static systematics* of the discipline with its precise categorisations of the fields of law has to an increasing extent become accompanied by – or is at least seeing the emergence of – a dynamic categorisation. Law as a phenomenon and object of regulation is being examined simultaneously from a number of different perspectives. A dynamic systematics provides the tools to avert the unwillingness to confront the new which could be seen in the case of the old, static system. In this way, the science becomes more sophisticated, elegant and the professional skill of practicing lawyers acquires a new effectiveness. This is one of the important messages that legal informatics wants to send in the Network Society, which is becoming increasing complex, legally and otherwise of course.

Adding to the number of scientific fields that bridge traditional disciplinary boundaries has generally been more difficult than specialising with a traditional field. For this reason, despite its unassailable importance, it has taken a comparatively long time for legal informatics to establish itself as a field of legal teaching, although the actual process has varied in different countries. It is only with the advent of a dynamic and versatile systematics in the last few decades, essential to the modern, rapidly developing constitutional state, that legal informatics has gained a more visible place in the family of legal sciences nationally and internationally. This is extremely important if we think of legal practice. Understanding IT and using it to and, by extension, legal informatics as a science must no longer be novel acquaintances to legal professionals; nor should the field's links to IT cause professionals to shy away from legal informatics for fear of inadequate skills. The basic messages written into the 1992 Recommendation of the Council of Europe titled "Teaching, research and training in the field of law and information technology" are today even more important than earlier.

2.2. Legal informatics as a science of societal changes.

Societal change is the second key driver in the development of modern legal informatics. The scope of the field has broadened beyond noticing innovations in IT. Early legal informatics – that seen in the late 1940s and in the following two decades and that was initially *jurimetrics*

as described by *Lee Loevinger* – drew its vitality primarily from observations made on the opportunities brought by the new information technology and on the positive and negative impacts it might have. This era is most certainly well behind us although one still comes across those lawyers for whom the use of IT and information systems, at least personally, is a regrettably unfamiliar practice.

Legal informatics as we know it today in Nordic countries – a science concerned with law and IT and law and information – examines questions that have become issues of crucial importance not only where the development of European society is concerned but, more recently, globally as well. For example, sophisticated data protection legislation has become one of the fundamental requirements for the development of international commerce. In the Network Society, geographical borders are declining in importance, but crossing legal borders in various activities is occasionally harder than before, particularly where the borders are those of the European Union. In the same vein, sophisticated data protection legislation is today one of the basic requirements that countries seeking membership in the EU must fulfil, for personal data protection is an important fundamental right in Europe.

It is beyond dispute that as changes have occurred in core infrastructures – particularly the information infrastructure – in the importance of information and its quality and in how IT is used, society has also changed in a fundamental way. The society that we used to live in, one that learned to reap the benefits of IT and for a long time was called the *Information Society*, has changed again to become what is known as the modern *Network Society*, a society where people live, work and communicate in a digital environment.

This transition is in many ways a significant one. Thus, the society envisaged in the EU Commission's action plan titled "eEurope 2005: an information society for all (COM(2002)163) was a society clearly based on an information infrastructure characterised by rapid information networks. Its follower, "i2010 – A European Information Society for growth and employment" (COM(2005)229) continued along the same lines. And the trend continued in the Digital Agenda published in 2010 (COM(2010)0245), which contains a sizeable number of detailed objectives based on the practical everyday use and functionality of networks.

Sophisticated information networks and their secure multipurpose use have become more important than ever before for the development of European society. In addition, one can now hear talk of the Green Information Society, a study on and draft programme for which were finished already during the Swedish presidency of the EU in 2009. The document can – at the risk of some simplification – be seen as an indication that IT is no longer referred to as a separate matter. IT cannot be detached from other social development, for example, in terms of its energy

consumption and other impacts on the economy or environment. Information technology, like everything else, must observe the principles of sustainable development. The age of ITC as something very special should be over.

The change in the significance of computers, information systems and information networks entails changes in the approach we must take to many legal issues and, ultimately, in rights. These span the gamut from citizens' rights to public use of open information networks to information wars that take place on information networks or affect those networks. Similarly, legal regulation is on the increase, the number of significant legal concepts is on the rise and legal principles as well are changing. Indeed, in the European Union we now routinely speak of the *new legal framework* of the Network Society.

The change whereby our society became a network society has temporally coincided to a considerable degree with an exceptionally significant change in the form of *state* we live in. We live in Finland and since the early 1990s, we have lived in constitutional state undergoing a transformation. The importance of that state for democracy is being increasingly emphasised and in new ways. The age of the old–fashioned Nordic administrative state is over.

Finland's accession to the Council of Europe (1989) and several years later to the European Union (1995) did much to speed up this development. Progress has been made from the older Nordic administrative state, which largely subordinated and sought to steer people, towards building the legislative base for a modern European constitutional state that is based more clearly on respect for the individual's right of self–determination.

The strengthening of the constitutional state has, among other things, led to a new type of juridification. The legislative core of that development is the scrupulous respect for *fundamental rights* based on *human rights* and, in particular, *human dignity*. Accordingly, in the relationship between the individual and government, we have seen the earlier general competence of an authority replaced by a special competence subject to detailed regulation. For example, this change limits the possibilities to use technology to monitor people or for other forms of surveillance. Moreover, the earlier quite open general *institutional (public) power* has now changed – and is still – changing to become special regulation to protect citizens' rights.

The difference between the modern constitutional state and the earlier administrative state is, or at least should be, considerable in both theory and practice. However, many conservative "open the law collection" lawyers have been slow to observe or to accept this change. And, unfortunately, there have been a few reluctant voices in the field of legal theory as well. Legal theory without following the changes of state and ICT is dangerous when thinking about the role of legal theory in our legal thinking.

In line with the above–mentioned developments, we see more and more matters that relate to information, information systems, information government, data processing and communication – and to individuals as well – being governed by provisions in the law; this is in fact required. And this is legislation, like all other in the constitutional state, that is enacted in increasing measure with due consideration for the rights of the individual. Properly formulating those rights requires enactment of legislation, given that personal data protection, privacy and freedom of speech are European fundamental rights. We can now speak with full justification of a new *legal network society*.

For its part, the development that has taken place in ICT justifies reference to a new digital working environment in the case of individuals as well as organisations. This is an environment in which – let me tell it once again – ICT is no longer viewed as a mere technical tool nor information as cheap raw material as once was the case. Rather, we are in practice – whether at work or play – in ever more ways dependent on that digital environment.

To put it succinctly, the use of information, information products, communications systems and IT, as well as the fundamental rights associated with these, are the underpinnings of the Network Society. Without them, that society could not function nor could justice prevail. Drawing on such an insight, German researcher in legal informatics and professor at the University of Münster, *Thomas Hoeren*, has pointed out that we have in fact adopted a new, significant concept of justice: *informational justice*. I agree with him wholeheartedly. It is one of the key forms of justice today, one meriting special consideration.

At the same time, the state itself has – as I have already mentioned – changed. The increased importance in the new constitutional state of human and fundamental rights, enshrined in international conventions, compels us to take a closer and more balanced look at the individual's right of *self–determination* and how this can be safeguarded in what is a changing society. In the modern constitutional state, law must be taken into account earlier and earlier. And this is one of the basic premises of modern legal informatics too. This no longer applies exclusively or primarily to a fair trial. What has happened is that the new concept of the human being, the constitutional state more generally, and the Network Society in particular have at the same time but for different reasons become central factors of change that influence one another. The rights of the individual have also taken on heightened salience in information systems and information networks.

Yet this is but part of the change that is occurring. With the information infrastructure now dependent to a significant extent on data processing, information systems, information tools, information networks and the information markets, we naturally see an array of novel

risks. Indeed, the Network Society is increasingly also a *risk society*. The risk society described by Professor *Ulrich Beck* in the beginning of the 1990s has, to an increasing extent, become a new kind of risk society. In the information security report published in 1997 by the Institute for Legal Informatics at the University of Lapland, we considered the risks that were associated with the development of the Information Society at the time. They are mostly still relevant. But now we are witnessing some other risks, especially *cyber risks*.

Disruptions in access to information and communication systems can well be compared with power outages in the national grid. The mutual dependency of networks is particularly critical for the activities of society as a whole. But the risks are not confined to the technical vulnerabilities of what is a critical infrastructure. The risks already arise where decisions are made on what kinds of information systems are planned and acquired and how and what kind of data is attached to different templates.

New risks naturally entail new challenges when it comes to law, legislation and drafting. Yet, at issue, here is more than ordinary juridification, which follows the development of society comparatively slowly; we are talking about early detection of risks. An illustrative case, a particularly important one, is *information security*: it is a topic that legal informatics studies but an area that to date is essentially unregulated – or at least the regulation we have is insufficient and less systematic than it should be. Internationally, however, development is gradually proceeding towards more comprehensive legislation in the area of information security. In this vein, in Finland, in the capacity of an overseer of legality, the Parliamentary Ombudsman has pointed out the importance of information security as an aspect of good governance. And good governance is a fundamental right in Finland:

> *Constitution section 21:*
> *Everyone has the right to have his or her case dealt with appropriately and without undue delay by a legally competent court of law or other authority, as well as to have a decision pertaining to his or her rights or obligations reviewed by a court of law or other independent organ for the administration of justice.*
> *Provisions concerning the publicity of proceedings, the right to be heard, the right to receive a reasoned decision and the right of appeal, as well as the other guarantees of a fair trial and good governance shall be laid down by an Act.*

Yet there is a flipside to this development. The heightened enthusiasm that has emerged for using computers and information networks for purposes of control and supervision is making the Network Society a surveillance and control society to an increasing extent. What at

once a time was a risk in the abstract, a peril described mostly in science fiction, is now becoming a concrete threat. The most recent evidence of this can be seen in the recently publicised logs of network surveillance carried out by various countries.

Surveillance that makes use of technology in a variety of ways and the desire to use it extensively are both increasing, testing the limits of the constitutional state and occasionally violating them. Furthermore, the desire to increase the use of biological identifiers and the interest in sharing various registers are objectives typical of a burgeoning surveillance society. Fuelling this development is the new generation of computing devices. For example, a smartphone is, as has been aptly noted in international discussion, a surveillance device that can also be used to make phone calls.

It is important to understand, that "surveillance society" is not only a slogan in the media and social media. It has been and still is a scientific concept. As for example Professor *David Lyon* has demonstrated many times, the Surveillance Society is partly a society where government strives for effectiveness with surveillance tools and partly a society where invisible surveillance is in use. The issue is in fact not new; the solutions are.

Legal informatics is one of the sciences that studies the risks – even the risk of surveillance – associated with the digital environment in which we live and work. Given this focus, the field has received increased societal support in recent years for its existence and importance with the changes that have occurred in in society. The transitions to electronic information government that is dependent on IT, to information and communication and, more generally, to network communication and e–commerce have also served to enhance the societal significance of legal informatics. Then again, there is nothing exceptional here if we think of the development of the science. Law, as a crucial *planning science*, should always carefully anticipate and observe changes. This function is essentially alien to conventional law, which waits for precedents and explains them in terms of established concepts.

2.3 Legal Informatics and the legal culture

As it has with other spheres of society, legal informatics has numerous links with the legal culture. Put briefly, a legal culture refers to the complex consisting of legislation, the mechanism by which it is applied and the circumstances under which law operates. In other words, the focus is not – unlike is often surmised – solely the relation between law and culture at large but rather, and above all, the culture of a community: the factors that underpin the activities of the legal profession. Professors *Rogelio Pérez–Perdomo* and *Lawrence Friedman* have in fact stated that without a legal culture law is dead, a *skeleton*, nothing but words on

paper. Living law, by contrast, owes its very existence to there being a legal culture. I fully agree. The crucial components of the legal culture are – to cite Swedish professor of legal history *Kjell Åke Modéer* – leading legal principles, the quality of legal norms, the structure of the decision–making apparatus, communication about law and the infrastructures that lawyers have at their disposal. I would add to these the quality of legal information and, above all, the readiness to detect changes. And I would like to add the citizen's point of view. We should not look at the legal culture only as the lawyer's culture. Not at all.

The legal culture has become an increasingly important perspective on law in recent years. After all, in the constitutional state we try to achieve an optimal legal culture – in fact we must try to do so. *Modéer* stressed this as well. Shortcomings and distortions in the legal culture jeopardise the realisation of the rights of the individual in the constitutional state. At the end of the day, the crucial element here is the professional skill of lawyers, although legislation and various legal mechanisms figure significantly as well.

The digital environment is a significant variable in the legal culture. Efforts to achieve an optimal legal culture that respects the rights of the individual require that we reassess the component factors of that culture. Of particular importance are the way in which the law is communicated and the changes that have occurred in the infrastructures that lawyers use. The path that legal information takes from being attached to the first computer program template to being processed by the end user must be wholly reassessed in the Network Society. Every disruption on that path – for example an information specialist with no legal training or an inconsistent practice in recording information – may prove very detrimental indeed.

Often, regrettably often, discussions of method ignore the role of libraries and of legal information maintenance more generally. Knowledge management and knowledge acquisition are seen as no more than technical matters and matters for others to handle, not lawyers. Here we see the importance of the path of legal information being forgotten. Correct information does not end up in the correct place by itself nor are traditional libraries as such sufficient to ensure the availability and accessibility of information.

Even back in the earlier age of legal databanks we could see a significant change where method was concerned. Above all, Professors *Jon Bing* and *Peter Seipel* demonstrated for the Nordic countries that the professional skills of a lawyer – a good lawyer – had come to include a new component: active information retrieval skills. *Seipel's* famous statement that sloppy information retrieval can make you 'lose your case and lose your face' rather says it all. It is of course still valid – even more so – when thinking about our modern digital information environment.

The transition to the use of legal data banks was facilitated by the fact that in most countries and for most tasks it was initially enough to know how one important databank worked. Today we have to master the use of a far wider array of information repositories. At the same time, the new expression *information literacy skills* has inescapably come to apply to legal life as well. Literacy has become part, a significant part, of the legal culture today. Our knowledge environment has changed from what it used to be to become a far more demanding one. The apparent ease of the digital environment in which we live and work and the methodological rigor that legal information retrieval demands of us challenge each other in both theory and practice.

In today's digital environment the *so–called arm's length rule* still operates but in a new form. This manifestation of methodological indifference, one of the many *Peter Seipel* has brought to our attention, rears its ugly head at its worst where information is sought using no more than a browser, most often Google, the most popular such application. Of course, correct information can sometimes be found this way or else added value can be had for earlier material. But this is not how a good lawyer works. Information retrieval skills, a part of our basic method, are something quite different from the unsystematic use of a browser to search the information space of the Internet. We must know as a matter of principle where, how and with what risks correct information can be obtained. The legal culture has, I assure you, changed markedly from what it was in the days when, for example, in Finland it was enough for a lawyer to be able to open the systematic printed statute collection *Suomen Laki (Finnish Law)* to the right page. The Finnish legal theoretician, Professor *Kauko Wikström* has most aptly referred to such behaviour as the *open the law book* doctrine of the sources of law.

When science fiction writer and futurologist *Isaac Asimov* delivered an address at the 70th anniversary of the ABA Journal in 1984, he predicted that the *balance of information* would improve in trials with the development of legal data banks in the decades to come. This observation was right on the mark. We now live in an age where data banks are being used more extensively in legal life in different countries. With this development, opportunities for an improved balance of information in different legal relationships are increasing. However, development has not been quite as simple as *Asimov* perhaps thought it would be. Just making the official, primary sources of law available to all has taken a surprisingly long time in different legal cultures. And the markets for secondary sources, which bring added value, often pose an obstacle to achieving a balance of information. Moreover, *Asimov* failed to anticipate the impact of the spread of the constitutional state internationally.

One upshot of the developments we have witnessed is that we must consider the changes they entail in the training of the legal profession. We no longer educate lawyers to work in the traditional manual operating environment. Yet, at this writing, this is what a sizable proportion of practicing lawyers have been trained for. This will give rise to tensions, and considerable ones, in terms of knowledge and skills between the old and new legal professional skill set. The basic methods of different generations of lawyers will end up varying, a development that may ultimately undermine the rights of citizens to a significant extent.

One of the many crucial phenomena in the Network Society where the legal culture is concerned is the requirement that legislation be informative. Now that the laws in force are increasingly available to citizens on open networks without intermediaries, we must ask ourselves what the text of a law should look like in order to be understandable. The basic principle here of course is that old one that citizens must know the law. Ignorantia juris non-excusat (Ignorance of the law does not excuse).

Another question we must pose now that the text of the law is more readily accessible to everyone is the extent to which interpretations by authorities or courts can be allowed that clearly depart from the primary wording of the law. Such interpretations will no doubt more clearly than before undermine people's perception of whether justice is being served. The old saying that the law is as it is read will, in the worst case, gain a new vitality as cases whose decisions depart from the letter of the law become more frequently available on open networks in the Network Society. If the decisions in case–law seem to run contrary to what is said in the written law, citizens will have difficulties understanding what is going on in the society.

One characteristic of the legal profession, as noted earlier, is its *conservative* nature. This collective focus on maintaining the status quo is a critical problem for professional skills in the Network Society, where developments proceed apace. Indeed, in different countries the profession – at least in the established legal culture – has been comparatively slow to wake up to developments in computer technology. Accordingly, one of the central tasks of legal informatics has been and continues to be pointing out change. In fact, legal informatics has sometimes been referred to as an *observatory* for detecting new developments. In more theoretical perspective legal informatics could also be described, at least in part, as futures research in law. All of this is essential to answering the question, what is the method of legal informatics?

2.4 Interdisciplinarity

The fourth element characteristic of legal informatics and pertinent to its method is its interdisciplinarity. As a field of teaching and research, legal informatics is distinctively multi– or interdisciplinary both when working within and crossing the boundaries of the science of law. As a matter of fact, this emphasis on interdisciplinarity has become somewhat of a catchphrase in describing the field.

Within law, when we say that legal informatics is interdisciplinary we mean that it is a field of research and teaching that bridges the boundaries of the traditional systematics of law, a feature noted earlier. Researchers in legal informatics are accordingly required to have a broader–than–average general education in law in order to avoid falling into what I have called the *specialist gap*. This is a shortfall in expertise, known in many other fields as well, that appears primarily as an inability to recognise problems – both traditional and novel – outside of one's own narrow specialisation. And of course the field's new dynamic systematics is a constant challenge.

Beyond the boundaries of law, legal informatics necessarily has essential links to IT, data processing, communication and, more generally, the information sciences. In addition, the vigorous development of information government unavoidably links the administrative sciences and law to one another in a new way. We clearly need more scientific *cooperation* in our digital environment.

One thing we cannot under any circumstances overlook when speaking about legal informatics is its relation to change in society and to other sciences that study such change. In traditional law, monitoring the development of society and identifying the legal challenges this posed were pursuits largely undertaken by legal theory and thus dealt with as highly abstract, theoretical issues. These very rarely had any impact to show on the interpretation of legislation. In contrast, legal informatics is a field where assessment of developments in society is most clearly a fundamental focus. When we speak of the Network Society today, we are confronted with basic questions of what kind of society we live in and what the requirements are that our changing society places on legislation. And, at the end of the day, what we are concerned with is implementing our conception of the human being in the Network Society.

These considerations make it necessary for those working in the field of legal informatics to have a broader–than–average scientific background. Depending on the topic, a researcher in the field must have a readiness to keep abreast of developments in IT, the sociology of knowledge, cognitive science, the activities of the media, the development of government and,

more generally, to follow scientific inquiry in other fields – sociology for one – that are concerned with technology–driven change in society.

All in all, the fundamental element of a broad scientific education – a readiness to identify problems and to engage in fruitful dialogue with representatives of other disciplines – is part and parcel of work in legal informatics, day in day out. This makes it a far more demanding legal science – particularly where its theory is concerned – than a conventional, narrow area of law focused on interpretation, which for quantitative reasons seeks to become ever–narrower.

At this juncture, it is appropriate to point out that that legal informatics is a very different matter than what is known as technology law, a field that has occasionally been mentioned in the same breath as IT. Monitoring the development of technology is by no means a novel matter for law or the legislator; far from it. As, for example, Professor *Dieter von Stephanitz* demonstrated back in the early 1970s, the relation between law and the exact sciences has long been a fascinating topic. Whenever the development and use of technology brings genuine legal problems to light, law – and possibly the legislator as well – should sit up and take note. For law, this role of observer comes naturally; it is among the basic functions of our science. Law is for society.

This issue is one that simply cannot be ignored on the level of general legal sciences: it lies at the very core of legal thought. Finnish philosopher, Professor *Timo Airaksinen* has demonstrated that there is an essential social demand for a philosophy of technology; I dare say we are every bit as in need of a legal philosophy and legal theory that concern themselves with the relation between technology and law. Scientific inquiries along these lines have rarely, very rarely, been undertaken.

If, to take the opposite tack, we think of establishing a special field of law that would examine the relation between law and technology, the matter appears to be significantly more complicated. After all, technology is a very broad field indeed, one that encompasses a diverse body of legislation and, above all, legislation that extends into many of the traditional fields of law.

In some of the legislation, regulation of the use of technology plays a significant role. This is the case with nuclear power, for example. And some of the legislation applies to the consequences of the everyday use of technology, an example being regulation on noise. Likewise, we are also used to prescribing the competence required for using various pieces of equipment. These provisions, too, are technology–related legislation. It would thus be utterly artificial to change the conventional classification of law to create a special subject that brings together legislation on technology far and wide on the level of legal doctrine and calls itself

"law and technology". The subject would juxtapose issues that in terms of legislation are not commensurate.

And this putative subject would require a combination of expertise's that no one is very likely to be able to acquire in the depth and breadth required. Likewise, such a subject might, like certain other subjects in law and other disciplines, find itself with a negative reputation among practicing lawyers – being theory for theory's sake. It is a different matter that internationally the relation between law and technology is examined in a number of legal journals. Good lawyers should always be curious. They do need such journals. Good examples are *Jurimetrics*, as well as the *European Journal of Law and Technology* (EJLT), whose primary focus is legal informatics.

Whereas the relation between law and technology is a long–standing topic – but a diffuse one that threatens to become even more so as technology progresses – legal informatics is for the most part a quite new entity. The integrity of legal informatics as a field is primarily ensured by its enduring focus on the developments in modern IT and communication and the impact of those developments. The progress in these two areas is rather modest as such; but it has astonishingly wide–ranging societal impacts and is an aspect of technological development that is constantly changing.

2.5 Legal informatics as an international legal science

Law has long been considered primarily a national science. And, accordingly, the legal profession has been offered training that draws primarily on domestic sources of law. This mentality is gradually but radically changing. Legal life is becoming more and more international in many respects. If nothing else, the increasingly international nature of legal source materials is changing law as a whole into an international discipline. In addition, human rights conventions and EU legislation and the related case–law necessarily introduce practicing lawyers today to international legislation and make them alert to trends in case–law. The *depth of the sources of law*, which has direct bearing on a lawyer's professional skill, is increasing.

The broader, very profound impact of the EU on the increasingly international character of law as we know it should not be overlooked in the least. In practice, there is no field within the legal sciences that can justifiably isolate itself and work exclusively within the confines of national legislation. Principles and concepts increasingly have an evident international background. The change that has occurred in the last two decades has been nothing less than staggering. The new European regulation relating to IT and information networks has figured prominently in that change.

Not to be overlooked of course is the international course on which legal informatics has embarked on its own. It is in fact a premier example of an international legal science. Even when research in the field focuses on the interpretation of national provisions, the laws most often pertain to the Network Society and have an international origin. This in itself creates a solid international orientation when comparing sources of law.

In other respects, as well, modern legal informatics has from the very outset been a distinctively international science. International cooperation in teaching and research has been and continues to be brisk. The development of legal informatics in Finland has been every bit as international as that elsewhere and visibly so; at the outset, it featured a particular focus on Nordic collaboration.

A closer look at the robust international nature of legal informatics as a legal science reveals at least three principal reasons for the development we have seen. First, very many of the issues that were important when the modern computer came onto the market were and still are essential concerns to be addressed by *legal theory*. And legal theory is the most international field possible within law: Questions of law, justice and what is right are important everywhere.

A second explanatory factor is the spread of IT and information networks and their extensive use throughout the globe. However, the development of the field was influenced earlier by the geographical context in which the use of IT grew. As the focus initially was largely on the United States, research in legal informatics had to – and still has to – assess concepts and procedures that arose in a very different legal culture. For example, American contracting practices, copyright legislation and privacy questions were not for the most part directly transferable to the domestic Finnish context. Research in that area required and still requires sufficient methodological skills in comparative law. This is a real problem in a country, where comparative law in legal studies has been in a minor role a long time.

The third key factor that has contributed to legal informatics being international is, of course, the emergence of the Network Society. It is an utterly international phenomenon. Networks network. Regulation of the information and communication markets requires international collaboration and the EU has in a comparatively short space of time become a driver of sorts for legislation on the Network Society.

An insightful example of this has been with us in the equivalence (adequacy) requirement set out in the Personal Data Directive (95/46/EC). Before personal data can be transmitted outside of the EU, it must be established that the data protection legislation of the receiving country is of an acceptable standard in European terms. This means that international businesses and international trade are in large measure guided directly or indirectly by the requirements of

the Personal Data Directive (in the near future by those of the Personal Data Regulation). A sound knowledge of data protection legislation together with information security is thus essential for anyone working with national and international business today.

3. Conclusion

I began with a short discussion of method and brought out that a method is more than just an inventory of essential practical skills; it is also closely linked to the systematics of the science and the legal culture. And, in the final analysis, it of course has to be bound to our concept of the human being.

I then continued by describing the links between legal informatics and society and societal development. Here I brought out five distinctive features of the field. Now, I owe it to the reader to combine these two somewhat disparate presentations. Let me now do this briefly and succinctly.

I would assert that legal informatics is an observatory for human rights in the Network Society, a society where information networks and information systems are not mere tools but a working and living environment for individuals and organisations. The fact that access to those networks and the resources on them has begun to be seen as a human right tells us something essential about the development of the Legal Network Society. It is precisely such considerations that lawyers are able to focus on when informed by a proper method in legal informatics.

As what might be a fitting conclusion for this article, I would like to present a decision by the Finnish Parliamentary Ombudsman. One of the Ombudsman's principal duties in Finland is to oversee the realisation of human and fundamental rights. Today that task requires an understanding of the Network Society.

The Ombudsman had in 2014 two cases (C 2617/2013) brought to his attention in which a person under guardianship had not been given online banking codes (typically a customer number and key). He noted in the ensuing decision that having such online banking credentials, which in Finland can be used to register – log into – for many other private and public services and for strong authentication, is one salient element of *equality*. The Ombudsman went on to explain his position as follows: "I would emphasise that not even persons under guardianship should be categorically denied secure access to society's services even when restrictions on their legal capacity might mean they cannot use online banking credentials. Rather, the actions taken by a guardian should be in reasonable proportion to the aims in the case at hand."

That is very much the case. In the new Network Society, we are witnessing the age of *access* rights. That is why we, even those of us who have guardians, need different kinds of access tools for personal identification processes when using modern network services. We all are dependent on networks. Our conception of the human being must change accordingly. The UN Convention on the Rights of Persons with Disabilities is the underpinning of this kind of thinking. But in our legal life this is very much a methodological question too. The basic method must be connected to the changed society.

And now shortly back to information. Is it as *Wolfgang Mincke* said, the key to the new methodology. Yes, it is. But it must also be seen as an important part of the Network society. Here we come also to the idea of *Herbert Burkert*. We must be able to see and seek the new role of information and information processes. So we do need legal informatics to understand better the legal challenges of the Network Society.

OPEN GOVERNMENT DATA: LEGAL, ECONOMICAL AND SEMANTIC WEB ASPECTS[1]

Dino Girardi[1], **Monica Palmirani**[2]

[1] Ph.D. Candidate, Institute for Law and Informatics – University of Lapland, CIRSFID – University of Bologna, dino.girardi@ulapland.fi
[2] Professor of Legal Informatics, CIRSFID – University of Bologna, monica.palmirani@unibo.it

Keywords: *open data, public sector information, open government data, linked open data, transparency, personal data, licences, charging, business models, semantic web, interoperability, formats, standards, metadata.*

Abstract*: This paper is an overview on the Open Government Data (OGD) environment in the EU. It aims to point out the relevant legal issues together with the economic aspects arising from the disclosure and exploitation of OGD. Therefore, the paper highlights the noteworthy technological aspects related with the opening of OGD datasets. This survey is based on an interdisciplinary approach. Interdisciplinarity in the digital environment means that OGD should be considered as an integrated, interoperable and collaborative ecosystem. The main legislative source taken into account for the survey is the Directive 2003/98/EC on the re–use of public sector information as recently amended by the Directive 37/2013/EU.*

1. An overview on Open Government Data

The concept of Open Data and specifically Open Government Data (OGD) refers to policies and practices of the States related to opening their datasets (constituted by Public Sector Information – PSI) and making them generally available for anyone free to access and re–usable for any lawful purpose.

The Open Knowledge Foundation – OKF[2] provides a definition of Open Data that is generally accepted and broadly used. As to the Open Definition "Open data is data that can be freely used, reused and redistributed by anyone – subject only, at most, to the requirement to

[1] Also published [in:] Saarenpää, Sztobryn (eds.), Lawyers in the Media Society. The Legal Challenges of the Media Society, Rovaniemi 2016
[2] The Open Knowledge Foundation –OFKN, trading as Open Knowledge, is dedicated to promoting the creation, sharing and application of Open Knowledge in the Digital Age. More detail about OFKN can be found at https://okfn.org/about/.

attribute and sharealike"[3]. The Open Definition sets out in detail the requirements for "openness" in relation to content and data in the "Open Data Handbook"[4].

In the Open Government Data website[5] the OKF defines Open Government Data as follows:

- "open" means data that is open according to the Open Definition, as above explained.
- "government data" means data and information produced or commissioned by government or government controlled entities.

Referring to the EU Directive 2003/98/EC, Government Data is synonymous of Public Sector Information (PSI). The public sector bodies of the Member States "collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, economic, geographical, weather, tourist, business, patent and educational information"[6]. This information, recorded as documents, "constitute a vast, diverse and valuable pool of resources (datasets) that can benefit the knowledge economy"[7].

The same concept is clarified in the Open Data Handbook: "Open data, especially open government data, is a tremendous resource that is as yet largely untapped. Many individuals and organisations collect a broad range of different types of data in order to perform their tasks. Government is particularly significant in this respect, both because of the quantity and centrality of the data it collects, but also because most of that government data is public data by law, and therefore could be made open and made available for others to use"[8].

In this paper, reference to the Open Government Data (OGD) means Public Sector Information (PSI) datasets opened and disseminated as to the Open Data notion.

The concept of OGD paradigm as a global phenomenon is based on several initiatives like the Obama's declaration[9] of 2009, the Tim Berners–Lee TED talk[10] in 2009 and the Cameron[11] letter in 2010. Therefore, in June 2013 the Open Data Charter[12] was approved by

[3] http://opendatahandbook.org/guide/en/what–is–open–data/
[4] From the OFKN website: "This handbook discusses the legal, social and technical aspects of open data. It can be used by anyone but is especially designed for those seeking to open up data. It discusses the why, what and how of open data – why to go open, what open is, and the how to 'open' data". The full version of the handbook can be downloaded at: http://opendatahandbook.org/guide/en/.
[5] Open Government Data website http://opengovernmentdata.org/
[6] Recital (4), Dir. 2003/98/EC.
[7] Recital (2), Dir. 2013/37/EU.
[8] Open Data Handbook Documentation, Release 1.0.0 p. 4, http://opendatahandbook.org/guide/en/
[9] https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
[10] http://www.w3.org/2009/Talks/0204–ted–tbl.
[11] http://webarchive.nationalarchives.gov.uk/20130109092234/http://number10.gov.uk/news/letter–to–government–departments–on–opening–up–data/.
[12] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207772/Open_Data_Charter.pdf

the G8 Members as a pillar strategic action for supporting transparency, accountability, participation, economic growth and innovation in society.

The 12th of December 2011 the European Commission, in order to achieve the aims as indicated in the Digital Agenda for Europe and to unlock the public data potential across Europe, has launched an "Open Data Strategy for Europe", enacting the so called "Open Data Package"[13]. The Open Data Strategy consists of:

1. a Communication on Open Data where the Commission presents its vision and policy on data re–use, including legislative, deployment and funding elements;

2. a proposal to revise the 2003 Directive on re–use of public sector information (Directive 2003/98/EC)[14]. The Directive has been recently amended by the "Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re–use of public sector information"[15].

Recital (4) of the revised Directive point out the importance of adopting in EU common and harmonized open data policies encouraging "the wide availability and re–use of public sector information for private or commercial purposes". The circulation of the information "can play an important role in kick–starting the development of new services based on novel ways to combine and make use of such information, stimulate economic growth and promote social engagement".

The new Directive in recital (6) recognizes that some of the MS's "have been adopting ambitious open data approaches to make re–use of accessible public data easier for citizens and companies". As a result, in the same Recital the need of "a minimum harmonisation to prevent different rules in different Member States acting as a barrier to the cross– border offer of products and services, and to enable comparable public data sets to be re–usable for pan–European applications based on them is stated. A minimum harmonisation is also required to determine what public data are available for re–use in the internal information market, consistent with the relevant access regime".

This paper is based on an interdisciplinary approach taking into consideration legal, economical, technological and semantic web aspects of OGD. The legal aspects of the survey consider transparency, accountability, data protection and licences. The economical value of OGD examines the issues related with charging of PSI and the need for developing sustainable

[13] http://ec.europa.eu/digital–agenda/en/open–data–0
[14] http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf
[15] The official version of the Directive is available at this link:
http://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX:32013L0037.

Business Models for OGD. Finally, the paper highlights the noteworthy technological aspects related with the opening of OGD datasets in the Semantic Web like formats, metadata, linked open data and interoperability.

The following analysis is mainly based on the content and perspective of the above–mentioned PSI re–uses Directive.

2. Transparency, Right of Access to Information and Accountability

The Principle of Transparency has a constitutional basis and provides the fundamental legal framework for the administrative action and policy. The Transparency Principle ensures all the citizens the freedom of information and the right to consult or obtain information and data maintained by the Public Sector Bodies. So far, Transparency has been granted under the national freedom of information regulations accordingly to the Principle of Access to the administrative acts and the Principles of Publicity of the acts[16]. Openness and availability of Public Sector Information are therefore ensured to citizens on the basis of the Right of Access.

The first 'freedom of information activists' were the enlightenment thinkers in Sweden and Finland who successfully promoted the adoption of Sweden's 1766 Freedom of the Press Act which establishes the principle of the openness of official documents and is widely considered to be the world's first access to information law. The right to access and use information were intrinsic to freedom of the press according to this constitutional law, which established a freedom to print in whole or in part extracts from *"correspondence, documents, protocols, judgments and awards* [produced by] *courts and government departments, our senior administrators and consistories or other public bodies ... which, when requested, shall immediately be issued to anyone who applies for them on penalty of the provisions following paragraph"*. Documents should be provided "immediately" and the penalty foreseen is loss of office for the public official who fails to provide the documents or in any way obstructs their release[17].

[16] Article 1, as to the Consolidated version of the Treaty on European Union and the Treaty on the Functioning of the European Union. http://eur–lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:EN:HTML.
Italy: Law 241/90 on Administrative Procedure and Access to Administrative Documents: http://www.ictparliament.org/node/2040.
Finland: Act on Openness of Government Activities: ec.europa.eu/information_society/policy/psi/docs/pdfs/implementation/fi_trans_19990621.pdf.

[17] "The World's First Freedom of Information Act", published by the Chydenius Foundation (2006) available at: http://www.chydenius.net/pdf/worlds_first_foia.pdf.

Finland was part of Sweden when the first Act on the Freedom of Publishing and the Right of Access to Official Documents was enacted in 1766. Finland, as an Independent Republic, adopted the Act on Access to Information Law in 1951.

The right of access to information has developed significantly in recent years, with at least eighty countries worldwide currently having a dedicated legal framework for requesting and receiving information[18]. The right is also enshrined in at least fifty national constitutions.

In the OGD environment Transparency and at the same time Accountability of Governments and Public Entities are fundamental issues. Following this, Barack Obama in the speech he delivered when he was elected president of the United States for the first time opened the way to a new process in the field of democracy in the digital era. In the Memorandum for the Heads of Executive Departments and Agencies on the 21 January 2009, President Obama declared: "My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government"[19]. In his Memorandum the President instructed the Director of the Office of Management and Budget to issue an Open Government Directive. The Directive was enacted on the 8 December 2009[20].

The three principles of transparency, participation, and collaboration form the cornerstone of an Open Government policy. From the Obama declaration we can read: *"Transparency promotes accountability and provides information for citizens about what their Government is doing. Information maintained by the Federal Government is a national asset. My Administration will take appropriate action, consistent with law and policy, to disclose information rapidly in forms that the public can readily find and use. Executive departments and agencies should harness new technologies to put information about their operations and decisions online and readily available to the public. Executive departments and agencies should also solicit public feedback to identify information of greatest use to the public"*.

Next, the EU Commission in 2011 with the Explanatory Memorandum of the Open Data Package invites the "European Parliament and the Council, within their respective responsibilities, to create the right framework conditions for the re–use of public sector

[18] Some examples: Italy: Law 241/90 on Administrative Procedure and Access to Administrative Documents: http://www.ictparliament.org/node/2040. Finland: Act on Openness of Government Activities: ec.europa.eu/information_society/policy/psi/docs/pdfs/implementation/fi_trans_19990621.pdf.
[19] Memorandum for the Heads of Executive Departments and Agencies, SUBJECT: Transparency and Open Government, http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
[20] http://www.whitehouse.gov/open/documents/open–government–directive.

information across the European Union, and to support the projects and infrastructures that can turn Europe's public data into a motor for innovation, growth and transparency". In particular as to the Memorandum "this will strengthen positive effect on the transparency, efficiency and accountability of governments and contribute to citizen empowerment"[21].

Subsequently in 2013, the G8 Open Data Charter Communication declared: "Open data can increase transparency about what government and business are doing. Open data also increase awareness about how countries' natural resources are used, how extractives revenues are spent, and how land is transacted and managed. All of which promotes accountability and good governance, enhances public debate, and helps to fight corruption. Transparent data on G8 development assistance are also essential for accountability"[22].

3. Open Government Data and Personal Data Legislation

Data Protection and the re–use of Public Sector Information in the European Union is a growing concern after the Commission has adopted the above–mentioned Open Data Package and the PSI Directive has been revised. Therefore, we should mention the proposal for a new Regulation on Personal Data Protection that Personal Data Protection that the EU is close to adopting.

In respect of processing personal data recital 11 of the revised Directive states: "the Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC". Therefore, the Member States should determine the conditions under which the processing of personal data is lawful. Furthermore, the recital highlights the Data Protection Directive principle which states that "personal data must not be processed further to collection in a way incompatible with the specified, explicit and legitimate purposes for which those data were collected".

It seems that the Directive has only partially taken into consideration the opinion issued by the European Data Protection Supervisor (EDPS) calling for data protection safeguards before public sector information containing personal data can be re–used[23]. The opinion of EDPS provides a detailed analysis covering many important aspects ranging from licensing,

[21] Proposal for a Directive of the European Parliament and of the Council Amending Directive 2003/98/EC on re–use of public sector information, http://ec.europa.eu/information_society/policy/psi/docs/pdfs/opendata2012/revision_of_PSI_Directive/proposal_directive_EN.pdf.

[22] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207772/Open_Data_Charter.pdf

[23] Opinion of the European Data Protection Supervisor on the "Open Data Package", http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12–04–18_Open_data_EN.pdf.

anonymization and transfer of data outside of the EU. Peter Hustinx, the EDPS, says: "The re–use of PSI containing personal data may bring significant benefits, but also entails great risks to the protection of personal data, due to the wide variety of data held by public sector bodies. The Commission proposal should therefore more clearly define in what situations and subject to what safeguards information containing personal data may be required to be made available for re–use."[24] In the opinion of EDPS, Open Data policies and Data Protection laws have similar objective: to create a fair environment for the circulation and the processing of data, but from PSI perspective, no personal data should enter in the open government data definition. This creates some weakness in the coordination between the two topics.

The EDPS calls for a proactive approach. As to the opinion of EDPS, "it is crucial that public sector bodies take a proactive approach when making personal data available for reuse. A proactive approach would make it possible to make the data publicly available with the explicit purpose of reuse, subject to specific conditions and safeguards in compliance with data protection rules".

To ensure data protection compliance, EDPS recommends that the Commission develop further guidance on the data protection aspects of PSI re–use, primarily taking into account anonymization and licensing. The EDPS suggests the implementation of a template for adequate data protection clauses in licenses.

Finally, EDPS recommends that the EC Proposal of amending PSI Directive should:

– establish the scope of applicability of the PSI Directive to personal data more clearly;

– require that an assessment be carried out by the public sector body concerned before any PSI containing personal data may be made available for reuse;

– where appropriate, require that data be fully or partially anonymized and license conditions specifically prohibit re–identification of individuals and the reuse of personal data for purposes that may individually affect the data subjects;

– require that the terms of the licence to reuse PSI include a data protection clause, whenever personal data are processed;

– where necessary consider the risks to the protection of personal data, require applicants to demonstrate (via a data protection impact assessment or otherwise) that any risks to the

[24] PRESS RELEASE EDPS/08/12, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS–2012–08_Open_Data_EN.pdf.

protection of personal data are adequately addressed and that the applicant will process data in compliance with applicable data protection law[25];

– clarify that reuse can be made contingent upon the purpose for which reuse is made, in derogation from the general rule allowing reuse for any commercial and non–commercial purposes;

In addition, the EDPS suggests that the Directive should:

– consider allowing costs of pre–processing (such as digitalization), anonymization and aggregation to be charged to license–holders where appropriate, and

– that the Commission develops further guidance, focusing on anonymization and licensing and consult the WP29[26] in this regard.

Concerning the anonymisation of OGD the WP29 has recently adopted the Opinion 05/2014 on Anonymisation Techniques (10 April 2014). In its opinion, the WP 29 "acknowledges the potential value of anonymisation in particular as a strategy to reap the benefits of 'open data' for individuals and society at large whilst mitigating the risks for the individuals concerned"[27].

The revised Directive has not ruled on this specific issue of protection of personal data leaving the decision to the MS's and generically referring to the Data Protection Directive into force.

In regards to *de lege ferenda,* the data protection reform package is aimed at building a single and comprehensive set of data protection rules for the EU. The issue of Open Data has no specific provision in the Regulation proposal[28]. Nevertheless, in the proposal we can find provisions on central thematic like privacy by design, privacy by default and the right to be forgotten that will have a significant impact to OGD (and also Big Data) policies and legislation.

Regarding the right to be forgotten, the recent decision of the European Court of Justice in the case–law Google v. Costeja[29] clearly states the existence of the right of a person to see

[25] In this respect see: EVPSI & LAPSI Final Meeting Turin, 9–10/7/2012 Eleonora Bassi University of Turin. In this work are indicated the recommended tools in order to fulfil the EDPS purposes such as: PETs, Privacy by Design, Anonymisation, Privacy Policies, PIA, Codes of Conduct, Guidelines, Anonymisation by Default. www.lapsi–project.eu.

[26] WP29 recommend to adopt a case by case approach "in order to strike the balance between the right to privacy and the right to public access" (Opinion 7/2003, wp 83). WP29 (Working Party 29) was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf

[27] The Opinion on Anonymisation Techniques adopted by WP29 is available at: http://ec.europa.eu/justice/data–protection/article–29/documentation/opinion–recommendation/files/2014/wp216_en.pdf

[28] http://eur–lex.europa.eu/legal–content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

[29] http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

personal data correctly represented according to the veracity of the facts and the context. Concerning OGD, this concept means that opening datasets containing personal data requires that the Public Administrations constantly update the dataset according to the current circumstances. This task requires a good deal of the Public Sector resources. The request to erase or alter information is managed by each MS differently: the data may be deleted at the source, i.e. from storage, or the data may be removed from the indexing in the search engine. The Open data paradigm requires any search engine be open and that the information is indexed to permit wide sharing of information on the Semantic Web. Therefore, the right to be forgotten raises this new, and critical, issue in light of our understanding of the broad and widely distributed information in the Open Data environment.

4. Government Data and Licences

The legal conditions under which PSI are made available is considered by the revised Directive at Recital 26 "In relation to any re–use that is made of the document, public sector bodies may impose conditions, where appropriate through a licence, such as acknowledgment of source and acknowledgment of whether the document has been modified by the re–user in any way". The revised Article 8 of the Directive leaves the public sector open to "allow re–use without conditions". Therefore, public sector bodies, as to Recital 26 and Article 8 of the Directive, may impose "where appropriate" conditions for the re–use of PSI "through a licence" placing "as few restrictions on re–use as possible". Accordingly, some Member States have established their own Open Data Licence for PSI re–use like, the UK[30], Italy[31] and in Finland the National Land Survey[32]. The EU has itself adopted the European Union Public Licence (EUPL)[33]. Some Countries has adopted the ODL (open database license)[34] published by the Open Data Common. This licence agreement imposes the limitation of *share–a–like* causing sometime a barrier to the economic re–use of the datasets.

Furthermore, the revised Directive at Recital 26 encourages Member States to use open licences available online "relying on open data format" "(…) which grant wider re–use rights without technological, financial or geographical limitations". This "should eventually become common practice across the Union".

[30] http://www.nationalarchives.gov.uk/doc/open–government–licence/version/2/.
[31] http://www.formez.it/iodl/.
[32] http://www.maanmittauslaitos.fi/en/NLS_open_data_licence_version1_20120501.
[33] https://joinup.ec.europa.eu/software/page/eupl/licence–eupl.
[34] http://opendatacommons.org/licenses/odbl/

The Creative Commons Licences CC–BY 4.0 and CC–BY–SA 4.0 are a practical option for publishing both data and content. The release 4.0 package of CC includes the *sui generis* right that is the best way to protect dataset according with the European Directive 2004/48/EC and related Statement 2005/295/EC and Directive 96/9/EC. The OFKN has marked, *inter alia*, CC–BY 4.0 and CC–BY–SA 4.0 as conformant[35] with the principles set forth in the Open Definition[36] In between numerous examples of publication under the Creative Commons Attribution 4.0, we can mention as an example the Finnish Meteorological Institute's open data service[37]. The issue of licences is more essential after the revision has extended the scope of Directive 2003/98/EC "to libraries, including university libraries, museums and archives" as to Recital 14 of the Directive 2013/37/EU.

Within this framework, we should mention as an example Europeana[38] (Europe's digital library) that releases its metadata into the public domain using CC0. However, this decision of Europeana to impose to every contributor the CC0 is disputable. The CC0 is a waive license, and it is contrary to the moral right that is inalienable in Europe. Moreover, an open government dataset is inalienable proprietary of the public administration (like beaches, soil, etc.) and the statement included in the paragraph 2 of the universal CC0 "To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights" is not applicable by any employee of the public administration. This is a great dilemma especially for the cultural heritage material that is proprietary of the patrimony of a national State. Secondarily, these considerations uncover a further problem: how to conciliate so large a variety of licenses in case the market needs to mash–up dataset for producing commercial product, service and application. This topic is unresolved and it is one of the most important legal barriers to the success of a real business model of the open government data[39].

5. Economical value and business models for Open Government Data

The Communication of 2011 of the European Commission to the European Parliament "Open data an engine for innovation, growth and transparent governance" has an emblematic

[35] http://opendefinition.org/licenses/.
[36] Read more about the Open Definition at: http://opendefinition.org/od/.
[37] http://en.ilmatieteenlaitos.fi/open–data–licence.
[38] http://www.europeana.eu/portal/.
[39] M. Palmirani, M. Mockus, *Open Government Data Licensing Framework* [in:] *Electronic Government and the Information Systems Perspective,* A. Kő, E. Francesconi (eds.) Fourth International Conference, EGOVIS 2014, Valencia, Spain, September 1–4, 2015, Proceedings, Springer, 2015.

and challenging heading: "Turning public data to business opportunities: new services and economic growth"[40].

As referred to above, the PSI is the single largest source of information in Europe. The Open Data Package included evidence in a careful and detailed survey in order to show the economic opportunities arising from the exploitation of Government Data.

The European Commission believes that "overall economic gains from opening up this resource could amount to € 40 billion a year in the EU. Opening up public data will also foster the participation of citizens in political and social life and contribute to policy areas such as the environment".[41] This information has a significant – currently untapped – potential for re–use in new products and services and for efficiency gains in administrations.

A recent study carried on by Graham Vickery[42] and commissioned by the EC estimates the total public sector information related market across the EU in the year 2008 at Euro 28 billion and in 2010 at 32 billion Euro. The study indicates that the overall economic gains from further opening up public sector information by allowing easy access are at around 40 billion Euro a year for the EU27. The aggregate direct and indirect economic impacts from PSI applications and use across the whole EU27 economy would be in the order of Euro 140 billion annually. As to the Vickery study, the average growth rate in PSI–related markets is 7%. The total direct and indirect economic impact of PSI reuse is from 70 up to 140 billion of Euro. Finally, the welfare gains from to marginal cost pricing of the PSI will be 40 billion Euro.

Hal Varian, Professor of Information Sciences, Business, and Economics at the University of California at Berkeley and Chief Economist, Google maintains that "the ability to take data – to be able to understand it, to process it, to extract value from it, to visualize it, to communicate it – that's going to be a hugely important skill in the next decades, not only at the professional level but even at the educational level for elementary school kids, for high school kids, for college kids. Because now we really do have essentially free and ubiquitous data. So the complimentary scarce factor is the ability to understand that data and extract value from it."[43]

The main issue arising from the revision of the Directive and affecting the economic value of datasets is the principles governing charging regulated in Article 6. The Directive in Article

[40] http://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX:52011DC0882.
[41] Communication on Open Data,
http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/open_data.pdf.
[42] Search on the web: Review of recent studies on PSI re–use and related market developments, G. Vickery, August 2011.
[43] Hal Varian on how the Web challenges managers
http://www.mckinsey.com/client_service/business_technology

6.1 lays down a charge, applying to all, for public sector data re–use in the EU, except the situations specified in Article 6.2: "public sector bodies may charge no more than the marginal cost of reproducing, providing and disseminating the documents". Nevertheless, article 6.2 of the Directive expressed the possibility "to sell" open government data reflecting "marginal costs incurred for their reproduction, provision and dissemination" along with "a reasonable return on investment".

The policy of lowering charges has been supported by researches and by the outcome of public consultations conducted by the Commission[44]. A series of case studies on public sector bodies that moved from full cost recovery to a marginal costs system show that the move not only increased re–use, but also benefited the public sector bodies concerned[45].

Heli Koski[46] from the Research Institute of the Finnish Economy has recently carried on a study about marginal cost pricing of PSI[47]. Assessing the performance of 14,000 firms in the architectural, engineering and related technical consultancy sectors, located in 15 different countries, the study analyses the effect of maximum marginal cost pricing for geographical PSI on the firms' growth performance during the years 2000–2007. The conclusions that Koski has reached are strongly supporting free data re–use.

This "reasonable return on investment" provision in the PSI Directive opens up an unexpected scenario for a business model based on the free circulation of knowledge not reflecting the OGD concept of datasets available free of charge[48].

However, the scientific research on business model (BM) of OGD is still scarce[49]. Therefore, the network economy is still facing a lack of studies that analyse and describe a suitable BM archetype for OGD.

---

[44]Commission staff working document SEC(2011) 1552 final; https://ec.europa.eu/digital–agenda/en/news/commission–notice–guidelines–recommended–standard–licences–datasets–and–charging–re–use.

[45] Study on 'Pricing of Public Sector Information', Deloitte consulting and others, June 2011.

[46] Does Marginal Cost Pricing of Public Sector Information Spur Firm Growth?', Heli Koski, The Research Institute of the Finnish Economy. http://www.etla.fi/files/2696_no_1260.pdf.

[47] About Principles governing charging see further on paragraph 3.2

[48] Monica Palmirani, Michele Martoni, Dino Girardi – Open Government Data Beyond Transparency in: Andrea K˝o Enrico Francesconi (Eds.) Electronic Government and the Information Systems Perspective Third International Conference, EGOVIS 2014 Munich, Germany, September 1–3, 2014 – Proceedings.

[49] Eight Business Model Archetypes for PSI Re–Use by Osella – Ferro,www.w3.org/2013/04/odw/odw13_submission_27.pdf; Open growth Stimulating demand for open data in the UK – by Deloitte's and The Open Data Institute, http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/deloitte–analytics/open–growth.pdf; Open data business models, by Jeni Tennison, www.theodi.org; D. Girardi, M. Palmirani, *Legal Issues and Economic Exploitation of Open Government Data*, "Jusletter IT" 15. Mai 2013; C. Bonina, New business models and the value of open data: definitions, challenges and opportunities, http://www.nemode.ac.uk/wp–content/uploads/2013/11/Bonina–Opendata–Report–FINAL.pdf; Magalhaes, Roseira, Manley, *Business models for open government data*, opendata500.thegovlab.org/files/Business_Models_for_OGD.pdf.

In our opinion, an appropriate and applicable BM archetype for Open Data should distinguish two different models: one for Enterprises and NPO's and one designed for Public Sector Bodies. Considering a BM archetype for Enterprises it basically requires to describe differences and peculiarities between those using OGD as core business and those using OGD as a complementary business. Nevertheless, in our opinion it is of fundamental importance to develop a sustainable BM tailored for Public Sector Bodies.

Thinking from a research point of view, the analysis for developing a sustainable Business Model archetype for OGD should consider for instance solutions regarding: the analysis of the possible re–use and exploitation of available datasets on a large scale not only for political purposes (transparency and accountability); the implementation of back up option in case of a luck of delivering of data; the analysis of the quality of data (i.e. punctual, timely, complete, statistics); the accessibility for the end consumer; personal data and copyright issues; the consistency with the original purposes that have enabled the opening of the datasets; the benefits and the value creation for the Public Sector Bodies and the whole society.

The BM should primarily consider the following budgeting components:

– the expenditures related with the operational costs for collection, production, digitalization, manipulation, processing, storage, and dissemination of the datasets;

– consequently, the budgeting components associated with the expected revenue streams for the Public Sector Bodies like charges and tax revenue;

– additionally, the so–called indirect benefits and the social benefits arising for the exploitation of OGD, whenever they can be monetized.

Finally, the BM should describe two archetypes designed for public sector bodies that are required to "charge PSI at marginal cost" and one for those who are "required to generate revenue". In respect of the latter model, we should recall Article 6 "principles governing charging, that at point 2 reads: "paragraph 1 shall not apply to the following:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) by way of exception, documents for which the public sector body concerned is required to generate sufficient revenue to cover a substantial part of the costs relating to their collection, production, reproduction and dissemination. Those requirements shall be defined by law or by other binding rules in the Member State. In the absence of such rules, the requirements shall be defined in accordance with common administrative practice in the Member State;

(c) libraries, including university libraries, museums and archives. Finally, "Where charges are made by the public sector bodies referred to in point (c) of paragraph 2, the total

income from supplying and allowing re–use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, preservation and rights clearance, together with a reasonable return on investment".

6. Technological issue for Open Government Data in the semantic web

Finally, from the previous paragraphs we have understood that Open Government Data is a global phenomenon adopted at political level by numerous public administrations. Therefore, the EU Commission have encompassed this crucial topic in the Digital Agenda as one of the main pillars in order to develop a Digital Single Market[50]. OGD implies a new cultural approach for implementing transparency, sharing of knowledge, participation and cooperation. OGD are also the essential instrument for supporting and developing a digital economy and for improving the quality of the life of the citizens. It is also a great instrument for fighting corruption, criminality, and bad administrative practices inside of the public administration. OGD also requires managerial competences and engineering skills in order to produce a culture of quality of data since the original digital information system inside the public administration requires reengineering.

Nevertheless, is indubitable that without technology principles OGD is only a manifesto. Therefore, we should comment on the need of technological methodologies, which enable the opening, and dissemination of reusable public datasets to ensure their interoperability in the Semantic Web. As in the Open Data Handbook,[51] "interoperability denotes the ability of diverse systems and organizations to work together (inter–operate), to cooperate, to exchange information automatically, to interact seamlessly anywhere, anytime on the base of common rules". In the case of Open Data, interoperability is the ability to interoperate – or intermix – different datasets. "The core of a "commons" of data (or code) is that one piece of "open" material contained therein can be freely intermixed with other "open" material. This interoperability is key to realizing the main practical benefits of "openness": the dramatically enhanced ability to combine different datasets together and thereby to develop more and better products and services. Providing a clear definition of openness ensures that when you get two open datasets from two different sources, you will be able to combine them together, and it ensures that we avoid our own 'tower of babel': lots of datasets but little or no ability to combine them together into the larger systems where the real value lies."[52]

[50] http://ec.europa.eu/digital–agenda/en/our–goals/pillar–i–digital–single–market.
[51] http://opendatahandbook.org/.
[52] http://opendatahandbook.org/guide/en/what–is–open–data/.

Recital (20) of the revised Directive reads: "To facilitate re–use, public sector bodies should, where possible and appropriate, make documents available through open and machine–readable formats and together with their metadata, at the best level of precision and granularity, in a format that ensures interoperability". As to Article 2.6 of the PSI Directive a format is 'machine–readable' when the "file format is structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure". Additionally, Article 2.7 defines 'open format' as a "file format that is platform–independent and made available to the public without any restriction that impedes the re–use of documents".

In the light of the legal provisions from a technical perspective, there are four main principles to consider:

i) Open format;

ii) Metadata;

iii) Ontology;

iv) Persistent URI.

Open format. Besides the legal definition in computer science, open format also means well documented, easily applicable, no proprietary and neutral respect the technology environment. Examples of open formats are: CSV, JSON, XML, RDF[53].

Metadata. The dataset itself is not enough for implementing the reusability. It is also necessary to explain the semantic of the data. For this reason, two more elements are necessary: metadata and ontology. Metadata is machine understandable information on the dataset, understandable in the Semantic Web platform[54]. Metadata are classified according to standard vocabularies to facilitate searching and interoperability. Without metadata, the dataset is only a list of values without meaning and contextualization. Article 2.8 and Article 6 of the Directive clarify that "both the format and the metadata should, in so far as possible, comply with formal open standards", "…which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability". So, it is important to have them jointly with the dataset for supporting a correct re–use according to the intention of the author. Without precise metadata, the re–use can produce corrupted results and the datasets are prone to the manipulation, mystification and wrong interpretation. One of the most important methodologies for providing metadata is RDF (Resource Description Framework) that permits to make assertion on the main source using triple method: subject (dataset), predicate

[53] For an exhaustive analysis about open format see: http://opendefinition.org/ofd/.
[54] http://www.w3.org/Metadata/.

(relationship), object (attribute). One typical assertion is to define creator, date of creation, subject of the dataset. An example is the following that states Palmirani is the creator of the dataset1 using Dublin Core[55] vocabulary:

```
<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22–rdf–syntax–ns#"
  xmlns:dc="http://purl.org/dc/elements/1.1/">
   <rdf:Description rdf:about="http://example.org/dataset1">
   <dc:title>dataset1 OGD</dc:title>
   <dc:creator>Monica Palmirani</dc:creator>
</rdf:RDF>
```

Ontology. As paradigmatic example of ontology, we can refer to DCAT[56] that "is an RDF vocabulary" developed by W3C "designed to facilitate interoperability between data catalogues published on the Web". EUROVOC[57] is a multilingual, multidisciplinary thesaurus covering the activities of the EU, the European Parliament in particular. Besides the datasets, sometimes it is fundamental to annotate also the schema, the vocabulary and taxonomies. ADMS[58] is a specific application of DCAT, used to describe *semantic assets* defined as highly reusable metadata (e.g. xml schemata, generic data models) and reference data (e.g., code lists, taxonomies, dictionaries, vocabularies) that are used for eGovernment system development. In this way, we can describe the dataset (e.g., XML), the metadata of the dataset (e.g., DCAT) and finally also the vocabulary or schema for interpreting the dataset (e.g., with ADMS).

Computational Ontology. Computational ontology is the abstract representation a specific domain using classes, attributes, relationships[59]. A computational ontology sets up a semantic modelization of the reality that, if it is shared among a community, can create a common meaningful map of concepts. Using axioms, it is possible to create inferential rules among the objects connected with the classes of the ontology. In order to exemplify the concept: "if the dataset is created by Palmirani and if Palmirani belongs to the University of Bologna, then the dataset is published by University of Bologna".

Persistent URI. The possibility to have persistent, meaningful, semantic URI, http based for each different web resource is a fundamental principle in order to make valid the RDF and

[55] http://dublincore.org/ Dublin Core is one important vocabulary for assigning metadata to the sources in the Web.
[56] http://www.w3.org/TR/vocab–dcat/.
[57] http://eurovoc.europa.eu/.
[58] http://www.w3.org/TR/vocab–adms/.
[59] http://tomgruber.org/writing/ontology–definition–2007.htm

the ontology statements. Using these ingredients, it is possible to create an interoperable infrastructure capable to be connected with the Semantic Web constellation of data. Tim Berners–Lee[60] defines the Semantic Web as "a web of data that can be processed directly and indirectly by machines"[61]. "The Semantic Web is a Web of Data — of dates and titles and part numbers and chemical properties and any other data one might conceive of. The Semantic Web stack[62] (URI, XML, RDF, OWL, Logic, Proof, Trust) provides a complete environment where the data are reference–able, modelled, enriched, inferenced and detected with provenance metadata. Additionally, Linked Open Data[63] methodology provides the best way to publishing the datasets in Semantic Web context. Linked Open Data publication requires four rules:

1. Provide a persistent URI for each dataset;
2. URI http based;
3. Use RDF metadata connected to the dataset;
4. Re–use other ontologies.

Linked Open Data is a best practice worldwide accepted about open data; however, it is not easy to implement it, so it is possible to apply this paradigm step by steps following, gradually, the method of the Tim Berners Lee's 5 stars[64]:

1. Provide dataset on the web with open license;
2. Provide dataset in machine–readable open format;
3. The open format should be non–proprietary;
4. Link the data to RDF metadata;
5. Link the data to other data available in the Linked Open Cloud[65].

Linked Open Data attempt to resolve the interoperability dilemma of the Web of Data. However, it is difficult to share the same understanding of a concept equally worldwide. The perception of the realty is different by each person, so we should add a level of provenance to the interpretation. As an example, the legal dataset is fundamental to permit multiple annotations of the same dataset with different licenses and different metadata datasets. In this scenario, the risk is to have too much dataset without the corresponding metadata and semantic that is fundamental for expressing the level of integrity and authority. The inferential process generated new knowledge derived by the datasets, but the outcomes are valid only if the

[60] http://www.w3.org/People/Berners–Lee/
[61] T. Berners–Lee, J. Hendler, Ora Lassila (May 17, 2001),"The Semantic Web". *Scientific American Magazine*. Retrieved March 26, 2008.
[62] https://en.wikipedia.org/wiki/Semantic_Web_Stack.
[63] http://www.w3.org/wiki/LinkedData.
[64] http://www.w3.org/DesignIssues/LinkedData.html.
[65] http://lod–cloud.net/.

premises are well supported by the evidence of accuracy, truthfulness and authenticity. For this reason ontology like PROV–O[66], devoted to tracking the provenance of the data, is fundamental for guaranteeing the validity over time of the information and avoid manipulation of reality. Another emerging topic in this respect is the issue concerning the long–term preservation of the dataset not only as historical memory of the cultural heritage of a nation, but moreover for archiving in safe and secure way the dataset produced by the public administration.

7. Conclusions

In the light of the current European Union panorama, so far, OGD policies have mainly met a political and social function in respect of transparency and accountability of Governments and public entities. The commercial value of OGD is so far evident in countries and regions that have adopted ambitious and strategic projects for the exploitation of OGD at any level (i.e. UK, Italy, Austria, Germany, Finland, Estonia). On the other hand, in part of the MSs Open Government Data, policies are still in early infancy.

The current EU scenario is like an archipelago with a lack of bridges connecting OGD policies and strategies in different Member States. The revised Directive on PSI re–use has established a minimum harmonisation to prevent different rules in different Member States acting as a barrier to the cross– border offer of products and services, and to enable comparable public data sets to be re–usable for pan–European applications. Nevertheless, the implementation of the Directive in the MS legislation is developing slowly, and OGD policies are left to the political decision of a single Member State. As a result, there will most likely be weak harmonisation.

This paper has pointed out the need for an interdisciplinary approach in order to enable a wider exploitation of OGD for commercial and non–commercial purposes. In our opinion, Open Government Data in EU should be considered as a harmonized, integrated and interoperable ecosystem. Citizen, users, public entities, NPO's and private enterprise should work, collaborate and especially cooperate. These various players, with their own special roles and skills, should cooperate in an interactive dialogue in order to prove and exploit the potential of Open Government Data. The availability of more OGD is not only a method for publishing data for the external end–users, it is also a great instrument for the cooperation between public sector bodies that often are not able to integrate the information systems, and to provide efficient services to citizens and enterprises. Secondarily, the paradigm of OGD is also a way for

[66] http://www.w3.org/TR/prov–o/.

enhancing the internal communication among departments of the same public sector bodies that are otherwise not consciousness of the wide repository of information available. OGD creates a new methodology of work inside and outside of the public administration and produces an innovative flow of data supporting the digital economy and enhances cooperation between the private and public sector preparing the next step of the Internet of the Thing[67]. This reinforces the concept that OGD is beyond the notion of transparency and accountability and would be one part of a real modern democracy in the network society[68].

[67] The Internet of Things—A survey of topics and trends, Andrew Whitmore, Anurag Agarwal, Li Da Xu, Springer, 2014.
[68] M. Palmirani, M. Martoni, D. Girardi, *Open Government Data Beyond Transparency* [in:] *Electronic Government and the Information Systems Perspective,* A. K˝o, E. Francesconi (eds.), Third International Conference, EGOVIS 2014 Munich, Germany, September 1–3, 2014 – Proceedings.

LESS PRIVACY, MORE SECURITY?
NETWORK SOCIETY IN THE TIMES OF PRISM

Part of dissertation: Abuses of Dominant ICT Companies in the Area of Data Protection

Aleksander Wiatrowski

Researcher, University of Lapland, Institute for Law and Informatics, awiatrow@ulapland.fi

Keywords: ***Mass surveillance, privacy, security, dominant companies, network society, data protection, PRISM, Deep Web***

Abstract*: Today we live in Network Society, the concept that replaced Information Society. University of Lapland Institute for Law and Informatics focuses on researching the complexity and scope of this new Network Society. In order to do that The NETSO Project was established – Network Society as a Paradigm for Legal and Societal Thinking. The NETSO project aims to generate basic knowledge of the theoretical foundations and context of the network society development and to discover the subsequent changes in the legal, communicational and societal aspects of the process.*

Nowadays, during the discussion triggered by the situation that very well might be called "mass surveillance crisis" we are in the need of asking, what society thinks about it and do society wants to do anything about it. Now, as never before, we know we are being spied and that dominant ICT companies are having significant role in it. How Network Society, society trapped in the network, can react to this? How can law react and is it prepared? Or maybe these are just questions without answers?

In this article I would like not only to present some facts concerning network society in the times of mass surveillance and challenges to privacy but also issues very much connected to these, such as the role of dominant ICT companies, or even growing importance of Deep Web, with Dark Web in particular.

1. Introduction

Benjamin Franklin for the Pennsylvania Assembly in its Reply to the Governor (11 Nov. 1755) wrote that *They who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety*. This quote over two centuries has been paraphrased in many different ways. Finally, in 21st century it is the best known as *any society that would give up a little liberty to gain a little security will deserve neither and lose both*. Significance of this paraphrased quote rises shortly after president's Barack Obama statement to reporters on The Patient Protection and Affordable Care Act (PPACA)[1] on June 7, 2013. While delivering several minutes of unscripted remarks about the NSA, Barack Obama said *I think*

[1] http://www.gpo.gov/fdsys/pkg/PLAW–111publ148/html/PLAW–111publ148.htm (access September 2015)

it's important to recognize that you can't have 100 per cent security and also then have 100 per cent privacy and zero inconvenience.

In the recent events, in the time when knowledge about mass surveillance is better than ever, questions about the position of society and state of our privacy have to be raised once again. Today, thanks to Edward Snowden we know, at least to some extent, the scope and complexity of mass surveillance: governments spying on citizens, other governments, using data collected by dominant ICT companies, such as Microsoft, Apple, Google or Facebook. Does all this make us feel more secure? Do we feel that our privacy is violated? Do we even have the privacy while being the part of Network Society, society addicted to technology on all levels?

Considering all these questions, I feel like there must be a place to look for positive aspects of this situation. Could it be possible that getting to know we are losing our privacy will help us reclaim some of it? Knowing about the recklessness in sharing private data in social media, gives us one grim answer. However, the significance and scope of mass surveillance may give different, more positive one.

Some of the questions can be answered only after putting the society known as Network Society in the context, in the new, mass surveillance situation. One thing is to know the definition, the other is to tell the story of society that has no choice as to react or "go with the flow". There is no possibility of ignoring the situation, or just saying that we are not interested. Being a part of network society, means, in my opinion, being trapped in the network, with no exit.

Following that is the state of privacy nowadays. In this part, I would like to give general definitions of this concept and present ways of losing it. In the part about legal framework, I need to present some information about existing solutions in EU and USA concerning data protection, which leads to privacy protection – personal data protection is part of the right to privacy. I write only about EU and US, as I am focusing on PRISM and other mass surveillance programs being a recognized problem in these two areas. Although PRISM is not the only mass surveillance program (there are at least 33 known programs), I will focus on describing only some of them, especially those that are similar to PRISM.

As this paper is part of my dissertation Abuses of Dominant ICT Companies in the Area of Data Protection, there is also place to discuss significant role of non–other than dominant ICT companies. According to what has been already revealed the role is indeed significant and puts the whole issue of these companies' abuses in the area of data protection in completely new light.

Finally, I would like to describe some consequences of the situation. There is already happening quite a lot ever since mass surveillance programs became a popular topic. In my opinion, some of it may be considered as very positive results, worth giving second thought. On the other hand, increasing surveillance and attempts to control Internet and its users have already an impact on the web. Deep Web, and its "invisible" part Dark Web is becoming more and more popular creating new challenges – challenges having an impact both on privacy as well as on growing efficiency of surveillance.

2. Our privacy

Writing about privacy is always a challenge. At this point of the discussion, probably everything was already taken under consideration and said. Yet, there is no correct answer to the question, what is the privacy. Ahti Saarenpää in his article *Openness, Access, Interoperability and Surveillance: Transparency in the New Digital Network Society* states that there is no point in having a precise legal definition of privacy.[2] The reason may be that defining privacy depends on large number of factors: social, legal, technical and historical, finally each culture has its own view of what privacy is.[3] Over time, we collected ideas and experiences from the past and present, and now we can tell long stories about how privacy could be understood. Indeed, I believe that there is no right answer to the question: *What is privacy?* For the purpose of this article and ultimately, for the purpose of my dissertation, I choose to aim in answering a different question: *How could privacy be understood?* Understood in general, by me and by Internet users, with special recognition of social media users. In this article, I would like to present only some of the ideas and conclusion having importance in the discussion about mass surveillance.

It is worth starting with the fact that privacy is a Fundamental Human Right.[4] It is recognized as such by the 1967 International Covenant on Human Rights and by Article 12 of the 1948 Universal Declaration of Human Rights:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[2] A. Saarenpää, *Openness, Access, Interoperability and Surveillance: Transparency in the New Digital Network Society* [in:] E. Schweighofer, F. Kummer, W. Hötzendorfer (ed.), *Transparency, Proceedings of the 17th International Legal Informatics Symposium IRIS 2014, Salzburg* 2014, p. 241.
[3] P. Leith, *Privacy as Slogan*, [in:] A. Saarenpää (ed.), *Legal privacy*, Zaragoza 2008, p. 99.
[4] W. Diffie, S. Landau, *Privacy on the Line. The Politics of Wiretapping and Encryption. Updated and Expanded Edition*, MIT 2007, p. 142.

The most often quoted idea on privacy seems to be the one presented by Samuel D. Warren and Louis D. Brandeis in their famous *The Right to Privacy*[5] – the right to be left alone. Following this, according to one of Oxford English Dictionary definitions privacy can be described as:

> The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.[6]

Interestingly, from the mass surveillance point of view, Oxford English Dictionary, among together six proposed definitions, gives us also this one:

> Absence or avoidance of publicity or display; secrecy, concealment, discretion; protection from public knowledge or availability.

It is also underlined that this definition is now rarely used, or as a part of the one quoted above. I decided to point out this one as one part of description of privacy in possible accordance to social media and mass surveillance.

Continuing on the thought that privacy can by understood in many ways, Ahti Saarenpää reminds us that privacy even as a concept can by understood differently in the international literature.[7] One the one hand side we have simpler definitions, mostly focusing on one aspect of the issue. Again, probably the famous *the right to be let alone* is a good example. On the other hand, Lee Bygrave decided to distinguish four general ways to understand privacy, by collecting several ideas. He states that *the privacy concept is pregnant with definitional variation. Analysis of the literature on privacy reveals four major ways of defining the concept.*[8]

- Privacy viewed essentially in terms of non–interference (Right to be left alone)
- Privacy in terms of degree of access to a person (Limited accessibility)
- Privacy in terms of information control (When, what and how information is communicated to others)
- Privacy related to aspects of persons' lives that are intimate and/or sensitive (As a result not every disclosure of information is a loss of privacy)

[5] S. D. Warren, L. D. Brandeis, *The Right to Privacy*, Harvard Law Review, 4(5), 1890, p. 193–220.
[6] http://www.oed.com/view/Entry/151596?redirectedFrom=privacy (access September 2015)
[7] A. Saarenpää, *Perspectives on Privacy*, [in:] A. Saarenpää (ed.), *Legal privacy*, Zaragoza 2008, p. 23.
[8] L. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International 2002, p. 128–129.

Knowing all that and even more, because literature on concept of privacy is so expanded that calling it unlimited would not be an exaggeration, we still have one problem. What about respecting the privacy? First of all, this article was written as an reaction to information about PRISM, therefore naturally in place it is to talk about mass surveillance as a thread to privacy. This is just one side of the coin. In today's globalized society, Network Society, Internet users very often do not respect their own privacy. Social media pages are designed to encourage us to reveal us much information as possible. *Teenagers will freely give up personal information to join social networks on the Internet*.[9] World of privacy became the place where teenagers reveal every detail about their lives online as well as a place where government agencies and marketers are collecting personal data about us. The ways to both reveal information and be the subject of collection are numerous if not unlimited. Social media pages, applications and services by Facebook or Google, mass surveillance programs such as PRISM or Tempora.[10] If that is not enough, also should be mentioned driver licenses databases, online shopping profiles, credit card companies databases, etc.

Susan Barns suggests that in the age of digital media we probably do not have any privacy.[11] What is more, today in the post 9/11 times, when government agencies should be responsible for the survival of privacy, they do quite the opposite – I again refer to mass surveillance and PRISM in particular.

I started with the question *What is privacy?* to abandon it for *How could be privacy understood?* and now I need to ask one more question. As stated above, there is probably no privacy, but is there any hope for it? In conclusion, of this article I will give some partial answers.

3. Society trapped in the Network

With the little exaggeration, we call the 21st century the age of networks.[12]

Following that words van Dijk states that networks are becoming the nervous system of our society, with having expected influence on out social live, *higher than construction of roads in the past*. Network Society, together with older concept Information Society, became a way

[9] S. B. Barnes, *A privacy paradox: Social networking in the United States*, First Monday, Volume 11, Number 9 – 4 September 2006, http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523 (access September 2015)
[10] More about PRISM and Tempora in part five: *PRISM and what stands behind it*.
[11] S. B. Barnes, *A privacy paradox*...
[12] J. Van Dijk, *The Network Society*, Sage Publications 2012, 3rd Edition, p. 2.

to define modern society, society of *high level of information exchange and use of information and communication technologies*.[13]

Van Dijk defines information society as:

> A modern type of society in which the information intensity of all activities has become so high that this creates:
>
> - an organization of society based on science, rationality and reflexivity;
> - an economy with all values and sectors even the agrarian and industrial sectors, increasingly characterized by information production;
> - a labour market with majority of functions largely or completely based on tasks of information processing requiring knowledge and higher education (hence, the alternative term *knowledge* society);
> - a culture dominated by media and information products with their signs, symbols and meanings.

The Network Society he defines as:

> A modern type of society with an infrastructure of social and media networks that characterizes its mode of organization at every level: individual, group/organizational and societal. Increasingly, these networks link every unit or part of this society (individuals, group and organizations). In western societies, the individual linked by networks is becoming the basic unit of the network society. In eastern societies, this might still be the group (family, community, work team) linked by networks.

It could be said that the Network Society is built onto the foundations of Information Society and focuses on networks and their organizational forms.

The big spokesperson for network society is without a doubt Manuel Castells. In the interview from 2001,[14] he defined Network Society as follows:

> The network society itself is, in fact, the social structure which is characteristic of what people had been calling for years the information society or post–industrial society. Both "post–industrial society" and "information society" are descriptive terms that do not provide the substance,

[13] Ibid., p. 23.
[14] Conversation with Manuel Castells, p. 4, http://globetrotter.berkeley.edu/people/Castells/castells–con4.html (access September 2015)

> that are not analytical enough. So it's not a matter of changing words; it's providing substance. And the definition, if you wish, in concrete terms of a network society is a society where the key social structures and activities are organized around electronically processed information networks. So it's not just about networks or social networks, because social networks have been very old forms of social organization. It's about social networks which process and manage information and are using micro–electronic based technologies.

Frank Webster, in his *Theories of the Information Society*, rather puts the Network Society aside. Of course, he does not ignore it the existence of the term, but also does not mention van Dijk's ideas. In the chapter dedicated to Manuel Castells work, he seems to treat Network Society as one part of Information Society, the part merely being focused on importance of networks, and not the completely new idea, let alone new or higher level of society.[15]

I mention that Network Society may be the completely new idea, or higher level of describing and interpreting the changes in modern society, as I follow Ahti Saarenpää. He is a big and consistent advocate for the idea that we should forget about Information Society – *The age of the information society is over*.[16] The time has come to tell the world that we are now living in the Network Society – *The network society has been a big step forwards from what in fact was a very static information society.*[17] One of the reasons to abandon Information Society in favor of Network Society is not the end of information, but increasing role of networks. The society is now more than ever reliant on infrastructure rather than on information.[18]

This short introduction to Network Society is now followed by my idea that our society nowadays is simply trapped in the network. Is it only Network Society or maybe Society trapped in the Network? It leads to another question: *Do you ever wonder if you use the net or the net uses you?*[19]

Without a doubt society today became dependent on technology and offered by it infrastructure. We reached the point of no return. We need it for work (ex. Driver's license

[15] F. Webster, *Theories of the Information Society*, 4th Edition, Routledge 2014, p. 106–136.
[16] A. Saarenpää, *Legal welfare and legal planning in the network society*, [in:] J. Luiz Barzallo, J. Tellez Valdes, P. Reyes Olmedo, Y. Amoroso Fernandez (ed.), *XVI Congreso Iberoamericano de Derecho e Informatica*, p. 57.
[17] Network Society as a Paradigm for Legal and Societal Thinking (NETSO), http://www.ulapland.fi/InEnglish/Units/Faculty–of–Law/Institutes/Institute–for–Law–and–Informatics/NETSO–Project (access September 2015)
[18] A. Saarenpää, *Openness, Access, Interoperability and Surveillance*…
[19] http://networksociety.org/about (access September 2015)

databases), to live (ex. Health care databases), for pleasure (ex. Facebook). Large multinational companies are pinning down consumers' preferences, lifestyle choices and general web behaviour.[20] No matter if we share the information freely, because of using social media pages, or online shopping or we share it as a legal requirement, little we give a thought to it. Very often, we do not see any issue in sharing most personal details about us, including phone number, home address, etc. in the Internet. Additionally social media pages are having tools to encourage us to reckless behaviour, for example by giving us more personalization, which leads to emotional attachment to our Internet profiles and as a consequence to share even more.[21] What we share became marketable good for companies and invaluable source for mass surveillance agencies.

4. Some words on legal framework

Before presenting legal framework dedicated to privacy and data protection, few words must be said about the big problem of legislation nowadays. This problem is recognized as overregulation. According to Wolfgang Kilian data protection is overregulated in the public field and leaves no longer a chance for self–determination of a data subject. Self–determination only matters in the private field.[22] He continues the critique of current state of data protection with following words:

> Data subjects are no longer able to maintain control on the use of their personal data effectively, for many reasons (e.g. data networks; Internet; hierarchies of users; commercial services).
>
> The current legal framework is based on the assumption that in the private field the informed consent of a data subject is structuring the collection, storage, use, and transmission of personal data. This is a fiction, since hidden primary and secondary uses of personal data are predominant. Personal data have become a marketable good.[23]

[20] D. Rowland, U. Kohl, A. Charlesworth, *Information Technology Law, Fourth Edition*, Routledge 2002, p. 4.
[21] S. B. Barnes, *A privacy paradox…*
[22] W. Kilian, Leibniz University Hannover, Germany, August 11, 2009, http://ec.europa.eu/justice/news/consulting_public/0003/contributions/citizens/kilian_wolfgang_en.pdf (access September 2015)
[23] Ibid.

We may have found ourselves nowadays in uncomfortable situation of actually overregulating data protection. This leads to slowing down regulatory efforts – the more regulations we create, the more problems appear.[24]

As written above, in *part 2: Our Privacy*, privacy is mentioned in 1967 International Covenant on Human Rights and in Article 12 of the 1948 Universal Declaration of Human Rights, but in Europe it is also acknowledged by Article 8 of the European Convention of Human Rights. Additionally, on international level, we have Treaties of Rome and Strasbourg by European Council and the Treaty on Civil Rights and Political Rights by United Nations. On national level: constitutions and national privacy laws. Recently privacy was the core topic in United Nations Privacy Resolution on November 2013 Draft Resolution: *The right to privacy in the digital age*:[25]

One of the most important documents treating on privacy is OECD and European Commission 8 principles formulated in 1980. OECD has revised in 2013 its Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.[26] Among them, I would like to point out four, which may be most significant in the protection of privacy discussion:

> *implementing privacy management programs* – essential elements discussed in this respect include privacy policies, employee training and education, provisions for sub–contracting, audit process and privacy risk assessment;
> *introducing mandatory data security breach notification* – requiring notification to the privacy enforcement authority where there is a significant security breach affecting personal data and notification to individuals where such a breach is likely to adversely affect individuals;
> *the need for privacy enforcement authorities and national privacy strategies* – the revised Guidelines recognize the need to establish authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis; they also promote the development of a coordinated approach across governmental bodies up to the highest levels; Member countries should also consider complementary measures, including education

[24] D. Rowland, U. Kohl, A. Charlesworth, *Information Technology Law…,* p. 5–6.
[25] http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf (access September 2015)
[26] OECD work on privacy, http://www.oecd.org/sti/ieconomy/privacy.htm (access September 2015)

and awareness raising, skills development and the promotion of technical measures;

improving global interoperability – to be improved through international arrangements (examples mentioned include the U.S.–EU Safe Harbor framework, the EU Binding Corporate Rules and the Council of Europe Convention 108 on the Automated Processing of Personal Data) and global cooperation among privacy enforcement authorities.

Original OECD guidelines had strong influence on Data Protection Directive. Today revised provisions could at least influence the draft EU data protection regulation's final wording on data breach notification.[27]

In 1995, European Union adopted Data Protection Directive[28] that regulates the processing of personal data within the European Union. Today we are on the verge of getting regulation that will supersede the old and in many aspects outdated directive – General Data Protection Regulation.[29] The main novelty of the Regulation is in fact the use of regulation in favor of directive. Rules on breach notification are new, but in general, Directive and Regulation cover mostly the same. According to Peter Blume, it is *due to the fact that the rules are technologically neutral*. He also points out that there is a risk of not including in the Regulation *new phenomena such as cloud computing in the better or more comprehensive way than it is made possible by the directive*.[30] Now not only we have to wait for Regulation to be enacted, but it will take many years before the next generation of data protection rules will emerge.[31] Nevertheless, occurring changes and growing attention given to privacy and its protection give a hope for positive changes in European Union.

In United States, things are more complicated. First of all, there is no legislation following OECD and European Commission principles. Secondly, there is no general privacy law including that there is nothing in U. S. Constitution. The right to privacy is also not enumerated in the Bill of Rights. However, it is protecting some specific aspects of privacy as U. S. Supreme

[27] R. Mitchell, *Revised OECD Privacy Guidelines Focus On Accountability, Notification of Breaches*, September 16, 2013, http://www.bna.com/revised–oecd–privacy–n17179877087/ (access September 2015)
[28] Directive 95/46/EC on *the protection of individuals with regard to the processing of personal data and on the free movement of such data*
[29] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on *the protection of individuals with regard to the processing of personal data and on the free movement of such data*
[30] P. Blume, *An Evolving New European Framework for Data Protection*, [in:] D. Svantesson, S. Greenstein (ed.), *Nordic Yearbook of Law and Informatics 2010–2012. Internationalisation of Law in the Digital Information Society*, Copenhagen 2013, p. 24.
[31] Ibid. p. 35.

Court has found a right to privacy through its interpretation of the First, Third, Fifth and Ninth Amendments.[32] This interpretation allows recognizing:

- privacy of believes,
- privacy of the home against demands that it be used to house soldiers,
- privacy of the person and possessions as against unreasonable searches,
- privilege against self–incrimination, which provides protection for the privacy of personal information;

The right coming from Ninth Amendment is giving protection of privacy in ways not specifically provided in the first eight amendments.[33] U. S. Constitution's protection of privacy is rather the matter of very broad interpretation. Yet, polls show most Americans support this broader approach.[34]

If these examples of how imprecise is regulation of privacy in United States were not enough to understand the issue, this is a statement by a U. S. Supreme Court on the subject of privacy:

> The makers of our Constitution understood the need to secure conditions favorable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality — the right to be left alone — the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect.

All above does not mean that the United States lacks provisions for data privacy. It is quite the opposite and it seems that American legal system also suffers from the overregulation

---

[32] J. R. Westby, Project Chair (ed.), *International Guide to Privacy. American Bar Association Privacy & Computer Crime Committee Section of Science & Technology Law*, ABA Publishing 2004, p. 11–12 [after:] *Development of the Right to Privacy in Information*, http://www.csu.edu.au/learning/ncgr/gpi/odyssey/privacy/orig_priv.html (from the U. S. Cogress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA–TCT–576, U. S. Government Printing Office, September 1993) (hereinafter *Development of the Right to Privacy in Information*).
[33] *The Right of Privacy. The Issue: Does the Constitution protect the right of privacy? If so, what aspects of privacy receive protection?,* http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (access September 2015)
[34] Ibid.

problem. According to InformationShield[35] United States Data Privacy Laws, consist of 28 acts![36]

One of the consequences of this division of laws concerning privacy is emergence of American Civil Liberties Union (ACLU). They say about themselves that *the ACLU is nation's guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country*.[37] ACLU is the most important organizations protecting privacy and fighting for civil rights in United States, established in 1920. The right to privacy understanding by ACLU is expressed as *freedom from unwarranted government intrusion into personal and private affairs.* ACLU is nowadays mostly focused on issues connected to mass surveillance:

> In the wake of 9/11, mass surveillance has become one of the U.S. government's principal strategies for protecting national security. Over the past decade, the government has asserted sweeping power to conduct dragnet collection and analysis of innocent Americans' telephone calls and e–mails, web browsing records, financial records, credit reports, and library records.

[35] http://www.informationshield.com/ (access September 2015)

[36] *United States Privacy Laws*, http://www.informationshield.com/usprivacylaws.html (access September 2015):

1. Americans with Disabilities Act (ADA)
2. Cable Communications Policy Act of 1984 (Cable Act)
3. California Senate Bill 1386 (SB 1386)
4. Children's Internet Protection Act of 2001 (CIPA)
5. Children's Online Privacy Protection Act of 1998 (COPPA)
6. Communications Assistance for Law Enforcement Act of 1994 (CALEA)
7. Computer Fraud and Abuse Act of 1986 (CFAA)
8. Computer Security Act of 1987 – (Superseded by the Federal Information Security Management Act (FISMA)
9. Consumer Credit Reporting Reform Act of 1996 (CCRRA) – Modifies the Fair Credit Reporting Act (FCRA)
10. Controlling the Assault of Non–Solicited Pornography and Marketing (CAN–SPAM) Act of 2003 law overview
11. Electronic Funds Transfer Act (EFTA)
12. Fair and Accurate Credit Transactions Act (FACTA) of 2003
13. Fair Credit Reporting Act
14. Federal Information Security Management Act (FISMA)
15. Federal Trade Commission Act (FTCA)
16. Driver's Privacy Protection Act of 1994
17. Electronic Communications Privacy Act of 1986 (ECPA)
18. Electronic Freedom of Information Act of 1996 (E–FOIA)
19. Fair Credit Reporting Act of 1999 (FCRA)
20. Family Education Rights and Privacy Act of 1974 (FERPA; also known as the Buckley Amendment)
21. Gramm–Leach–Bliley Financial Services Modernization Act of 1999 (GLBA)
22. Privacy Act of 1974 – including U.S. Department of Justice Overview
23. Privacy Protection Act of 1980 (PPA)
24. Right to Financial Privacy Act of 1978 (RFPA)
25. Telecommunications Act of 1996
26. Telephone Consumer Protection Act of 1991 (TCPA)
27. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
28. Video Privacy Protection Act of 1988 discussion and overview

[37] https://www.aclu.org/about–aclu–0 (access September 2015)

> The government has also asserted expansive authority to monitor Americans' peaceful political and religious activities.

5. Few words on PRISM (and Tempora)

PRISM (US) and Tempora (British) are both clandestine mass electronic surveillance data mining programs, both classified and secret until revealed by Edward Snowden, both are part of government sponsored mass surveillance programs. British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls and shares them with NSA according to Snowden. NSA stores massive information with examples including email, video and voice chat, videos, photos, voice–over–IP chats (such as Skype), file transfers, and social networking details. British Government Communications Headquarters (GCHQ) had probes attached to more than 200 internet links; each probe carried 10 gigabits of data a second. PRISM and Tempora both have centralized mass databanks. Data in PRISM is maintained for Archived system audit logs and backup data is stored for a minimum of two years.[38]

Even after all these information, got revealed U. S. President defended NSA and its mass surveillance program:

> When it comes to telephone calls, nobody is listening to your telephone calls. That's not what this program is about. (…)
> What the intelligence community is doing is looking at phone numbers, and durations of calls; they are not looking at people's names and they're not looking at content. (…)
> If the intelligence committee actually wants to listen to a phone call, they have to go back to a federal judge, just like they would in a criminal investigation.[39]
>
> President Obama on June 6, 2013

These words were said on June 6 2013. Only month later in July, another NSA operation was revealed, standing in contradiction to Barack Obama's statement. Xkeyscore – Formerly secret computer system used by the NSA for searching and analysing Internet data about foreign nationals across the world. The program is run jointly with other agencies including Australia's

[38] M. Rifkind, H. Porter, *Henry Porter v Malcolm Rifkind: surveillance and the free society*, http://www.theguardian.com/commentisfree/2013/aug/24/rifkind–porter–debate–miranda–surveillance (access September 2015)
[39] J. Voorhees, Obama Defends NSA Surveillance: "Nobody Is Listening to Your Telephone Calls.", June 7 2013, http://www.slate.com/blogs/the_slatest/2013/06/07/obama_defends_nsa_surveillance.html (access September 2015)

Defence Signals Directorate, and New Zealand's Government Communications Security Bureau.[40]

For a while, there was a claim that even low–level analysts are allowed to search the private emails and phone calls. The claim became a fact when The Guardian's Glenn Greenwald revealed that it is possible to *listen to whatever emails they want, whatever telephone calls, browsing histories, Microsoft Word documents. And it's all done with no need to go to a court, with no need to even get supervisor approval on the part of the analyst*.[41] If the words of a journalist are not enough then NSA summed up the program: *XKeyscore is its "widest reaching" system for developing intelligence from the Internet. The program gives analysts the ability to search through the entire database of your information without any prior authorization — no warrant, no court clearance, no signature on a dotted line. An analyst must simply complete a simple onscreen form, and seconds later, your online history is no longer private. The agency claims that XKeyscore covers "nearly everything a typical user does on the Internet."*[42]

One of the results of growing mass surveillance threat is mentioned above United Nations Privacy Resolution on November 2013 Draft Resolution:

> In response to growing concern about the scope of electronic surveillance, the U.N. General Assembly is considering a resolution affirming that privacy is a fundamental right. Civil society organizations have long urged international organizations to update and strengthen global frameworks for privacy protection. The UN resolution now under consideration is a response to reports that the United States conducted surveillance of many foreign leaders, including Brazil's President Dilma Rousseff and German Chancellor Angela Merkel. Brazil and Germany are leading the effort at the United Nations on the privacy resolution.

PRISM and Tempora are giving the extreme examples of surveillance, including spying on world leaders.[43] Sadly, those two programs are not the only. Easily even 33 mass surveillance programs and initiatives can be named.[44] Even if not all of them are aggressive and

---

[40] Active surveillance program XKEYSCORE, http://digital–era.net/active–surveillance–program–xk–eyscore/ (access September 2015)
[41] abcnews.go.com (access September 2015)
[42] *New leaks say NSA can see all your online activities*, 31 July 2013, http://net–security.org/secworld.php?id=15328 (access September 2015)
[43] J. Ball, *NSA monitored calls of 35 world leaders after US official handed over contacts*, 25 October 2013, http://www.theguardian.com/world/2013/oct/24/nsa–surveillance–world–leaders–calls (access September 2015)
[44] List of government mass surveillance projects, http://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects (access September 2015)

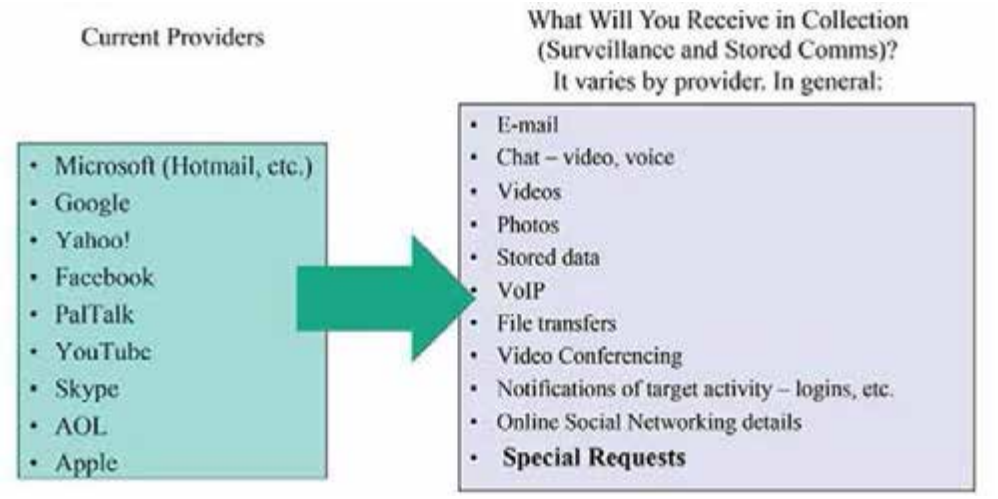
the role is not to spy, it shows the range of collecting data. It is not hard to imagine how much it endangers the privacy. The other issue connected to large number of mass surveillance agencies and programs is the amount of collected data. Similarly, to overregulation in legislation, collecting too much data may cause the situation in which this data is useless or hard to analyse. For example, NSA using various programs collects all they possibly can from the Internet. Yet, United States agencies missed some details warning about terrorist attack, which later lead to Boston Marathon bombings on April 15, 2013. This raises two questions. What is the point of uncontrollable data collection? How much surveillance is too much?

Surveillance was supposed to be a tool in the fight with terrorism, however, especially now when we know so much about PRISM and other similar programs, it is hard to think differently than just that mass surveillance became similar threat as terrorism itself. Our privacy is endangered, because ways to protect as from external enemies now are also aimed on us, citizens. Governments should not forget that privacy is a basic human right and as such cannot be violated on daily basis by mass surveillance. Privacy has important role in promoting democracy and significant impact on other fundamental rights, for example freedom of expression. Mass surveillance as a defensive tool cannot be also a tool costing us losing freedom and democratic values.[45] Uncontrollable data collection by mass surveillance agencies creates also other dangers – agencies may get access to files collected for other purposes, collected data may cause linking once separate information and eventually creating citizen profiles, finally mass databases are in big risk of losing confidential data.[46]

6. The role of Dominant ICT Companies

Thanks to Edward Snowden we now know how significant was and still is the role of biggest ICT companies. In the course of writing my Dissertation, it is interesting to see on the list all the dominant ICT companies that I like to call global dominant companies[47] – Facebook, Microsoft and Google and Apple. Facebook, Microsoft and Google are the core of my dissertation project.

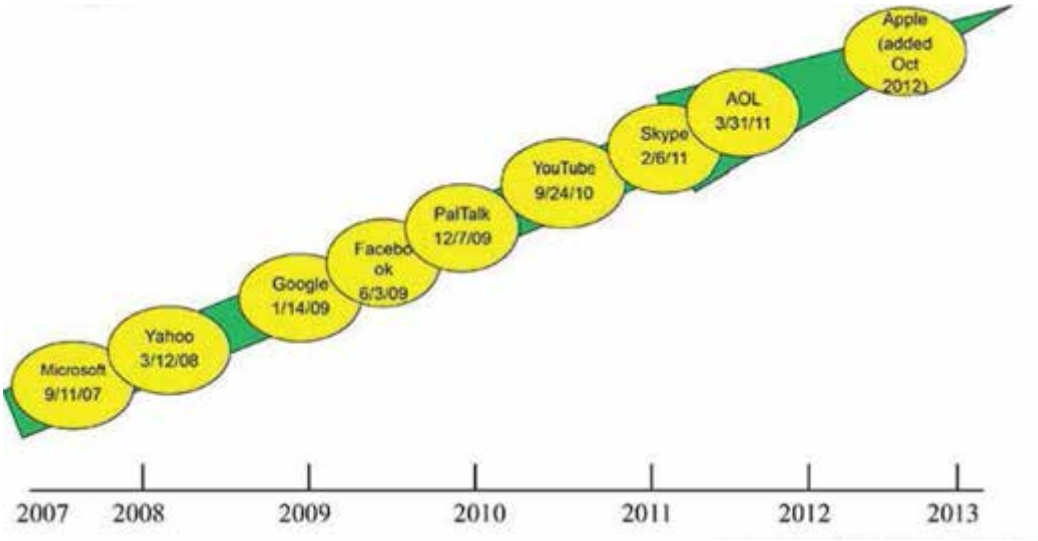
[45] B. Goold, *How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and Political Value of Privacy*, [in:] D. W. Schartum (ed), *Overvåking in en Rettsstat*, 2010, p 45–46.
[46] F. Webster, *Theories of the Information Society…,* p. 299
[47] A. Wiatrowski, *The "Dominance" in Abuses of Dominant Companies: More Than Super Dominant*, [in:] D. Svantesson, S. Greenstein (ed.), *Nordic Yearbook of Law and Informatics 2010–2012. Internationalisation of Law in the Digital Information Society*, Copenhagen 2013, p. 358.



Most interestingly when rumours about biggest IT companies cooperating with NSA arisen, all four companies immediately denied taking part in any mass surveillance program:

> *Microsoft*: "We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition, we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data, we don't participate in it."
>
> *Facebook*: "We do not provide any government organization with direct access to Facebook servers. When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law."
>
> *Google*: "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a 'back door' for the government to access private user data,"
>
> *Apple*: "We have never heard of PRISM. We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order."[48]

[48] J. Brustein, The Companies' Lines on Prism, June 07, 2013, http://www.businessweek.com/articles/2013–06–07/the–companies–lines–on–prism (access September 2015)



Above graph indicates that companies' statements have more or less the same value as, already mentioned in this paper, words of President Obama about NSA mass surveillance programs.

The role of the dominant ICT companies is significant not only for PRISM but in general, when it comes to collecting data. Fred Cate, James Dempsey and Ira Rubinstein wrote an article about systematic government access to private–sector data.[49] Private sector has nowadays almost unlimited access to data shared by users all around the world. As shown above PRISM and Tempora were using the biggest companies in the world for their purposes. In the mentioned article, which is also an introduction to reports about systematic government access in nine countries[50], eight issues were pointed out:

1. *Lack of transparency* – difficulty in assessing activities and laws concerning systematic government access,
2. *Significant expansion in systematic access* – despite of difficulties with transparency, in every country addressed by these papers there is evidence of a significant expansion in government demands for private–sector data in general and for broad, systematic access in particular,
3. *Significant commonality across laws* – data collection for law enforcement and national security are either exempted from general data protection laws or constitute permissible uses under those laws,

[49] F. Cate, J. Dempsey, I. Rubinstein, *Systematic government access to private–sector data*, [in:] *International Data Privacy Law*, volume 2, number 4, 2012, p. 195–199.
[50] Canada, China, United Kingdom, Japan, United States, Australia, Israel, Germany, India

4. *Inconsistency between law and practice* – inconsistencies between what law says and what governments are reportedly doing. It doesn't necessarily mean that the activity is illegal, but rather that it occurs subject to a legal interpretation that is withheld from the public or takes place in the interstices of national regulation,
5. *National security and law enforcement exceptions* – data collection and use for national security and law enforcement purpose is often excluded from oversight applicable to other data processing activities or subject to far less transparent standards and oversight regimes.
6. *The declining "wall" between national security and other uses* – national security and law enforcement gain access to private–sector data with greater ease plus the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected causes a substantial weakening of traditional data protection,
7. *Systematic volunteerism* – the most plausible means for systematic government access to private–sector data us through voluntary agreements with the operators of the systems and databases,
8. *Importance of multinational access and sharing* – cross–border access to data is essential to national security, law enforcement, and other government activities.[51]

7. Some consequences

Mass surveillance crisis brought us several consequences. I like to believe that surprisingly they are mostly positive. To say at least this issue came out to the light. It became obvious to most that using Internet and broadly understood Social Media comes with a cost. The cost of losing all privacy, not only to companies, but also to governments. Most definitely to US and British governments, but it is hard to believe that there are no other states conducting similar practices.

This growing awareness lead to the situation in which global ICT companies must have changed their business policies. Simply stating that they had nothing to do with mass surveillance is not going to work anymore. Therefore, some companies decided to take different

[51] F. Cate, J. Dempsey, I. Rubinstein, *Systematic government access to private–sector data…,* p. 197–199.

path, show that they are privacy and data protection friendly. Two best examples are Google's Project Zero and Microsoft's campaign "Putting people in control" that can be concluded with the words: *Microsoft experiences will be unique as they will reason over information from work and life and keep a user in control of their privacy*.[52]

It seems that both Google and Microsoft realized that to keep customers' trust they need to prove that they really have nothing to do with mass surveillance. At least not anymore.

Project Zero is a group of top Google security researchers with the sole mission of tracking down and neutering the most insidious security flaws in the world's software. Those hackable bugs, known in the security industry as "zero–day" vulnerabilities, are exploited by criminals, state–sponsored hackers and intelligence agencies in their spying operations. Google hopes to get those spy–friendly flaws fixed. What is also very important, Project Zero's hackers won't be exposing bugs only in Google's products but they'll be given free rein to attack any software whose zero–days can be dug up and demonstrated with the aim of pressuring other companies to better protect Google's users.

Microsoft chose different path, path of informing and educating. They say that are helping put user in control in three ways:

1. **Building privacy into policies and practices**. Putting you in control means offering transparency, starting with company policies that provide simple and easy to understand explanations of how we use your personal information.
2. **Building privacy into products**. We design and build products with security and privacy in mind, from our software development processes to using best–in–class encryption to protect your data. These steps are critical to keeping your information safe.
3. **Advocating laws and legal processes that keep people in control**. We require governments around the world use legal process to request customer data. We have challenged laws to make privacy protections stronger. In addition, we advocate for better public policy to balance privacy and public safety. [53]

Additionally, Microsoft created a simple guidance including following tips:

[52] http://blogs.microsoft.com/on–the–issues/2015/01/28/data–privacy–day–2015–putting–people–control/ (access September 2015)
[53] https://googleonlinesecurity.blogspot.fi/2014/07/announcing–project–zero.html (access September 2015)

1. **Once posted, always posted**: Think twice about posting comments, images or videos that you would not want your employer to see. Share, but do not over–share!
2. **Be knowledgeable about security and privacy settings**. Control who sees what you post by judiciously using social networks' privacy settings. For example, you may want to limit the people who can see Facebook photos from your cousin's bachelor's party to just a close circle of friends.
3. **Keep personal info personal**. Do not make cyber–criminals' jobs easier by sharing sensitive information such as your address or other personal data.
4. **Correct any inaccuracies**. If you see information about yourself that is wrong or that you do not want to share online, take the necessary steps to correct it. If someone posts a photo of you on Facebook that you don't want others to see, untag yourself or ask the original poster to remove the photo altogether.[54]

Finally, Microsoft promotes Microsoft's Safety and Security Center[55] and the National Cyber Security Alliance[56].

However, putting aside ICT companies attempts to prove us that suddenly they care about our security and privacy, there is a very recent development in European Union that we owe to Max Schrems and the European Court of Justice. The case was originally sent to the CJEU by the High Court of Ireland, after the Irish data protection authority rejected a complaint from Schrems. He had argued that in light of Snowden's revelations about mass surveillance, the data that was transferred from the Facebook's Irish subsidiary to the US under the Safe Harbour was not safely harboured. Advocate General Yves Bot of the CJEU agreed[57] with Schrems that the EU–US Safe Harbour system did not meet the requirements of the Data Protection Directive, because of NSA access to EU personal data.

In September 2015, CJEU stated that "the access enjoyed by the United States intelligence services to the transferred data constitutes an interference with the right to respect for private life and the right to protection of personal data, which are guaranteed by the Charter of

[54] http://lumiaconversations.microsoft.com/2015/01/28/stop–think–connect–safeguarding–online–reputation/ (access September 2015)
[55] Protect your privacy on the Internet, http://www.microsoft.com/security/online–privacy/prevent.aspx (access September 2015)
[56] http://www.staysafeonline.org/ (access September 2015)
[57] Opinion of Advocate General Bot delivered on 23 September 2015, Case C‑362/14 Maximillian Schrems v Data Protection Commissioner, http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=326249 (access September 2015)

Fundamental Rights of the EU." According to the Advocate General, the big issue is "the inability of citizens of the EU to be heard on the question of the surveillance and interception of their data in the United States," which therefore amounts to "an interference with the right of EU citizens to an effective remedy, protected by the Charter."[58]

Finally of October 6th 2015 Court of Justice of European Union has ruled that the transatlantic Safe Harbour agreement, which lets American companies use a single standard for consumer privacy and data storage in both the US and Europe, is invalid.[59]

The main points of the CJEU decision are:

- Individual European countries can now set their own regulation for US companies' handling of citizens' data.
- Countries can choose to suspend the transfer of data to the US.
- The Irish data regulator will now examine whether Facebook offered European users adequate data protections, and it may order the suspension of Facebook's transfer of data from Europe to the US if so.

Decision by Court of Justice of European Union is very important. It will change the situation in the area of privacy, data protection and mass surveillance. For exact consequences, we have to wait. However, already now I can see that companies such as Google and Microsoft will be vastly influenced and European Union, the states to be more specific, should now be able to prevent them from massive abuses to privacy.

8. Conclusion

The Soviet Union, East Germany, and other totalitarian states rarely respected the rights of individuals, and this included the right to privacy. Those societies were permeated by informants, telephones were assumed to be tapped and hotel rooms to be bugged: life was defined by police surveillance. Democratic societies are supposed to function differently.[60]

Mass surveillance programs, knowledge about it, about PRISM in particular, the role of the companies with which we share sensitive data on a daily basis, it all have both very negative and some positive results for now and for the future of privacy and data protection.

[58] Court of Justice of the European Union PRESS RELEASE No 106/15, Luxembourg, 23 September 2015 http://curia.europa.eu/jcms/upload/docs/application/pdf/2015–09/cp150106en.pdf (access September 2015)
[59] Court of Justice of the European Union PRESS RELEASE No 117/15, Luxembourg, 6 October 2015, Judgment in Case C–362/14, Maximillian Schrems v Data Protection Commissioner, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015–10/cp150117en.pdf (access October 2015)
[60] W. Diffie, S. Landau, *Privacy on the Line…,* p. 143.

Today we live in the new Network Society, which is also a Surveillance Society. Together I like to call it a society that is trapped in the network and this network is under constant mass surveillance. The simplest way to explain it, the reason to call this situation as being trapped in the network is that there is no choice anymore. As a society and as individuals we are in every aspect of our lives completely dependent on technology and infrastructure provided by technology. I cannot imagine a person living in modern society not being a subject of some kind of surveillance, as well as I cannot imagine this person being able to break with the access to technology.

However, there are attempts to seek for privacy in the Internet. Growing popularity of services hidden in Deep Web[61] are the sign of it. Unfortunately, hiding in Deep Web may expose us to even bigger threats to our privacy. Deep Web today is a place for all sorts of criminal activities, a haven for thieves, child pornographers, human traffickers, forgers, assassins and peddlers of state secrets and loose nukes.[62] Yet, more and more people chose to hide there, as this is the area unavailable for any kind of surveillance. It shows how desperate are some people in seeking privacy, but also it shows growing privacy awareness.

I absolutely do not support the idea of popularizing Deep Web, as a place highly dangerous, but I like the idea presented by Susan Barnes. She suggests that education about dangers on social media pages, especially education of younger generation may be the way to protect privacy and to raise privacy awareness.[63] It may be little naive, but knowing how recklessly young people give up sensitive data about themselves, it could be important solution and way to protect us from real life threats caused by losing our privacy on social media pages.

It is a good thing that there are attempts to save privacy or what has left of it, but the attention drawn to the problem suggests it seriousness and for how long we ignored this problem.

We have to remember that challenges to privacy are even bigger now, when Information Society changes into the Network Society. There are more risks, society seems to be more

[61] The surface level of the Internet is basically everything that is indexed by search engines such as Google. Facebook, Youtube, these are all surface sites. However, according to The Guardian, you can only access around 0.03% of the total internet on a search engine. Deep Web is World Wide Web content that is not part of the Surface Web, which is indexed by standard search engines. – *Exploring the Hidden Internet ("Deep Web")*, http://www.teamliquid.net/forum/general/229525–nsfw–exploring–the–hidden–internet–deep–web (access September 2015)

[62] L. Grossman, *The Secret Web: Where Drugs, Porn and Murder Live Online*, November 11, 2013, http://time.com/630/the–secret–web–where–drugs–porn–and–murder–live–online/ (access September 2015)

[63] S. B. Barnes, *A privacy paradox…*

willing to share sensitive data and standards of information security are very modest. Altogether, privacy requires sophisticated information security.[64]

All these efforts for privacy are very positive as there is no doubt that privacy will be beneficial for society also in the future. Legal systems must continue to contribute effectively to privacy and data protection. The contribution may be almost impossible on a national level.[65] However, it is possible within international legislation, but might result in overregulation and consequently in loopholes, inconsistency and ultimately in even more interpretations leading to violating privacy.

Regarding the topic of mass surveillance, it is impossible to end with this practices. In my opinion, surveillance is a necessity for both governments and private companies, the dominant ones in particular. Yet it is important to remember what ECHR article 8 gives us. "Any interference by a public authority with a Convention right must be directed towards an identified legitimate aim (…) The sorts of aims which are legitimate are interests of public safety, national security, the protection of health and morals and economic well–being of the country or the protection of the rights and freedoms of others." Convention approach is to decide whether a particular limitation from a right is justified. Meaning that limitation must be proportionate to the legitimate aim pursued.[66]

The way to protect our privacy is to limit surveillance's infinity. The idea called Privacy–Protective Surveillance (PPS)[67], by Ann Cavoukian, is an answer to typical approaches of protecting privacy, where while ensuring measures to counteract terrorism, we seek to strike a balance between privacy and surveillance. This often leads to making privacy the less important value, in favour of the more significant one, which is public safety. PPS is an alternative to current counterterrorism surveillance systems. One of the most attractive elements of PPS is the fact that its intelligent agents will only collect data that is considered significant. Significant data is defined by transactions or events that are believed to be associated with terrorist–related activities, for example, purchasing fertilizer capable of bomb making or accessing a bomb–making website. An important consequence of PPS's collection of significant data is that intelligent agents would effectively be blind to seeing any other information they may run

[64] A. Saarenpää, *Perspectives on Privacy…,* p. 24–25.
[65] P. Blume, *The Importance of Information Privacy and its Future*, [in:] S. Greenstein (ed.), *Vem reglerar informationssamhället?*, Stockholm 2010, p. 169.
[66] J. Wadham, *Human Rights and Privacy – The Balance*, speech given at Cambridge (March 2000), http://www.liberty–human–rights.org.uk/mhrp6j.html, more in D. J. Solove, P. M. Schwartz, *Information Privacy Law*, Fourth Edition, New York 2011, p. 1072, 1073.
[67] See A. Cavoukian, K. El Emam, *Introducing Privacy–Protective Surveillance: Achieving Privacy and Effective Counter–Terrorism*, September 2013, http://www.privacybydesign.ca/content/uploads/2013/12/pps.pdf (access September 2015)

across during their searches. Additionally, the use of homomorphic encryption would allow PPS to make computations or engage in data analytics on encrypted values – data that cannot be read because it is not in plain text. This provides additional assurance to individuals that recording or monitoring their actions within the system is impossible. Finally, the intelligence gathered by PPS would be context–specific. In order to become information of value, data must be placed in the appropriate context.[68]

Fortunately, the privacy issues are recognized not only by Internet users and scholars. International Data Privacy Day[69], watchdog organizations, Data Protection Regulation, revision of OECD principles, legal actions against Google[70], Max Schrems actions and CJEU ruling, are some of the recent examples of the increased awerness of privacy issues. Together with recognizing that we do not need more legislation, but the legislation, which is consistent, we still have a chance of keeping our privacy. Not the one we would like to have, for that it may be too late, not what has left of it, but new modern privacy for modern society, Network Society. This privacy cannot, nor will be complete but it has to be ready for challenges that may come. Today mass surveillance is no longer surprising to us, now we must work to never be surprised by what can come in future.

[68] A. Cavoukian, K. El Emam, abstract of *Introducing Privacy–Protective Surveillance: Achieving Privacy and Effective Counter–Terrorism*, September 20, 2013, http://www.privacybydesign.ca/index.php/paper/introducing–privacy–protective–surveillance–achieving–privacy–effective–counter–terrorism/ (access September 2015)
[69] See https://www.staysafeonline.org/data–privacy–day/ (access September 2015)
[70] H. Dixon, M. Warman, *Google gets 'right to be forgotten' requests hours after EU ruling*, May 14, 2014, http://www.telegraph.co.uk/technology/google/10832179/Google–gets–right–to–be–forgotten–requests–hours–after–EU–ruling.html (access September 2015)

AN ATTEMPT FOR CLARIFICATION: WHAT DO WE MEAN WHEN WE SPEAK OF MEDIA CRISIS – AND HOW IS IT RELATED TO MEDIA AND COMMUNICATIONS REGULATION

Hannu Nieminen

Professor of Media and Communication Policy, University of Helsinki, Department of Social Research Media and Communication Studies, hannu.nieminen@helsinki.fi

Background

1. The basic point of departure in this paper is that as a result of major transformations in the capitalist mode of production between the 1970s and the 2010s, fundamental changes have taken place in all areas of social and cultural relations. Although these transformations began in the economic sphere already in the late 1960s and early 1970s, their full repercussions have been felt (and understood, at least partly) in the field of the media much later, from the 2000s onward.

2. The general background can perhaps be explained briefly in the following way. In the development of the modern state the role of the media – originally the newspaper press, then radio and television – have been elemental, as the national organization of interests was their central function. In this way, the media have been pivotal in the social and cultural construction of modern nation states. From this viewpoint, the media can be compared to other major nation–building institutions, such as the education system, the church, national army, and civil service. They all can be characterised epistemic institutions, creating and reproducing a form of knowledge that is centrally constructed around national concepts and symbols.

3. Different media have served this process of nation building in different ways. The early newspaper press was established in order to organise competing interests (between different classes and other social forces) but this competition was situated sternly within national frames – that required a recognition of differing interests, sharing however a common framework or symbolic reservoir (e.g. as in the concepts of Englishness, Finnishness, etc.). As a result, from this form of external pluralism, something like a

class–based understanding of citizenship was formed, the shared concept of citizenship being a common denominator.

European radio broadcasting, and later television, represented a different form of interest organisation. Instead of particular interests as presented by newspapers – and the form of external pluralism that they represented – the radio broadcasting epitomised public interest, in a sense that particular interests were negotiated and organised within a single medium. Against the class–based citizenship, this form of internal pluralism promoted the idea of universalist citizenship. The commercialised newspaper press, which took over from the party press in Europe between the 1930s and 1970s, offered still another way of organising national interests based on universalised internal pluralism: a market–based organisation (consumer identity), where the market took a place of a non–partial arbiter of particular/private interests.

4. A high time for national epistemic institutions was the intensive period of European reconstruction after the WWII (the late 1940s—the end of 1960s) when economic recovery required the integration of all social groups in the process of reconstruction. This period was characterised by the deployment of an extensive mode of reproduction (in contrast to the intensive mode adopted later). The central metaphor was large–scale industrial production: factories, Taylorism, division of labour, etc. For the effective organisation of industrial production, a policy of social and political pacification aiming at softening down class differences was adopted. A number of important social reforms were carried out by the early 1970s; in many countries, the left parties, earlier excluded from political life, were now invited into national negotiations and consensus building efforts; new ways of workers' participation were experimented in industrial relations; etc.[1]

5. In order to enhance the values and ethos of national reconstruction, the main epistemic institutions were engaged in this work. This concerned equally education, church, cultural institutions (arts, museums, and libraries), universities and sciences, as well as the media. It must be emphasised, however, that in each country the situation was different, and the relations between different institutions reflected national peculiarities. Thus, for example in the Nordic countries the (neo–)corporatist arrangement of social

[1] Ralf Dahrendorf's concept of the peaceful settlement of societal conflicts was influential in these processes. See Dahrendorf 1959.

relations was more extensive than in Central and Southern Europe, which was reflected also in the status and position of the media.

6. Following what was stated above, from this 'critical functionalist' perspective the role and function of the media – like all epistemic institutions – started to change profoundly from the 1970s onward. The basic mode of capital accumulation changed from the extensive to the intensive mode, which did not require any more the same kind of integrative social and cultural policies. Instead of the policy that aimed at equalising societal differences, policies promoting social dis–integration and segregation were now adopted, as they promised better economic benefits – at least in the short term. This was the promise of the neoliberal turn, which started to gain foothold, first in the US and UK in the late 1970s and later in most European countries.

7. At the same time, the traditional global system based on a negotiated balance between nation states (of which the UN was an emblematic example) appeared to have run its course: the political and economic sovereignty of nation states created now an obstacle for global capital accumulation. If European countries and companies were willing to compete with the US and Japan in the global market, it required the establishment of single European market, supported and enhanced by respective social and political structures.

8. This process toward global competition in the form of the unified European economic and political framework, and doing away with the old regime of nation states, not only challenged the 'old' epistemic order, which still was based on the idea of nation state democracy and national institutions, but it undermined the latter's basic dynamics. An extreme interpretation of the direction of change, described above, can be presented from the perspective of 2013 roughly as follows.

Conditions for the old (meaning here after the WWII) relations of social production, which used to be based on the principles of full employment and national social and cultural integration, lost much their ground during the 1980s and 1990s. Instead, after the early 2000s the relations of production are increasingly based on the segregation of labour market, 'flexible' work contracts, increasing reserve of un– or under–employed workforce, etc. The national regulatory structure, and the practices based on it have lost their competence, as the

coordination of social production does not take place any more on a national but on a supra–national level.

Additionally, the coordination of productive relations used to be regulated by political decisions, based on the balancing of competing interests and achieved by democratic means – first on a national level, then – if needed – between the governments on the international level. Today this coordination appears to take place by the decisions of the 'market forces', which the political bodies – governments and inter–governmental organisations, such as the EU, then translate into policy guidelines. [2]

Three levels of crises

In order to understand the historical context for the changes and crises in media regulation, it might help to make a distinction between three different levels of the crisis. The first concerns a more general crisis of the capital accumulation (see above), which has direct consequences to the functioning of the media; the second concerns the crisis of the media system, which is partly a reflection of the former but has also a logic of its own; and the third is about the crisis in media regulation, which is closely related to the two previous levels but works still on another level.

In what follows I will first, in very general terms, try to clarify how these three levels are related; after this, I will to study somewhat closer the crisis on the level of media regulation.

1) The crisis in the 1970s

1. Before the first oil crisis in 1973 the Western European countries had enjoyed, together with the US and Canada, a long period of continuous economic growth.[3] This 'Long Boom' brought along rising living standards for most population. The expansion of education opportunities provided for increasing social mobility. The increasing free time combined with new affluence invited the growth of new industrial branches, especially those in the area of symbolic production: tourism, entertainment and leisure industry, mass media (television, sound recordings, glossy magazines etc.) and other forms of mass culture started to proliferate. All this – combined with the rise of the

[2] See e.g. Crouch 2004; Duménil & Lévy 2013; Beaud 2001; Michalis 2007, 10–16.

[3] From the aftermath of the WWII and the reconstruction period until the early 1970s the OECD member countries enjoyed real GDP growth rate averaging between 4 and 5 per cent in the 1950s and 1960s, compared with 3% in the 1970s and 2% in the 1980s.See Marglin & Schor 1990.

Keynesian welfarist social policy – amounted also to the pacification of social relations: the economic growth had a smoothing effect to class conflict.

Under all the years of the Long Boom there loomed, however, the Cold War and a fierce ideological struggle between the two world systems. The fear of communism was felt intensely in practically all West European countries, with attempts to isolate the Western communist parties and to minimise their public influence. In Western Europe and the US as well, the increasing economic affluence was joined with political and ideological paranoia, allowing for the continuous militarisation of societies.

2. By the early 1970s the Western economy started to suffer from structural problems. Starting from the US, economic growth stagnated, joined with rapidly rising inflation ('stagflation'). Social and political stability, long reined by the fruits of growth, faltered and resulted to increasing signs of mass discontent (France 1968) and terrorist activities (Germany, Italy, USA). At the same time hopes for liberal changes and 'socialism with human face' created tensions within the socialist block, resulting to a conservative backlash (Prague 1968). Political and military tension between the Cold War parties heightened and led to an escalating arms race.

The Long Boom ended finally in 1973 when the first Oil Crisis paralyzed the Western economy. The economic dynamism (increasing consumer demand in an expanding market place) which had guaranteed a constant growth for the previous almost 20 years was worn out, and Western capitalism had to re–programme itself. The new programme was slow in developing and got its shape only step by step, through several new crises (depending on the criteria, the periods of recession were experienced in 1979, 1991–92, 2000–02, 2008–09, 2011–13).

3. Solutions to the crisis and the means to return to higher rates of growth were sought from several directions, some traditional and some new. They included:
   - Lowering the costs of industrial production: transferring production to low wage countries; flexibilizing labour contracts (crushing the union power); substituting computerized work processes for human labour (post–fordism); removing global and regional trade barriers.
   - Reconstructing the financial mechanisms to promote growth: expanding the non–productive sector of economy (banking, insurance, taxation); creating global financial market; inventing new instruments to intensify the circuit of capital (options and other incentives; hedge funds)

- Exposing previously non–market functions of society and culture to market logics (the process of commodification of the symbolic sphere): privatisation of public utilities and services; adopting the 'New Public Management' principles to public administration; commodification of culture and symbolic production (education, universities, arts and other cultural institutions, the media)
- Re–redistribution of wealth: promoting private monopolies through privatising public utilities (windfall profits); rewarding the capital owners and other high-income groups by tax redemptions paid by cuts in public services.

4. In order to manage and coordinate all these different elements of the transformation of capitalism, several basic conditions were needed:
   - Politically, a new elite consensus was needed. The old one, based on a modelled Keynesian economic ideal, favoured the political elite as it had rested much on the instruments of financial and economic policy. A new balance of power between political and economic elites emerged, based now on a shift of power to the side of the economy.
   - Technologically, the new global economic and financial formation required a constant monitoring and controlling both the processes of production and trade and the flow of financial transactions. A new global information network with very high capacity was necessary.
   - From the viewpoint of global security, the new constellation created also unexpected vulnerabilities. In the post–Cold War constellation, the Western elite consensus with its military dimensions (Afghanistan, Iraq, Israel) was met with increasing global dissatisfaction. A new global security infrastructure was required in order to control the new global economic and political order (the War on Terror; the Patriotic Act; etc.).
5. The question is, how all this is connected to media and communications? Briefly:[4]
   1) The new political consensus needed popular legitimacy. The media had a major role in constructing public consent to support the new policies – which, in many respects, were undermining the previous achievements on social policy and labor relations.
   2) On the other hand, as entertainment and cultural industries were becoming increasingly important areas on new commerce, media and communications policy

[4] See also e.g. Crouch 2004; Michalis 2007.

was met with new pressures and expectations to open the market by reducing regulation on these areas.

3) The new global economic and financial order required the rapid expansion of computerized information network – the internet. In the name of efficiency, all societal institutions and organizations needed to be linked to the network – industry, administration, households. The internet (or new ICT more generally) promised to fulfill several mutually benefiting economic functions: a) it provided a necessary conduit for economic and financial information (b–t–b); b) it created a new business area in itself (Google, Microsoft, Apple, Facebook; mobile telephony); c) it opened up new global business opportunities and models for business; and d) it offered new ways for interaction between public administration and citizens.
4) In order to protect both the safety of the networks and that of the whole society, which has become more and more dependent on the network, both the online traffic and the internet users are increasingly under constant surveillance by the security authorities, as the disclosures on the US security agency NSA by Edward Snowden graphically have recently shown us.[5]

2) The economic crisis of the media system

There are several possible strands that we can follow when studying the crisis of the media system. However, in my analysis it is basically a crisis of traditional media economy: the traditional business models did not function any more – both politically, as they could not provide any more the socio–political stability and cohesion, as was the case in the reconstruction period after the WW II; and economically, as people's consumption patterns changed at the same time as the costs in media production started spiralling. For this reason, I will limit my focus here on the general description of the economic decline in the traditional media industries, newspapers and television.[6]

Before the 2000s

1. The crisis of the media system in Europe can be divided in two (or three) main phases. As stated above, my starting point here is that it is basically an economic crisis which has significant reflections on the political and cultural levels too. The sources for this are at least twofold: 1) on one hand, as the media was, as a result of the more general

[5] See http://www.bbc.co.uk/news/world–us–canada–23768248.
[6] I try to analyze the political implications of the crisis elsewhere.

shifts in the capitalist economy (described above), now taken as an industry among other industries, it was expected to generate significant profits. For a number of years this was the case: in Finland, the rate of profit in media industries (especially the newspaper industry) was steadily between 15 and 25 per cent. 2) On the other hand, because of increasing free time and cultural consumption combined with the higher education level, the media consumption – in its different forms – kept rising. Thus for example the newspaper circulation in Finland was its all times highest in 1989: 824 copies per 1000 inhabitants (in 2011 the figure was 509). Daily average television viewing time in 1990 was 109 minutes (in 2012 it was 183).

2. However, from the late 1980s and early 1990s onward changes in people's free time activities and consumption patterns led to a decline in the traditional business models of media industries. People – especially the youth – began to look other sources for information and entertainment. In the early 1990s, the circulation of newspapers began their long and steady decline. Although radio listening has remained popular, it has declined clearly among the younger age groups; the same goes with television watching.

Especially the newspaper market has become more and more competitive as the companies are fighting over fewer and fewer readers. Both traditional sources of newspapers' became endangered: the number of subscriptions (and single copy sales, which in Finland were only some 8 per cent of total sales) declined from year to year; the income from advertisements decreased as advertisers paid less for having an access to the dwindling number of readers. In 2000, the advertising income of the dailies was 528 € million; n 2012 it has dropped to 404 € million.[7]

3. In the rapidly developing European electronic communication (television and radio) business competition has been as hard. As European television industry was, to a great extent, privatized and deregulated in the 1980s and 1990s, new businesses entered the market in great numbers – especially in the fields of cable and satellite television. Although the governments attempted to regulate the market by imposing obligatory licensing for an access to radio frequencies (in terrestrial broadcasting), in the satellite

[7] Finnish Mass Media 2011; http://www.mainostajat.fi/mliitto/sivut/Mainosvuosi2012lehdistotiedote.pdf.

and cable transmission the competition was practically all but unregulated.[8] One of the results was a strive for controlling the market by (cross–)ownership concentration, leading in many countries to the formation of big media houses, some of which expanded soon to major transnational actors (such as Fininvest, Bertelsmann, News International, Vivendi).

4. Increasing competition influenced directly media contents, too. As described above, commercial values started to be emphasized more in news selection and news framing, leading to a major change in how the relationship between journalism and reading audiences was conceived. This has been characterized as a shift from citizen–oriented to customer–oriented journalism. As concluded above, this has naturally meant also a major change in how the role of the media used to be understood in democracy.[9]

After 2000

1. Although these two long-term developments – the financial decline of the traditional media and the commercialization of their contents – started already in the 1980s, they were much intensified by the introduction of digital media technology (ICT) in the 1990s and 2000s. On one hand, new ICT opened up new opportunities for developing and improving the production processes in many ways (computerization and automatisation of manual tasks); on the other, as it soon came out, together with the advent of the Internet, the traditional strengths of the 'old' media (fastness, connectivity, engagement) were now captured and accelerated by different forms of new media.

2. The challenge of the new media to the traditional media comes at least from two directions: first, from the free delivery of news and information services; and second, from the increasing popularity of the social media platforms.

    1) Firstly: as the Internet was able to deliver the news and other traditional newspaper contents 24/7 and as the online services were 'free', compared to the subscription or single copy fees, the Internet news sites gathered increasing number of audiences or

[8] In satellite transmission, however, the TVWF directive stipulated the 'country of origin' principle which functioned as a guiding principle.
[9] See e.g.Curran 2011; Nieminen & Trappel 2011; Nielsen 2010.

'users'. This led the advertisers to navigate to the Internet, too, with the effect that the negative income spiral of newspapers got worse: the decrease in the number of readers was aggravated by the loss of advertising money.

With the digitalization of television, the same challenge was met by traditional television companies. Audience was shifting in great numbers first to the competing niche channels, leading to the decline in advertising money. First, it was attempted to counter with pay channels (movies, sports, life style) but it did not bloc audiences from shifting to the Internet and its 'free' offering.

2) Secondly: from the viewpoint of the traditional media, the problem with the social media (Facebook, YouTube, and the like) is that they offer much more effective channels to advertisers to target their desired consumer groups, thus diverting advertising money from newspapers, both in their print and online forms.

3. The traditional media companies are still struggling to change their business models profitable in the online environment. Newspapers are experiencing with different ways to make money from their online versions – both by 'personified' advertising and by experimenting forms of 'pay walls' – but at least by now, without a sustainable financial solution.

Television companies have a different problem: despite the total audience figures keeping constant or even slightly increasing,[10] because the audiences are spread to a number of smaller (digital) channels,[11] traditional channels are losing advertisers. As a counter tactic, the companies are developing their pay–online services, but have realized that they must compete with specialized 'OTT service' companies (such as Netflix, HBO, Hulu).

4. For newspapers, the solution has been to continue the commercialization of their ways of operation on the cost of traditional journalism. The costs of production must be brought down by any means; each unit of the 'output' must be able to create income. The whole culture is oriented to making money. The smaller number of journalists must

[10] See Nordicom statistics, http://www.nordicom.gu.se/eng.php?portal=mt&main=showStatTranslate.php&me=1&media=Television&type=media&translation=Television.

[11] In four Nordic countries (Finland, Iceland, Norway, Sweden, there were in 2001 together 36 national tv–channels. In 2011, they were 103. See Nordicom, http://www.nordicom.gu.se/eng.php?portal=mt&main=showStatTranslate.php&me=1&media=Television&type=media&translation=Television.

produce more 'output'. The 'new' journalism is lighter, more opionated and personified, less edited, aimed at being interesting and gathering attention.[12]

5. From the economic point of view, who are the winners and who are the losers? The winners include 1) the internet operators, both the connection suppliers (telecoms and cable companies) and the content service operators; 2) the equipment industry (smart phones, tablets, mobile computers, 'connected' TVs). The losers or the *crisis industries* are 1) the newspaper industry, 2) traditional terrestrial television, 3) traditional audiovisual industry (cd, DVD). *From the viewpoint of traditional representative democracy, with the demise of the traditional news and information services and in the lack of corrective news and information provision, the ultimate loser is the informed citizenry.*

3) The crises of media and communications regulation

1. As a result of the changes in media system from the 1980s, the old regulatory framework was plunged into crisis. It concerns the general incompetence of the old system of regulation to face the three–level challenge: first, the one posed by the neo–liberalist belief into the virtues of the market (a long–term trend); second, that of digital convergence, which undermines the traditional sectoral regulatory framework (a mid–term trend); and third, the immediate crisis of the media after 2008 (immediate crisis).

2. As the general crisis of the media system has long historical roots, so does media regulation. We can distinguish between three recent phases in the development of the media regulation (for periodization, see e.g. Gibbons & Humphreys 2012; Michalis 2007; Harcourt 2005):

    1) The period between the 1980s and the early years of the 2000s was characterised by regulatory liberalisation (de–regulation) and privatisation of public communication facilities. It was based on the belief of market self–regulation; the governments only providing suitable conditions for markets to provide.

[12] see e.g. Nielsen 2012, https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/Working_Papers/Nielsen_–_Ten_Years_that_Shook_the_Media.pdf; Barnett 2009, https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/Journalism_Democracy___Public_Interest_for_website.pdf

2) The period between the double crash, the DotCom and Telecoms crashes (2001–2002) and the crisis of 2008–2009. From a regulatory viewpoint, this was a period when it became clear that the market self–regulation is not sufficient and cannot guarantee fair competition and consumer choice, as it was expected. What followed was a regulatory re–engagement of the state to establish proper conditions for competition (regulation for economic benefits). This included the strengthening of the role of independent national regulatory authorities.
3) The third period started in the aftermath of the crisis of 2008–2009, and is characterised by the emergence of a number of issues which neither the market self–regulation nor the state's competition regulation have been able successfully solve, such as: hate speech/mail, protection of minors, protection of privacy, data protection, digital divide, consumer protection, copyright infringements, and others. What is expected is that the regulatory responses must now include more emphasis on the social dimensions of regulation. What might be a possible development is a regulatory framework which combines all three elements: market self–regulation, state–led competition regulation, and regulation promoting social and cultural values.

3. The main problem facing the future of the media is however the deepening systemic crisis of European economy that has resulted in increasing social and political polarization. At the moment, in summer 2014, we don't yet know if and how Europe will solve the crisis, and how does the general European social, political and cultural landscape look like after this.

E–JUSTICE AND THE NETWORK SOCIETY
SOME COMMENTS FROM THE FINNISH POINT OF VIEW[1]

Ahti Saarenpää

Professor emeritus, Institute for Law and Informatics, Faculty of Law, University of Lapland, Docent, Faculty of law, University of Helsinki, Vice Chair, Finnish Data Protection Board, Finland, ahtis1@gmail.com

Keywords: ***network society, information government, openness, right to know, access, information law, legal design,***

Abstract: *New concepts and terms take their time maturing. We certainly see e–justice covering quite a range of topics today; the term is still far from being well established.[2] Then again, the term is not used that extensively in different legal contexts. In fact, it has not been used much in Finland to date. Yet, this does not mean that we are behind the times – or at least not too far behind. As we have in many comparisons seen, Finland was internationally active early on in developing legal databases and information systems for the courts and court administration.*

As far back as in the early 1980s, Finland created a big national legal database. Finlex, as it became known, owes it origin in large measure to the early initiatives of the Council of Europe. Perhaps not surprisingly, in the mid–1990s we were one of the world's most advanced countries when it came to information management in the Ministry of Justice and the related computerization of the courts.[3] After that the progress has not been as outstanding. Now we are however building a new information system called AIPA, which can be described as a third–generation system that compels judges to use the system. The system we see there is no longer a mere tool but a comprehensive digital environment for adjudication, information management and communication.

My article examines the various dimensions of the concept of e–justice, takes a brief look at certain earlier phases of development and, lastly, takes up the present situation and aims in Finland. Looking back, we have seen many successes but also substantial problems. The latter have emerged in areas ranging from attitudes to IT know–how and from research and teaching to the new professional skills of digital lawyers; they have even extended as far as the economics of information when planning and implementing extensive information systems. Planning e–justice always involves far–ranging solutions.

My point of departure here is a fairly straightforward one. We have progressed from the early technical development of office automation to the high quality

[1] Will be published in Brazil.

[2] See for example Xanthoulis Introducing the concept of 'E–justice' in Europe: How adding an 'E' becomes a modern challenge for Greece and the EU in address: effectius.com and Herberger E–justice Kompetenz: Plädoyer für einAusbildungskonzept p392–394 in Gottwald (ed), Festschrift für Martin Schneider: neu bei Editions Weblaw (2014).

[3] About the important role of the Council of Europe even nowadays see Stawa The Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe: Information and communication technology (ICT) in the courts (e-justice and e-courts) pp 579–598 in Gottwald (ed), Festschrift für Martin Schneider: neu bei Editions Weblaw (2014).

required of the various implementations of e–justice in the modern European constitutional state in a sophisticated Network Society. Contrary to what many think, e–justice is not just one stage in the computerization of electronic administration. Rather, e–justice should be viewed as a significant step towards improving the quality of legal information, enhancing legal professional skills and promoting equitable administration of justice in the new Network Society. Appropriate e–justice services, appropriately implemented, further our right to information and to the equitable administration of justice in a constitutional state, a state that respects the rights of its citizens.
Legal systematics serves to constrain the power typically exercised by experts and authority. That´s why it is important to say, that my opinions are mostly based on the principles of information law.

1. A historical starting–point

When computers had developed to the point where they began to be used for commercial and administrative purposes – the 1950s and 1960s – it was no surprise that the idea arose of using the new technology in the courts. It was time to move on from the theoretical explorations of *Lee Loevering* in the 1940s to practical applications.[4]

One of the first people in Finland to delve deeper into the question was *Eiler Hellström*, a lawyer at IBM. He proposed that an extensive study should be done on the automating the judicial administration. *Hellström* put particular emphasis on ordinary office tasks and archiving. We found ourselves in the midst of a transition to the era of office automation.[5] In fact, the early 1960s saw attention being drawn to this development widely. A committee was appointed in Finland to consider the need in general for computers in government administration.

Later, no fewer than two committees – each known as the EDP committee – submitted reports on the computerization of the administrative division of the Ministry of Justice. The documents, completed in 1973 and 1974, set out the foundation for a new era.[6] To use a modern term, *e–justice i*n Finland was born with the discussion that the two committee reports stimulated.

That discussion proceeded on two levels. On the one hand, within the Ministry of Justice it centred on the opportunities for increased use of the new technology. Statistics, registration

[4] See *Loevinger* Jurimetrics — The Next Step Forward. Minnesota Law Review 1949 pp. 455
[5] The comments of Mr *Hellström* can also be seen as a part of IBM marketing activity at that time in many countries.
[6] Oikeushallinnon informaatiojärjestelmän kehittämissuunnitelma, KM 1973:58 and Oikeushallinnon informaatiojärjestelmän kehittämissuunnitelma: kehittämistyön organisointi, järjestelmän edellyttämä koulutus ja teknisten ratkaisujen perusteet: KM 1974:6. Both reports are unfortunately in Finnish only.

and archiving stood out as the naturally most interesting applications, as *Eiler Hellström* had suggested they would be. Consideration was also given to the prospect of developing *legal databanks*. Part of the impetus here was the active role being played by the *Council of Europe*. While for political reasons Finland was not a member at the time, it nevertheless followed the activities of the Council very closely. And, in traditional Nordic fashion, the EDP Committee had familiarized themselves with the work that was being done – and had started somewhat earlier – in Sweden.

The second level of discussion was that in the discipline of law, although at the end of the day this was scanty indeed. Earlier, in 1965, *Kaarle Makkonen*, in his doctoral dissertation that became well–known internationally as well, had rejected the idea that a judge could be replaced by a computer.[7] *Kaarle Makkonen* was later professor of legal theory at the University of Helsinki.

I myself was perhaps the most outspoken critic of the first committee report, which had considered the IT prospect. I drew attention to the numerous problems in the committee's plans, which were very optimistic but presented largely in checklist fashion. On the other hand, I also described the report as important and interesting. The authors had noticed the problems involved in combining information and undertaken to present a comprehensive picture of what constitutes significant legal information.[8]

One outcome of the report was the creation of what is known as the judgement system. It was considered desirable to write the operative part of judgements in a standardized form in order to facilitate enforcement. In practice, the system, opposed by judges as compromising the independence of the judiciary, was created by Justice *Martti Leisten*, who had been a member in the committee, who later directed a project to develop e–justice systems and to computerize the courts and also created the Finlex legal databank.[9] He subsequently served 1988–1997 as President of the Rovaniemi Court of Appeal, where he tried to get a somewhat reluctant staff used to using information technology. And he was bit by bit successful in this project too.

After this necessarily brief historical overview, to be augmented in parts later, I would now like to move on to look at the contemporary debate on e–justice.

[7] *Makkonen* Zur Problematik der juridischen Entscheidung : eine strukturanalytische Studie.
[8] *Saarenpää* Oikeudellista tilastointia, Oikeus 3/1973 pp. 39–48 .
[9] Finlex is an official national legal databank hosted by the Ministry of Justice. It is open without charges in the following address : www.finlex.fi/en/

2. E–justice in the modern constitutional state

When IT began to become established in administration and commerce, Europe was still living in the era of the traditional *administrative state*. In a word, it was a state where the individual existed for the government. People were referred to as subjects of their government. In such a state it was natural to think about IT and plan its use of primarily in terms of achieving increased administrative efficiency. And this is what was done in Finland, as elsewhere.

In today's European *constitutional* state, everything in principle proceeds from the rights of the individual – *fundamental* and *human rights*. Society is for the people in it. The difference vis–à–vis the old administrative state is significant. Likewise, the judicial system is primarily designed to realize people's human and constitutional rights. It is only to a limited extent that it carries out the functions of bureaucracy, supervision and punishment. And even then the rights of the individual are of central importance. Thus, at the end of the day, the efficiency of the judiciary and of the judicial administration – the efficiency of IT – should contribute primarily to realizing the rights of the individual and organizations.

However, we would be old–fashioned and behind the time to think of the electronic services being developed today in the narrow terms of court judgements and their enforcement. E–justice encompasses – and should do – a broader and richer range of legal affairs. Moreover, the increasing international character of legal life has added an international perspective to the issue. The present *European e–justice portal* has been dubbed an "access to justice" portal, "conceived as a future electronic one–stop–shop in the area of justice." Much as the free movement of people and goods is important in the EU, so too is the mobility of law and of legal expertise. The e–justice portal is one – but only one – element contributing to this aim. [10] The name of the portal is as such a lot misleading.

In the digital environment of the *Network Society* in which we live and work there is a risk that e–justice will be understood in excessively broad terms. Today, we really live in a dynamic Network Society. The old static Information Society is, or at least should be, a thing of the past. It was a society where we understood computers and networks mostly as tools only – a short step forward from the first age of office automation. Unfortunately, one still sees the term used rather often – even officially.

In the modern Network Society, we – every one of us – are increasingly dependent on access to networks and to the information they contain and services they offer. [11] We can speak

[10] http://ec.europa.eu/justice/criminal/european–e–justice/portal/index_en.htm

[11] See more for example *Saarenpää* Regulating the Network Society. A challenge for the Quality of Legislation and other activities pp 99 in Schweighofer – Saarenpää – Böszörmenyi (eds) KnowRight 2012 and Saarenpää

about a *digital environment*. Society has definitely changed. That is why I would like to speak about the Network Society, not about Information society or Cyber Society. Not everything that is law–related and operates in the digital environment however can be tucked under the concept of e–justice. It is essential that we define the scope of the issue with some exactitude.

I would distinguish a number of perspectives before we embark on this effort: (1) those of the citizen, (2) legal services, (3) the courts, (4) enforcement, (5) the media and (6) IT.[12] They are all important in considering how functional and meaningful the phenomenon of e–justice becomes in the constitutional state where *information law* nowadays is a very important area in legal systematics.[13]

2.1 The citizen's perspective

Central to the citizen's perspective on e–justice is our right to information, which derives from our human rights. This is also one of the core principles of modern information law. We have a *right to know* what is correct. We have a right to know how and where our legal affairs are dealt with and a right to know the grounds for any decisions made that affect us.

This is all naturally an aspect of *transparency* and *openness* in society. In fact, transparency is a time–honoured principle in the Nordic countries, one that has traditionally been put into practice primarily in the form of *public access to documents* and *the publicity of trials*. Both of these practices have been continually emphasized when comparing Nordic and European transparency. When the present Finnish law on publicity in Government was enacted and translated 1999, the name chosen for it in English was the Act on *Openness* in Government Activities, or Openness Act for short. The choice was motivated by Finland's desire, as president of the EU at the time, to stress the importance of openness principle in European society.[14]

Yet, reference merely to the principle of openness easily renders a significant a goodly number of our rights invisible in the *digital Network Society*. From the citizen's point of view, the *path* that information must travel – be it manual or digital information – is a crucial consideration. It is a long one, starting from who information has created and how it is stored

---

Legal welfare and legal planning pp 47–69 in Barzallo – Valdés – Reyes Olmedo – Amoroso Fernándes (eds) XVI Congreso Iberoamericano de Derecho e Informatica (2012)

[12] Cfr. Reiling Information Technology in the courts in Europe pp 601–616, where Dory Reiling also does open different points of view to analyse e–justice.

[13] See about the importance of Information Law already Saarenpää Information and Law in the Constitutional State pp. 443–452 in Traunmüller (ed.) Electronic Government Third International Conference, EGOV 2004.

[14] See more Saarenpää Openness, access, interoperability and surveillance: transparency in the new digital network society pp. 239–248 in Schweighofer – Kümmer – Hötzendorfer (eds.) Tranparenz. IRIS 2014.

on a particular platform and extending to the end of the line, where it is erased, archived or declared secret. Unless all of the stages along this route are implemented properly using the appropriate IT solutions, our right to know may be jeopardized. Where this happens, e–justice is not working, as it should.

A crucial difference to observe here is that we are no longer talking only about the right to inspect traditional paper documents or get copies of them. Citizens should also have *access* – access to information networks and the information systems on them and access to information. We have already, following Art.19 of the UN International Covenant on Civil and Political Rights, begun to view *access to information* and in this connection access to Internet as a new human right.[15] Access to information systems, for its part, is one means by which IT implements transparency.

When talk began of *e–government*, a mentality arose whereby government information systems could – and should – be divided into two categories – *front office* and *back office*. The front office would provide citizens with information and electronic services. The back office was an internal information service for government itself. Applications fitting this description are undoubtedly still out there. In today's constitutional state, they are no longer adequate. As I see it, to be acceptable, systems built in keeping with the principles of *good government* require at least four basic components, or offices: a system information office, a service information office, a service office and a back office.[16]

The system information office should contain the basic information on the software the system uses and how it logically works as well as the basic information on the type of information the system contains. People have the right to know these basic facts. The systems should be more than "black boxes".

The service information office provides general information in a manner that allows citizens to access it without having to identify themselves. We have the right to use government services, including submitting requests for information, *anonymously*. It is only when the information we ask for requires identification of the person asking for it can presentation of some form of identification be required. This principle was very difficult indeed to understand in traditional government.

[15] See also *Sartor* Human rights in the information society in papers.ssrn.com/sol3/papers.cfm?abstract_id=1707724

[16] In Finland, good government is one of our constitutional rights. We have the right to good government.

The service office, as the name indicates, is the component of the information system in which rights are realized when it becomes necessary to prove our identity and perhaps provide additional information.

The back office is the heart of the system, which the average person has no business accessing. In contrast, the service information office – as noted above – should provide sufficient information on how the system works. And, at the end of the day, we always have the right in principle to know who has been processing our data.

2.2 Judicial services

The perspective of judicial services is closely connected to that of the citizen. The focal question here is what kind of electronic judicial services are developed for citizens and organizations. In the constitutional state, these issues, too, must be seen as having implications beyond the courts. In fact, early on, when information systems were developing, thought was also given to databases of legal information. To be sure, the focus then was primarily on the courts. Today, the scope of the issue has been broadened, and fundamentally so, to include the general right to familiarize oneself with legislation. With everyone in a democracy having an obligation to be familiar with the law, it must be made available to everyone as effectively as possible.

I consider this general principle to be one aspect of judicial services. Society must ensure that citizens and government authorities are on equal footing when it comes to accessing the law. Here we can speak of there being a requirement of *information balance*. In a democracy there cannot be secret legislation that is known and accessible solely to government authorities and the courts but no to citizens.

One corollary of this principle is that legislation in the constitutional state should be available free of charge to everyone. There can be no balance of information where the average citizen has to pay for essential information but government officials can access it for free. Progress towards free digital access to legislation has been surprisingly slow, however.[17] Even in Finland legislation did not become available in legal database free of charge until 1997.[18]

A second crucial question where judicial services are concerned is the kind of electronic services the courts and other authorities making legal decisions have and how these services

[17] See generally Bing Legal Information Services: The Policies of Publishing pp 83–95 in Peruginelli – Ragona (eds.) Law via the Internet. Free Access, Quality of Information, Effectiveness of Rights (2009).
[18] See also Saarenpää THE NETWORK SOCIETY AND LEGAL INFORMATION. Some observations from the Nordic point of view. LAW via Internet 2011 papers in www.hklii.hk/eng/Free_Access_to_Law(eng).pdf

are organized. In the European Network Society, the basic assumption is that electronic services are available online. In this vein, the EU assumes in its programmes that access is guaranteed to everyone.[19] The point of departure is that the average citizen has network connections at his or her disposal and that everyone, including disabled persons, can use such connections. This sets significant requirements for quality, for example, in the design of user interfaces.

Being able to initiate an action electronically is a typical basic e–service. Previously there were considerable limitations when trying to do so due to the requirements that a diverse range of original paper documents had to be attached to the documents. Not surprisingly, electronic services have been easier to implement and more widely implemented for so–called summary, standard–form matters than for others. As the technology has improved and it has become easier to convert documents into digital form, electronic initiation of an action matter has become one of the principal ways in which e–justice is implemented. Actions are brought and dealt with digitally to the extent that they can be without the parties being present. Ultimately, this development compels us to think about the extent to which we can relax the requirements of physical presence that a traditional trial mostly imposes.

In the course of this same process, care must be taken to ensure openness where judgements are handed down digitally. We cannot content ourselves a system in which documents flow in the digital environment and no more. Citizens have the *right to know* where and how their cases are being dealt with. I will have more to say on this issue later, when I discuss the Finnish system.

How services are paid for is an issue–area unto itself. Where the idea is to favour electronic services, it readily comes to mind that the costs of proceedings could be made lower where the case is processed electronically. After all, e–justice as a whole is an ambition which should save money. Countering such considerations are concerns for *equality* among citizens. E–services are not necessarily an option. At least as yet not everyone has e–services available. This being the case, having costs differ depending on how proceedings are initiated would mean inequality. That would be difficult to endorse.

Deadlines and requirements of form have as a rule been essential elements in the realization of our rights. Although the range of actions that can be taken without deadlines or strict requirements of form is now greater, the transition to e–services rather often requires in practice that deadlines and requirements of form be imposed. Another typical change that has

[19] Directives 2002/19/EC and 2009/136/EC

occurred as part of the transition to e–services has been to set the end of a 24–hour period rather than the end of traditional business hours as the deadline where there is a deadline to be met.[20]

One basic condition if e–services are to function properly is *interoperability* of the software used. Public officials should be able to process the materials they receive appropriately. And, by the same token, citizens should know what software the officials are using. A few years back this was quite a serious problem in Finland.

Another key issue, one meriting particular emphasis here in this connection, is the importance of *information security*. E–justice is an area where information security should be of a higher calibre than in ordinary operations. The main rule is straightforward: services should be offered via a protected network connection whenever the maters of an identifiable individual or organizations are involved. In Europe, the *data protection legislation* in fact imposes this obligation.

Identifying a client is yet another basic problem in providing e–services. I will return to this issue later.

2.3 The perspective of the courts

Presentations of the development of e–justice typical focus on the technology involved. The journey from the initial phases of office automation to extensively computerized courts has been long one – and many countries still have quite a way to go. It has taken time even for the questioning of witnesses via video link to become routine. Then again, particularly in the United States, sophisticated *electronic courtrooms* have been used for years. The famous project Courtroom 21 and the related Courtroom Information have been the principal drivers of this development. Everything that can be done electronically and over a network is done that way. Proceedings become paperless. All the parties may use IT. One could of course say that the technological imperative is at work here, but all in all Courtroom 21 has been a rather successful step forward in combining law and technology.[21]

But computerizing the courtroom or court as such is only one facet of implementing e–justice. A court is merely one component in a larger network. It receives and sends information. This observation, simple as it is, necessarily prompts the question of how this information is transmitted. This in turns forces us to think of the basic issues relating to the *interoperability* of technology and content. When information is transferred, it should retain its form and content,

[20] Following old administrative traditions, we still can sometimes find practice, where bureaucracy is using its own time limits.
[21] See more in www.law.wm.edu/academics/intellectuallife/researchcenters/clct/

with no extraneous material coming into the court being passed on by it. Ensuring this requires sophisticated planning of the relevant information systems and documents.

The core issue here is who uses the information systems in a court and how. If the users are primarily assistants among the court staff, true e–justice will never be achieved. At best, we can speak of advanced office automation. Where the most important users will be judges, planning and building systems poses a very demanding task indeed. The systems have to support the judges in making their decisions and, at the same time, save them as much as possible from having to do routine technical tasks. This is where various *expert systems* might come into play. The old, often wrongly formulated question of whether a computer can replace a judge is addressed effectively by having systems include expert systems that support judges in their work. Where this occurs, it contributes a great deal to modelling the work of court – the basic idea of an expert system.[22]

Earlier, I mentioned the importance of *information security* when e–services are being offered. It is every bit as important – if not more so – where the work of a court is concerned. The information security systems of a court must be more sophisticated than average. The greater the progress towards e–justice, the greater the demands on information security will be.

An electronic court produces electronic documents and messages. Word–process has given way to document systems. They make it possible to produce partially different documents for different purposes, offering a technical solution for protecting personal data and confidential information. For this to work, however, we have to design documents designed with their legal function in mind and the embrace the concept of a *dynamic document*; dynamic for different purposes The era of working with nothing but static paper documents should be well behind us when planning systems geared to e–justice.

2.4. Enforcement

Another necessary and natural facet of e–justice is that it should facilitate enforcement of judgements, in particular those in criminal proceedings. It would be odd indeed in such cases to leave enforcement dependent on manual information. As we already have e–justice systems in place that can handle distrait orders and other decisions, adding court judgements, or any other new elements, to the mix calls attention to the importance of interoperability. The systems in use in different organizations must have a sufficient degree of interoperability. No doubt this

[22] Cfr. Lauritsen Liberty, Justice and Legal automata in address http://www.kentlaw.iit.edu/Documents/Institutes%20and%20Centers/CAJT/88–3_09_Liberty_Justice_and_Legal_Automata.pdf

requirement will cause bureaucratic problems in different countries, as meeting it will involve a variety of officials having to work together.

2.5 The media

Transparency in society very much includes the right of the media to obtain official information. This can be – and has been – handled in many ways in different countries. The electronic administration of justice opens a new realm of opportunities for the media, too.

The principal issues here are clearly access to the document systems used in the administration of justice and the possibility of following the work of the courts and other authorities more or less in real time. These are questions of both transparency and, ultimately, the economic viability of the media.

The concept of a dynamic document, which I have mentioned earlier, figures crucially here. Transparency can be served adequately by making use of documents prepared for the media that do not contain personal data or confidential information.[23] Press releases are a different matter.

2.6. Information technology

Any discussion of e–justice must always consider the perspective of IT. By this I mean questions of the quality of information systems, their usability and who is responsible for supplying them. One paradox of in the development of administration is that technological considerations have often been overlooked even as society has become increasingly computerized. The end result in Finland, in addition to problems with quality, is that we work with a collection of information systems that that to one degree or another fail to work together properly. Similarly, we were very slow to notice the role software with closed and open source code plays in public administration. Among the other basic problems, we face, in addition to interoperability or a lack of it, are issues in principle and in practice that have to do with the geographical location of bodies of information and the outsourcing of operations. I will take these issues up later.

[23] In a report that I prepared for the Finnish Ministry of Finance in 2009, I submitted that we should effect an urgent transition to the era of dynamic documents. This has yet to occur, although at the beginning of 2011 the Ministry of the Interior changed over to electronic document production in which paper documents are a secondary alternative to electronic ones. This change was not accompanied by any re–assessment of the concept of a document, however.

3. E–justice in Finland

3.1 Background

Describing e–justice as a whole in Finland would require a far more extensive topic. Today we are unequivocally bound to our digital environment and networks. Given this dependency, I no longer speak of the Information Society. That is an era past. We live in the *Network Society*, in which the role of IT is no longer that of a mere tool. We have to take our digital environment and the use of information systems into account in all legal planning and in legislation as well.

The first thing to mention where legislation is concerned is for key laws that affect the development of e–justice. These are the Act on Information Management Governance in Public Administration, the Act on Electronic Services and Communication in the Public Sector, the Personal Data Act and the Openness Act. These are all general laws but have a significant impact of the administration of justice.

The Act on Information Management Governance in Public Administration, enacted in 2011, is legislation which – at long last – tried to rein in and manage the scattered software and systems develop in the public sector. It also made interoperability of systems a key objective; today this can be considered self–evident. The first section of the Act describes this aim well:

The purpose of this Act is to improve the efficiency of activities in public administration and to improve public services and their availability by laying down provisions on information management governance in public administration and on promoting and ensuring the interoperability of information systems.

Today, the Act provides a framework for building a new *comprehensive architecture* for information management in government. The issue thus goes beyond merely concentrating purchases of software. The aims are compatibility, comprehensive architecture, information security and, in the final analysis, cost savings as well. Thinking of and purchasing information systems and software applications as separate tools has cost the country millions of euros in money and working time. I have many times pointed out that the Act came into force 30 years too late. But we might not have it even today if the *National Audit Office* had not urged the powers–that–be to start the drafting process. This move is a good reflection of the new relationship between public finance and IT solutions in the Network Society. [24]

[24] The Auditor General, doctor of law Tuomas Pöysti has been very active to analyze the quality and economy challenges of the new digital government. He himself discussed about information law already in his doctoral dissertation 1999. See more about the National Audit Office in the address: www.vtv.fi/en.

The Act on *Electronic Services and Communication in the Public Sector* was enacted already in 2003. It was considered essential given the significant growth of electronic services that had occurred. The point of departure in the law is the obligation of any government authority to develop easy–to–use e–services. Information security was another objective of the new legislation. The section setting out the objective reads as follows:

The objective of this Act is to improve smoothness and rapidity of services and communication as well as information security in the administration, in the courts and other judicial organs and in the enforcement authorities by promoting the use of electronic data transmission. The Act contains provisions on the rights, duties and responsibilities of the authorities and their customers in the context of electronic services and communication.

Among other things, the Act lays down provisions on the division of responsibility in cases where communication fails, on how deadlines are calculated and on the obligation of an authority to send notifications that messages have arrived. The principle is that the sender is responsible for communication. The main rule as regards the arrival of answers requested by an authority is that the deadline is the end of the day in question; in other words, the law has embraced the principle of 24–hour service. Another interesting provision is that an authority has to notify the sender of a message immediately after the message has arrived. One way in which this can be done is to send an automatic delivery receipt. In practice, this obligation to notify is neglected very often indeed.

Another important point in the law is its position on the importance of signatures. The traditional mentality tells us that a document acquires meaning only when it has been signed. In keeping with this, legislation makes provision for electronic signatures, the use of which is governed by the *Act on Strong Identification and Electronic Signatures.* In practice, however, a digital signature proper is replaced by electronic identification when logging on to a service. Then again, the Act on Electronic Services gives citizens the option of not having to use an electronic signature. One is not needed if there is no uncertainty regarding the sender or no doubt concerning the origin or integrity of a document. This provision does, however, not entitle a person to an exception from the main rule when a signature is required by law.

At this juncture, I should mention that Finland introduced an *electronic identity card* back in 1999. The card is still in use but users are quite few. The reason for this is simple. People had to pay for the card and had to have a reader for it on their computer to use it. As banks already had their own identification systems up and running at the time, the identity card simply could not compete. Not surprisingly, today one can log on to most public–sector services using bank codes. On the other hand, in a democracy, everyone should have a right to a digital identity

issued by the government. It is peculiar for a person to have to resort to systems provided by commercial actors to prove his or her identity when using a public service.[25]

3.2 Citizen's account

One interesting administrative solution is the *citizen's account*. It is one of the infrastructure services provided by the government. The account makes it possible to receive services and decisions from authorities through a secure connection. It is thus in principle a channel providing services with proper information security.

Unfortunately, the citizen's account is not available in the case of all public services. Only some authorities have adopted the system. Most are municipalities. In the area of e–justice the principal services are contacting the police and being able to obtain decisions on public legal aid electronically.

The idea of a citizen's account is an excellent one. Unfortunately, the authorities in the public sector have not been required by law to make it available. The legislation merely states that the citizen's account is one possible electronic service. For this reason, only some authorities have made the service available.

The next step in Finland will be the national data exchange layer. Estonia started to build this kind of X–road infrastructure already 2001.[26] Now even some other countries have followed the Estonian way. It should be open possibilities to flexible data exchange between different public sector offices and citizens and to be much more effective than citizen's account.

3.3 Legal information maintenance

Legal information maintenance typically refers to the body of measures and activities designed to produce, maintain, develop, market and store legal information forming a legal information resource. Law, being communication, requires effective maintenance if it is to function properly.

It is essential to the work of authorities in general and courts in particular that the official sources of law are available in as up–to–date a form as possible when decisions are being made. This basic premise was the impetus for establishing the national databank Finlex in 1980. At the time, the only materials available were the headnotes of precedents handed down by the

[25] At the end of 2014 government gave to parliament a government bill where the main idea is to collect acceptance of different commonly used digital signatures under a common administrative "umbrella" managed by the state Population Register Centre.
[26] See more in address: e–estonia.com/component/x–road

Finnish Supreme Court. The legislation component was purchased later from a private company. Later on, in the 1990s, Finlex came to include 30 different databases with materials ranging from legislation to precedents and drafting documents. But they were only available for a fee. Individual practicing lawyers and small law firms could not afford to use the service extensively. Use was free of charge for the courts. This was the how things went at a time when there was a serious information imbalance.

The first steps of Finlex as a free service were taken in 1995, when we decided to open up the information in *Parliament* and make it available free of charge online. Drafting materials could be accessed for free. The next step was to open Finlex and make it free of charge. It consists of which an electronic collection of statutes, consolidated legislation, the full text of Supreme Court precedents, summaries of Court of Appeal judgments, summaries of certain decisions of government authorities, translation of legislation and a number of other legal databases.[27]

One of the basic tools in the databank, used in everyday legal life, is the database of *case–law in the literature* (FOKI). It contains information on where in printed legal literature a particular case has been cited. The value of database, maintained for almost the last 20 years by the Institute for Legal Informatics at the University of Lapland, could be described by saying "Someone is doing your reading for you". We maintain the database as a service of the Ministry of Justice, for the needs of the courts in particular, but it is available to everyone and free of charge, like the other databases in Finlex. I for one am of the view that in the modern constitutional state a database like this is not only a useful, but an utterly essential, component of legal information maintenance. It serves the needs of practicing lawyers as well as researchers.[28]

Another important part of Finnish legal culture, one that will soon have been with us for 60 years, is the collection of statutes known as *Suomen Laki*. Initially it was a printed work for practicing lawyers comprising a systematic collection of the most important statutes. It contained the text of the laws, information on the history of their enactment and, section by section, information on relevant precedents. Today the work is published in both print and electronic form. Being an edited legal work, it is a commercial product, not free like Finlex. Added value has a price.

[27] See more Saarenpää Towards legal information and legal knowledge: some basic issues in Finnish perspective pp 509–525 in Magnusson Sjöberg – Wahlgren Festskrift till Peter Seipel (2006)
[28] At the end of 2014 there were in FOKI together 865.000 notes to 140.500 cases.

Although Suomen Laki now has a commercial rival, it can be found on the desk of virtually every practicing lawyer. Professor *Kauko Wikström* put things most appropriately when he wrote about the "open the law book doctrine of the sources of law". A law book has become a primary source; often, it is considered sufficient as well. A considerable number of legal matters are simple enough that a good lawyer can identify the problem, and often solve it as well, using a law book. The problems arise when we need more information.[29]

3.4 Judicial court information systems

When examining the information systems used by the Finnish courts, it should be pointed out at the outset that Finland took a considerable step forward in the early 1990s. In December 1993 every Finnish judge was given the opportunity to personally use a computer in his or her work. At the same time, they began using the information system TUOMAS, designed for civil cases and providing for processing information and sending it on. At the time, we were one of the world's most advanced e–justice countries. This was noted at the extensive meeting of the Council of Europe held in Ankara, Turkey, in 1992. Finland, Norway and Austria were at the cutting edge of development.[30] Later in the same decade, in 1996, a largely corresponding system for criminal cases, SAKARI, was taken into use; however, it did not support judges as much in producing judgments as much as TUOMAS. [31]

SAKARI was replaced in 2012 by a system known as RITU, which was supposed to be more clearly geared to helping judges draft judgments. Although efforts were made to design RITU so it would function smoothly and effectively from the user's point of view, the project and the introduction of the system were less than successful in some respects. In fact, the largest district court in the country, Helsinki District Court, issued an assessment at the beginning of 2014 saying that use of the RITU system reduced the efficiency of the court's work by as much as *one third*. The principal technical problems cited were shortcomings in the user interface and even the lack of an auto save function. Test of the system had used sample cases that were too simple. But another factor involved here was considerable resistance to change, particularly among the senior management of the law courts.

---

[29] Originally, Suomen Laki was a joint project with the Ministry of Justice and Finnish Lawyers Association. Nowadays Ministry of Justice is cooperating with Edilex company. That state owned company is also publishing a commercial law collection.

[30] Morten Hagedal has the opinion, that Norway had been number one. When participating that conference, I could however see that Finland and Austria were at top. Cfr Hagedal IT in the Norwegian Courts p. 77 in Oskamp – Lodder – Apistola IT Support of the Judiciary (2004).

[31] See more: Hietanen E-Justice in Finland – Trends and Challenges pp 757–770 in Gottwald (ed), Festschrift für Martin Schneider: neu bei Editions Weblaw (2014).

A new system, AIPA, is being built and efforts have been made in the process to avoid the planning problems that plagued RITU. AIPA is an electronic database containing all the documents related to a judicial matters dealt with by prosecutors, district courts, courts of appeal and the Supreme Court. All officials with access to the system may use these documents in their work.[32]

AIPA is a particularly interesting and novel e–justice system in four ways. Firstly, it is a system which should force a judge to sit at a computer. Previous systems and the ways in which they were used gave judges the option of having clerical staff be the ones sitting at the terminal. Now the system is being designed such that it must be primarily a judge who is the user.

Secondly, efforts are being made to implement the system such that the flow of information can be managed within the same application from the point where a case becomes pending to when it is electronically archived. This feature requires extensive interoperability among the system used by different actors. For example, the flow of information between the police, prosecutors and the courts will have to be ensured using interoperable solutions. In this area we have been behind certain other countries.

The third fundamental principle in the system is that the system makes available to judges in a flexible fashion all the basic materials they need technically in the process of making a decision without having to act as support staff as well. Here the design of the user interface plays a crucial role. Then again, planning must still take into account the need to use support staff to some extent.

The fourth key feature actually derives from what was said above. It is the idea of paperless judging.

It has been estimated that the planning and completion of AIPA will take five years. Work on the project began in 2014.[33]

In this connection it should not be forgotten, however, that knowledge management in the courts has had to be, and will have to be, laid down in the law. A law was enacted in Finland on a national information system for judicial administration[34]. The legislation specifies how materials produced by the courts are processed and how information on those materials is made available.

---

[32] All administrative courts are still outside this system.

[33] Unfortunately, there are not any idea to combine this ICT project and modernization of procedural rules. It seems to be so, that the historical divide between ICT and procedural legislation will be a negative burden in the modernization. Cfr. Harsági Digital Technology and the Character of Civil Procedure pp. 122–133 in Kengyel – Nemessányi (eds) Electronic Technology and Civil Procedure New Paths to Justice from Around the World New Paths to Justice from Around the World (2012).

[34] Information systems Act: Act on the national information systems of the law court administration (2010).

The starting–point in the law is the obligation of the courts and other authorities to connect to the system and supply information. This in itself is nothing new, because the established view in the centralized Finnish judicial system has been that it is a ministry that decides on information systems and the communications infrastructure. Nevertheless, given the increasing importance of the information system, it was considered necessary to set things out in the law. At the same time the legislator took a position on the processing of personal data in the information system used in judicial administration. The upshot of this was that the *Data Protection Act*, as a general law, proved to be ill–suited for the system.

With regard to decision making, enactment of the law could be readily criticized for its opening up the possibility of joint use. The law allows one court to access the documents of another through a technical connection. At the same time, separate provisions were enacted on the publicity of court proceedings that allowed courts other than the one hearing a case to access trial documents that had otherwise been deemed secret. These changes were justified in the name of achieving consistency in the judicial practice. The changes signalled an exception to the basic principle that consistency in judicial practice derives from the decisions of higher courts. At the same time, there is a danger that the information being processed becomes detached from its original context and is understood.

Typical elements of electronic proceedings have been the hearing of witnesses and parties over the telephone or other link. These procedures were late in being adopted in Finland and are still used rather rarely. However, their importance is growing, particularly in hearing experts. For example, in the case of doctors, the procedure no doubt brings significant savings and avoids disruption of the work of healthcare facilities.

Everything that I have discussed here pertains to proceedings in *general courts*. In administrative courts and the different boards, we have, progress has unfortunately been slower. Accordingly, I have chosen not to deal with them here.

3.5 The media

The Finnish principle of *openness* has been an instrumental element in the work of the Finnish media. Earlier, the traditional public access to documents also served the media quite well. Information on pending court cases, which could be obtained from the court register, was a valuable source. In the digital environment the media became interested in the possibility of getting a technical real time connection to the register. This was arranged when the *Information Systems Act* was enacted. The right was extended to cases that would be coming before the

court within a month. This expansion of the rights of the media, a significant one in almost anyone's estimation, did not spark much in the way of debate.

On the other hand, in Finland the publicity of court proceedings does not mean that the media are allowed to take photographs in or send direct television broadcasts from the courtroom. At the beginning of a session, the parties may be photographed for a period of time decided by the judge presiding over the proceedings. The upshot of this is unfortunately that most of the trials that interest the media begin with the accused covering their face. This detracts from the status of the proceedings in the public eye. In fact, the trials take on a grotesque twist rather than being the dignified proceedings people have come to expect.

Another side–effect of this development is that the prosecutors, parties and, to a lesser extent, the attorneys involved provide comments outside the courtroom on ongoing proceedings. *Trial by newspaper* has been replaced by *trials stage–managed by the media in the corridors of the courthouse*. This is a regrettable development. Informational justice is in a danger zone.[35]

4. Conclusion

E–justice is clearly an important societal matter. The administration of justice simply must keep up with developments in IT in society. But, by the same token, it must not leave itself open to the detrimental effects of the technological imperative. E–justice is a far more challenging sector than most when it comes to the application and implementation of IT solutions.

In Finland, courts have traditionally worked under the *Ministry of Justice*. Although they are independent in making their decisions, the Ministry is in charge of the development of judicial administration. Recent years have seen increased support for the idea that Finland, like the other Nordic countries, would have a centralized, independent judicial administration. However, the ministry of Justice is still responsible of e–justice.

In 2013, an *advisory committee* appointed by the Finnish Ministry of Justice released its proposal for developing the administration of justice in Finland in the period 2012–2025. The programme outlined by the report describes the development of information systems and the impacts of those systems as significant. These are seen as part of other development activities. But the issue has to be seen in broader scope that merely the development of IT. The advisor committee expressed particular concerned about the slow development of IT in the

[35] About the idea of the informational justice see more Hoeren Eine kontraktualistische Konzeption der Informationsgerechtigkeit; Rechtstheorie 34 (2003), pp. 333 – 345.

administrative courts. Further, one prominent theme was the development of electronic services with a focus on the perspective of the average citizen.

The objectives put forward in the committee's report were given a largely favourable reception. Indeed, the Finnish AIPA system, now being built, is undoubtedly one response to the committee's recommendations. One thing I, as a teacher of Legal Informatics, would like to have seen in the report is a clear new realization of the need to train a new breed of *digital lawyers*, lawyers who no longer see information systems as mere tools. Such considerations are however lacking for the most part in the report.

Legal decisions are – with perhaps some simplification – a matter of combining facts and knowledge of the law. If knowledge of the law is deficient or wrong, the facts may lose any significance. Professor *Peter Seipel's* now time–honoured statement on the *critical importance of legal information retrieval* in legal life looms more important than ever as the quantity of legal information increases.

Achieving and maintaining a balance of information among the parties – and the judges – in court proceedings is one of the cornerstones of a fair trial. And this is a crucial consideration in efforts to develop a judge's workstation. The business of the judicial administration cannot include limiting the sources available – literature for example – before proceedings even begin. This is one of the principal challenges e–justice faces in the near future. What can a judge see and seek when opening his or her terminal? He or she must be a good digital lawyer in the new digital environment.[36]

I began this presentation by mentioning a number of people who have influenced developments in Finland. I will conclude by mentioning again judge *Martti Leisten*, former president of the Rovaniemi Court of Appeals. His motto was '*panta rei'* – everything flows. This remark, which can be attributed to *Heraclitus* of early antiquity, is extremely important to bear in mind in today's constitutional state. The systems developed for judicial administration must be dynamic and easily upgraded yet at the same time systems that unfailingly respect citizens' rights.[37] Sluggish progress in developing huge information systems and conservative lawyers are a very bad combination in trying to develop the modern constitutional state connected to the digital environment. Let me close this paper when telling one sad example:

[36] Professor Ethan Kash wrote already many year ago: "Yet, the digital lawyer will be employing a broader range of skills and an outlook that reflects not simply what the new technologies do but the manner in which they do it." See Katsh Digital Lawyers: Orienting The Legal Profession To Cyberspace, 55 Pitt Law Review (1994) p 1169.

[37] See also Prins A balancing Act pp. 401–413 in Wiese Schartum – Bygrave – Berge Bekken (eds.) Jon Bing En hyllest /// A Tribute (2014) and Pöysti Information Government in Practise: Functional Gains and Legal Perils in Scandinavia Studies in Law (2010) pp 91–124.

Several but not so many years ago, I was talking with a young judge about how some judges were found to have trouble deciding copyright cases involving software and online music distribution. The judge, who held a doctorate in law, saw nothing strange in this situation. He pointed out that these were such new issues. We should not wait for expertize in new phenomena.

THE ELECTRONIC PAYMENT PARADIGM – BETWEEN TRUST AND CRIMINALITY

Vlad Dan Roman

Research Trainee (August–October 2014) – Institute for Law and Informatics, University of Lapland, Rovaniemi, Finland, roman_vd@yahoo.com

Keywords: ***virtual currency, bitcoin, criminality, innovation, payment system.***

Abstract: *Technological evolution has always challenged individuals to rally their social rules and way of interaction to the new instruments that have been developed over time. This way, the projection of technology in one's daily existence represents the leitmotiv of our era and also, a certainty for the next ages. However, as the process per se is governed by a great dynamic, individuals face changes at a much higher peace, fact that exposes them to more and more vulnerabilities. This is as well the case of payment instruments, area in which individuals have evolved from very rudimental barter transaction to digital modern currencies. The concept of a two–edged sword represents the best analogy for introducing the idea that great innovative achievements might, besides great evolutionary effects, have the potential of being misused for antisocial purposes.*

1. Structural and methodological stance

The paper analyses from a legal perspective the way in which modern societies tend to replace conventional financial forms with new ones. It is designed as a case study on a very actual topic, namely modern, decentralized virtual currencies; in the same time, it is not referring to the centralized ones (i.e. issued on receipt of founds), which are already subject to regulatory frameworks in many jurisdictions and seen most often as money transmitters.[1] When exemplifying, I shall use the case of Bitcoin, which has been the world market leader and the most notorious alternative to fiat currencies.

The structure shall fallow a logic of causality. It will first of all introduce the idea of decentralized virtual currencies (i.e. cryptocurrencies[2]) and continue with the actual regulatory *status quo*. Afterwards, it shall develop on the consequences deriving from the current, mostly European, state of affairs and will analyse possible remedies for the problems. Finally, the author will have his own concluding remarks. Considering semantics, it must be emphasized that decentralized virtual currencies are to be found in the paper as: virtual coins, digital coins,

[1] FinCEN, Guidance – Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (2013) seen on FinCEN's webpage, p. 4 on 2014.09.01.
[2] Intermediary used in trade that relies on cryptography in order to secure the transactions and to control the issuance of new units.

modern virtual currencies, digital currencies, cryptocurrencies or just simply, virtual currencies, all of them describing the same idea.

When it comes to the research, it is primarily based on empirical evidence (doctrine, media sources), mostly qualitative, as it considers the substance of the information and also analytical due to the fact of interpreting legislation, case–law with the aim of proposing a feasible solution. Furthermore, as the author analyses an ongoing process, most of the used sources are very recent (i.e. from 2014).

Also, it must be said that the realistic–technological model of legal dogmatics is the main method used. This implies that the writer chooses a state of affairs as the most desirable and offers arguments sustaining that a certain legal policy is suitable to achieve this outcome.[3] However, the first part the work will be more descriptive as there is a clear need to present the 'starting point' – actual *status quo* – both, *de jure*, in a systematic way and *de facto,* as an aftermath of the current legal situation and the author's view will mostly be presented in the final section.

2. Introduction

The world as we know it today represents the sum of humans' evolutionary achievements; if we are looking at this century's peace and at the ongoing trends, it is for sure that the living paradigm of the generations to come will be based on more and more change. Moreover, as innovation will increase at an ever larger scale that what we are experiencing it today, it can be presumed that societies shall need to adapt their lifestyle to a more dynamic rhythm characterized by short and many transition periods between the new and the ultimate.

Novelty is for sure present in more and more areas from our existence and one example is being represented by the way in which we used to understand trade and the different perspective we share nowadays. For example, in the ancient times people used non–monetary techniques, like barter, as goods were exchanged for other items of an equivalent value.[4] The attribution of trade value to an otherwise conventional object such as a coin or a trade bill grew as individuals and their trading partners developed a 'psychological aptitude to place trust in each other', trend that grew as individual understood the system's benefits (e.g. re–usage as an alternative to the idea of coincidences of wants).[5]

[3] Álvaro Núñez Vaquero, 'Five Models of Legal Science', *Revus*, No. 19 (2013), p. 70.
[4] Jack Weatherford, 'The History of Money', (*Three Rivers Press*, New York 1997) p. 32.
[5] David Kinley, 'Money: A Study of the Theory of the Medium of Exchange', (*Macmillan*, London 1904) p. 48.

Going further, this way of mutual trust has evolved nowadays in more institutionalized and regulated shapes, namely currencies. Today there are 168 officially recognized currencies[6], which are being backed and regulated by national banks and domestic governments. Furthermore, as the financial markets have been subject to progress in the past years, there are also supranational institutions that have attributes in this resort.

In concreto, national banks configure and implement the monetary policy, issue coins and banknotes that are used as legal tender or 'oversee the smooth operation of the payment systems with a view to ensuring financial stability'[7], while domestic governments develop financial policies with the purpose of assuring economic stability and monetary strength. In the same time, there are external agents that might contribute to this financial logic; exemplifying, it is the case of the European Central Bank which manages the euro and gives authorization to central banks within the Eurozone to remit euro banknotes;[8] the coins and banknotes, no matter which currency they belong to, can afterwards take the form of e–money which basically represents the electronic storage of cash on a payment card.

On the other hand, the recent years came with an alternative to the legal tender regime as we used to know it. By giving primacy to an innovative pattern, private companies have constructed an electronic monetary system which comes to compete with the traditional one; so far, there are more than one hundred undertakings (Bitcoin, Litecoin, Namecoin etc.)[9] that provide this service; however, the system started growing in popularity ever since 2009 and tends to identify itself with the worldwide biggest market player which is Bitcoin.[10]

The most important difference between real currencies and virtual 'currencies' is that the last are not publicly administrated as the classical financial policies are replaced by a mathematical formula that is used to guarantee the system's functionality. However, even though virtual currencies are being generated in digital format they are not the same with e–money as they are created without being backed by conventional, fiat money.

Lato sensu, digital currencies can take several models: centralized, where all transactions take place through an intermediary and decentralized, 'where the network distributes transactions between nodes of a network', the case of Bitcoin and Litecoin.[11] However, as

[6] *Currencies* seen on XE Currency Converter's webpage on 2014.08.08.
[7] *The National Bank's objective and role*, seen on Romanian National Bank's webpage on 2014.09.03.
[8] *European Central Bank* seen on European Union's webpage on 2014.09.02.
[9] *List of all cryptocoins* seen on Bitcoin Talk's webpage on 2014.09.02.
[10] Simon Barber, Xavier Boyen, Elaine Shi, Ersin Uzun, 'Bitter to Better – How to Make Bitcoin a Better Currency', *Lecture Notes in Computer Science*, Vol. 7397, (2012) p. 399.
[11] Danton Bryans, 'Bitcoin and Money Laundering: Mining for an Effective Solution', *Indiana Law Journal*, Vol. 89, No. 441, (2014) p. 443.

mentioned in the first section, of interest for this study is only de second category of digital coins.

Decentralized virtual currencies became more and more popular because of the advantages they bring. It is for sure that consumers will always seek cheap, fast and easy money transfers, all qualities developed by the digital currencies' networks. Being able to avoid both, the 'unfriendly' banking transfer fees and the limited schedule, all of this backed by the possibility of easy value carriage (e.g. memory stick, hard drive) increases for the new products.[12]

In the same time, the fact that users are anonymous represents a safety net for the ones involved in transactions; this is the situation in matters involving account freeze as the secrecy prevents individuals from having their account values seized by third parties.[13] The same thing can be said about identity theft, crime that has lately been the preoccupation of the European Commission due to its growing character. In this second case, the absence of identification makes a possible theft lack object as no personal data is being shared while transacting.[14]

Besides the typology of consumers that use such payment networks for sole money transfer purposes, there is another category of individuals which understand the financial potential of the system and which invest in the digital currency *per se*. As the system becomes more and more popular and the cash flow increases, the exchange rate raises proportional with their financial benefit. For example, in 2013, the value of Bitcoin increased 8,000% fact which made investments from 2009 humongous profitable.[15]

If this is the most desired *status quo,* on the other hand, besides the great achievements for their daily existence, novelty might also expose the users to several vulnerabilities given, first of all, the relatively low level of consumer emancipation (i.e. literacy) in comparison to the innovation rate and, second of all, the possibility of miss usage for criminal purposes. It shall however be seen in the later sections how the reverse of the medal takes place.

---

[12] *Bitcoin: Decentralized, Peer–to–peer, Cryptocurrency* (2011) seen on Stanford University's webpage on 2014.09.03.
[13] Ibid.
[14] *Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft* (2012), seen on European Commission's webpage on 2014.09.03.
[15] *Price of Bitcoin Surges Past $1,000, up 8,000% in One Year* seen on Techvibes's (2013) webpage on 2014.09.03.

3. From classic to dynamic

As it has been previously mentioned, virtual currencies represent a medium of exchange accepted by the members of a particular online network. In more technical words, it represents a 'software–based online payment system that has its own currency' that, nowadays, compared with the incipient (centralized) forms of digital money, has no central depository and no single administration. The network software is designed for the creation of a specific number of coins, which users get on the basis of 'solving some system number crunching tasks – procedure called mining'.[16]

Having this as a premise, transactions and the issuance of digital coins are carried out in a collective way by the network *per se*; afterwards, the coins can be sold or exchanged for fiat money or used to purchase goods and services from providers that accept them as payment instruments.[17]

The whole financial policies and regulatory measures imposed by a sovereignty or supranational entity are being replaced by a mathematical formula which is meant to assure the network's functionality (e.g. avoidance of inflation). Citing from the doctrine, 'rather than relying on confidence in a central authority, it depends instead on a distributed system of trust'[18] in which the state does not have any contribution or influence.

4. Controversial nature

The novel technological approach implemented in the creation and use of the new types of digital money generated several views when assessing on its legal nature.

Having regards to the European Union, which is the primarily area of interest for this study, it can be said that one of the most important positions came from 2013 and belonged to the German Finance Ministry which assumed that 'virtual currency is not e–money or foreign currency but is still a financial instrument.' Later on the same year Irish Revenue Commissioners considered that, 'bitcoins have elements both of a commodity and a currency' while in early 2014 Swedish Tax Authority representatives had the view that Sweden is 'likely to view virtual currencies as an asset, like art or antiques, and not currency.'[19] On the other hand, Finland had a different approach than its neighbours and, through its Central Bank, stated

[16] *How does it work* seen on Bitcoin's webpage on 2014.08.10.
[17] Ibid.
[18] *Bitcoin under pressure* (2013) seen on The Economist's webpage on 2014.09.03.
[19] Perkins Coie LLP (2014), 'Virtual Currencies: International Actions and Regulations', seen on Perkins Coie's webpage on 2014.08.14;

that ‘Bitcoin is not a currency or a payment instrument, but is more comparable to a commodity.[20]

In some countries where financial or political institutions were silent, it was for the judicial authority to impose its point of view. This is the case in the Netherlands where, a district court in a civil case ruled that digital coins ‘like gold, are a medium of exchange that is an acceptable form of payment in the country but that cannot be defined as legal tender, common money, or electronic money.’[21] This definition is close to the one given by Finland or Ireland, as it fits the description of commodities, point of view that seems to be embraced by more European and worldwide states.

It is the case of the United States of America as well where, after a controversial Texas judgment in which bitcoins were seen as 'a currency or form of money’ due to the fact that they ‘could be exchanged for conventional currencies and used to purchase goods and services’[22], in May 2014, the US Internal Revenue Service clarified the situation and decided that virtual money 'will be seen as property and treated similar to any other valuable commodity.'[23]

Summing up, it can be seen that consensus has been reached when differentiating virtual currencies from real money; also, the lack of coherence when it comes to the actual nature seems to disappear as, in the Organization for Economic Co–operation and Development’s view, more states perceive this new financial instrument as commodity.[24]

Anyhow, from a broader perspective, things are far from being settled in this matter and this also happens because there is still a lack of harmonization at the European Union level. As it will be seen in the next section, few legal loopholes are enough to permit virtual currencies escape the regulatory framework.

5. (No) Regulatory framework

Within the European Union the main piece of legislation dealing with the digital equivalent of cash is the ‘E–money Directive’[25], which has been enacted in 2009, time when the nowadays big virtual currency networks were just initiating their activity. Even though, as

[20] Ibid.
[21] *Regulation of Bitcoin in Selected Jurisdictions* (2014) seen on The Library of Congress’s webpage on 2014.09.08.
[22] *‘Bitcoin is a currency': Federal judge says the virtual cash is real money* (2013) seen on: NBC’s webpage on 2014.08.16.
[23] *IRS Rules Bitcoin Is Property, Not Currency* (2014) seen on Techcrunch’s webpage on 2014.09.08.
[24] Adrian Blundell–Wignall, ‘The Bitcoin Question Currency Versus Trust–Less Transfer Technology’, *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37 (2014) p. 12.
[25] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, OJ L 267/7.

mentioned before, virtual currencies undertakings are not considered to be electronic money institutions, the European Commission, when sending its proposal, codified in the recital that 'the definition of e–money should cover […] not only all the electronic money products available today […] but also those products which could be developed in the future.' Having this as a starting point, it can be seen that it was aiming for a broad, *lato sensu* definition, which would also include other possible financial instruments that were to be developed in the future years. This safety net would have been a good compromise meant to avoid future regulatory gaps fostered by the difference in pace between the very fast innovation cycles and the quite lengthy and bureaucratic legislative bargains.

However, even though the Commission embraced a visionary way of making legal policy, in the European Union jurisdiction the recital is perceived as soft–law, non–legally binding, which most of the time has interpretative value upon the actual hard law provisions, which are the main articles.[26]

In our case, the Commission's primarily will be diluted even beyond the possibility of having it as an interpretative tool due to the fact that, after the procedure in front of the Parliament and EU Council, article two came with a very clear and exhaustive definition, fact which leaves no place for ambiguity or interpretations. Citing, 'electronic money means electronically, including magnetically, stored monetary value […] which is issued on receipt of funds for the purpose of making payment transactions […] and which is accepted by a person other than the electronic money issuer.' As it can be seen, there are three cumulative – *sine qua non* – conditions that need to be fulfilled in order for a payment instrument to fall within the scope of the Directive.

Because of this regulating strategy, bitcoins and other modern virtual currencies evade the legal provision as, for example, they are generated automatically within the network and not issued on receipt of funds. To this extent, the second condition is not fulfilled and, in consequence, the whole act becomes inapplicable.[27]

This way of reasoning and conclusion are being embraced both, in the United States and European Union. For example, in 2012, the European Central Bank, in one of its reports has stated that virtual 'currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual

[26] Michael Koeding, 'Active Transposition of EU Legislation', *EIPASCOPE*, No. 3 (2007) p. 29.
[27] Niels Vandezande, 'Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?', *International Journal of Law and Information Technology*, Vol. 1, No. 16, (2014) p. 6.

community'[28] while the United States Financial Crimes Enforcement Network (FinCEN), has released an official point of view in which it confirms that bitcoins and other decentralized digital currencies are not regulated.[29]

Within the European Union, the fact that modern virtual currencies evade the e–money Directive's scope has a lot more implications than this pure fact of not having to be in line with 'the prudential regime for electronic money institutions' (e.g. establishing, functioning).[30] As there is a set of interlinked secondary legislation acts (i.e. Directives, Regulations) that use the definitions from the 2009 Directive, this makes modern virtual currencies avoid the application of a broader regulatory framework.

A first example is represented by the Payment Service Directive,[31] law stating which category of organizations can administer payment services. Due to the fact that in article 1 (b) it refers to the previously mentioned e–money definition, bitcoins and other cryptocurrencies are not covered by this piece of legislation either. As a result, the business conduct standards imposed by the European legislator do not apply; for example, rules on how to allow and execute transactions, parties' rights and obligations, transparency of data, liability in case of illegal use, refunds or the revocation of payment orders[32] are non–binding for this area of activity.

In the same time, consumers cannot prevail upon their standard European Union rights as the main piece of legislation addressing such matters, namely the 'Consumer Protection' Directive[33] provides that any type of financial service is excluded from its scope.[34] This happens due to the fact that provisions related to their rights are found in the *lex specialis* (e.g. Payment Service Directive) that governs this particular type of legal relationship but which, as mentioned before, is not applicable in the case of modern virtual currencies.

Moving from consumer's private interest to the public one, the rather narrow definition of financial institutions which is codified in the 'Anti Money Laundering' Directive[35] and the

[28] European Central Bank (2012), *Virtual Currency Schemes* (European Central Bank, Frankfurt am Main) p. 13.
[29] Niels Vandezande, op. cit., p. 7.
[30] *E–money* seen on European Commission's webpage on 2014.09.05.
[31] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal, OJ L 319/2
[32] Directive 2007/64/EC art. 28–78.
[33] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ L 304/64
[34] Ibid, art. 3.
[35] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309/15.

fact that Regulation on information on the payer accompanying transfer of funds[36] makes reference to transfers made only 'through payment service providers'[37] allows modern, decentralized virtual currencies to escape the application of several financial surveillance measures meant to protect against money laundering and terrorist financing.

As it can be seen, the way modern digital currencies networks function permits them to take benefit of the several loopholes that the actual legislation has and function in a shadier, clandestine environment where authorities are not present.

Because of this, a whole set of vulnerabilities and problems occur; for consumers, they can severely lose their investments, amounts can be stolen from their 'virtual wallets', the EU refund rights are not protected and, deriving from the digital money's nature, there is also uncertain tax liability. In the same time, there are big concerns for the general public as well due to the fact that such instruments can be used for criminal activity.[38]

6. Dealing with the problems

6.1 Value loss

One of the first problems that might occur regards the high volatility of the digital coins. As they are generated by private financial systems that have as main idea the distributed system of trust between the network participants, this is problematic due to the fact that the network is based on simple logic of supply and demand.[39]

Having this as a premise, such schemes can be facile targets for all kind of manipulation strategies. For example, promoting the threat of possible deflation, bad press campaigns can influence users to withdraw their money out of the system, fact that would lower the demand and, as a consequence, decrease the virtual currency's unit price to an unexpected low level.[40] Linking this kind of strategy to severe previous fluctuations (e.g. in 2013 the exchange rate of a Bitcoin to United States dollars fell about 60 % in a single day and this year, the value dropped by as much as 80 % in 24 hours[41]) can for sure damage the network's strength and reputation.

Continuing the analysis, during this year the Bitcoin exchange rates in relation to the major currencies varied ten times more than the average fact that made several European Union

[36] Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds OJ L 345/1
[37] Ibid, art. 2.
[38] European Central Bank, (2012), p. 47.
[39] Reuben Grinberg,' Bitcoin: An Innovative Alternative Digital Currency', *Hastings Science & Technology Law Journal*, No. 158 (2012), p. 177.
[40] Benjamin Wallace, 'The Rise and Fall of Bitcoin', *Wired Magazine*, (November 2011) p. 7.
[41] Coindesk, *Bitcoin price index chart 2013–2014*, (2014) seen on Coindesk's webpage on 2014.08.18

National banks warn that 'because they are not issued or guaranteed by a central authority there is a possibility of value loss due to their high volatility'.[42]

Drawing a conclusion, virtual currency networks might be the victims of their own faulty functioning and bad reputation. On the other hand, besides the poor economic logic backing up the creation and transfer of digital units, the system can also be endangered by different users whom have enough capital to try and manipulate the market by artificially (e.g. using deceptive transactions) increasing or decreasing the unit value; the networks might be good places for Ponzi schemes or other newer fraudulent strategies due to the fact that the attraction for fast gain among users is very high[43] especially for the ones whom speculate the exchange rates.

6.2 Refund issues

As mentioned before, when it comes to consumer protection, virtual currencies evade the scope of both: *lex generalis* (i.e. the Directive on Consumer Rights) and *lex specialis* (i.e. the Payment Service Directive).

With regard to this fact, the refund rights provided by the second directive are not enforceable in suits involving modern virtual currencies. In consequence, such network companies are not offering the type of assistance the individuals are expecting from a bank or other financial institution. As payers and payees are anonymous and no account details needs to be provided (e.g. names, address, phone number, country), zero interference with their transactions takes place. In consequence, digital money undertakings (e.g. Bitocins, Litecoins) deny any liability for consumer losses if funds are lost by negligent transfer or stolen.[44]

Summing up, the refund rights are not being protected due to the fact that, first of all, the technicalities on which the network functions are as such that it is hard for the administrators to check the scope and legitimacy of a payment. On the other hand, the fact that the legislative burden does not apply to the modern virtual currency systems, makes such companies neglect consumer protection standards.

6.3 Theft

Not having a proper refund policy in the matter of unpermitted transfer of funds from users' accounts is a big incentive for thieves. This way, once the money is transferred from the

[42] *Regulation of Bitcoin in Selected Jurisdictions* (2014) seen on 2014.09.01.
[43] Sandra S. Benson, 'Recognizing the Red Flags of a Ponzi Scheme', *The CPA Journal* , Vol. 79, No. 6, (2009) p. 18
[44] Frank Tudor, 'Making Money with Bitcoins, Litecoins and Other', (*Smashwords Inc*., Los Gatos CA 2014), p. 12.

initial place to another anonymous account, there is no way back except a voluntary return. However, users of digital money, who lose their deposits while administrated of third–party exchanges, have the option to demand refund and damages from the exchanges.[45]

It has been claimed that 'security is difficult and expensive, and virtual currency startups generally do not have the revenue and profits sufficient to attract the capital that would allow top–notch security to be implemented'.[46] Having this as a premise, ever since 2010, there have been stolen bitcoins worth of approximately €380 million, amount which represents about 7% of the total number of this particular type of coins that were generated so far.[47] However, the number refers only to coins released by one market player, which is just one company; in the same time, there might be other fraudulent transactions not uncovered to this extent which can raise the total amount.

Within the information technology community it is generally recognized that crypto systems are strong enough that the only way to penetrate them is by trying every possible key (i.e. algorithms of symbols that can amount to millions of combinations).[48] However, looking at the particular causes that allow such big frauds to happen, it can be said that undiligent users are always a target. For example, the fact that most of the accounts are not secured by alternative authentication (i.e. hardware token or one–time–password generator as SMS) or do not even have a basic password (i.e. the majority of the virtual wallets being just an internet address that once discovered and accessed gives permission to make transactions) represents a serious vulnerability.[49]

In the same time, not only regular user can be negligent when handling such information; poor data protection by currency exchange database administrators represents one of the biggest concerns in this resort. Having a database of hundreds or even thousands of accounts that can be accessed by breaking a security system which most of the times is not proportionate to the financial value it should protect is by far the most desirable target for outlaws.[50]

---

[45] Ajibola Ogunbadewa, 'The Virtues and Risks Inherent in the 'Bitcoin' Virtual Currency', (2014) p. 19 seen on SSRN's webpage on 2014.09.08.
[46] *How is all this bitcoin theft happening* (2013) seen on Bitcoin Stock exchange's webpage on 2014.09.10.
[47] *$500 Million Worth Of Bitcoin Has Been Stolen Since 2010* (2014) seen on Businessinsider's webpage on 2014.08.19
[48] Bert–Jaap Koops, 'The Crypto Controversy – A Key Conflict in the Information Society', (Kluwer Law International, Hague 2001) p. 42.
[49] Christopher Mann and Daniel Loebenberger, Realizing Two–Factor Authentication For The Bitcoin Protocol (2014) pp. 1–2 seen on Cryptology ePrint Archive's webpage on 2014.09.10..
[50] Tyler Moore, Nicolas Christin, 'Beware the Middleman: Empirical Analysis of Bitcoin–Exchange Risk', *Financial Cryptography and Data Security Lecture Notes in Computer Science* Vol. 7859 (2013) pp. 25–26.

In the same time, one last problem with which the whole digital currency community has to deal is represented by specially designed malware programs (e.g. received in the mail inbox or when accessing a webpage) that have the aptitude to steel information or foster double spending operations, all in the detriment of the network members.[51]

6.4 Taxes

When it comes to trading and financial instruments, legal certainty, in general, and foreseeability, in particular, are very important principles due to the fact that costs need to be anticipated in an easy and transparent way.

However, this is not always the case for modern digital currencies; as they still have a controversial nature (e.g. being categorized as commodities, stocks or assets by different jurisdictions), the taxation regime differ depending on the applicable legislation (e.g. users will either pay payroll, property, income, capital gains or profit taxes).[52]

Having regard that the tendency is towards treating virtual currencies as commodities for tax purposes, it must be said that they shall have the same legal regime as gold, oil, wheat, coffee and other fungible goods. More exactly, commodities are a category of goods for which there is demand and which qualities are uniform among producers; exemplifying, a tone of grain is mostly the same product, as it does not really matter who produces it.[53]

Taking the case of Finland, country in which modern digital currencies are treated as commodities, buying a €2 ice–cream in 2014 with bitcoins purchased for €1 in 2013 would generate €1 in capital gains for the ice–cream consumer (i.e. pay capital gains tax) and €2 of gross income for the supermarket (i.e. pay profit tax).[54] Furthermore, most of the states require that digital coins 'miners' will have to notify their gains as taxable income with a value equal to the worth on the moment the coins were received from the system.[55]

However, the lack of harmonization in fiscal matters is not the only issue. Like cash transfers, virtual currencies are hardly traced by tax authorities due to the fact that the users are anonymous. Even though the transaction reports are public, this does not help because no identification is attached to the parties involved in the transfers.[56] As it shall be seen in the

[51] *Cashing in on Cybercrime: New Malware Target Bitcoin* (2012) seen on Trendmicro's webpage on 2014.09.10.
[52] *Bitcoin Taxes* seen on Bitcointaxes's webpage on 2014.09.11.
[53] *Commodity* on Inverstorsworld's webpage seen on 2014.09.11.
[54] *Virtual Currency Taxation* seen on the Finnish Tax Authority's webpage on 2014.08.20
[55] McLeod, Patrick, 'Taxing and Regulating Bitcoin: The Government's Game of Catch Up', *Journal of Communications Law and Technology Policy* Vol. 22, No. 2 (2014) p. 390
[56] Adrian Blundell–Wignall, op. cit., p. 13.

future section, besides hindering the refund process and fostering theft, tax evasion or market manipulation, anonymity is also a good incentive for hard core criminality (e.g. money laundering, terrorist financing, illegal purchases).[57]

6.5 Public interest

It has been said by a financial strategic analyst that 'the biggest barrier in the fight against crime is the data' and that 'there are literally trillions of transactions going through the world's financial systems.'[58] Adding anonymity to the already challenging situations, the outcome reached is one in which authorities are in the impossibility of handling the situation.

Looking at the numbers, there have been about 12 million transactions over 6 years which involved €5 billion for child pornographers, drug dealers, identity thieves, hackers and other outlaws, all encouraged by the rapid and anonymous exchange of virtual coins; in the same time, because of this, several individuals are dealing with possible life imprisonment charges.[59]

Having regard to this fact, in July 2014 the Russian Government considered banning digital coins; moreover 'entities that use or exchanges in virtual currencies are subject to suspicion of money laundering or other criminal activities.'[60] However, this official position might change in time due to the fact that the usage of digital money might be a good alternative in order to compensate for the financial sanctions[61] imposed by Visa and MasterCard as a result of the Ukrainian crisis.

Turning back to the actual crimes, which use anonymity, a United States government official assumed that if Al Capone was alive today he would use these networks to hide his money.[62] The fact that payments are clandestine protects against any control (i.e. to detect, ask justifications and freeze assets) from public authorities over the users' accounts and this is a good way for corrupt politicians or other criminals to hide their illicit income.

In the same time, without the possibility to tie an identifiable user to a particular virtual currency address, tracking the injection, layering, and reentry of laundered money would be

[57] Raj Samani, François Paget, Matthew Hart (2013), McAffe White Paper – 'Digital Laundry – An analysis of online currencies and their use in cybercrime', (*McAffe Inc*., Santa Clara, CA) pp. 14–16.
[58] Cindy Williamson, Jason Vazquez, Jason Thomas, Katherine Sagona–Stophel (2013), Thomson Reuters Accelus Report – ' Technology in the Fight Against Money Launderingin the New Digital Currency Age' seen on Thomson Reuters's webpage p. 11, on 2014.08.21.
[59] Ibid, p.4.
[60] Perkins Coie LLP (2014), op. cit.
[61] Juan C. Zarate (2013), 'Conflict by Other Means – The Coming Financial Wars', *Parameters,* Vol. 43, No. 4, (2013) pp. 90–92.
[62] *Online Currency Exchange Accused of Laundering $6 Billion* (2013) seen on The New York Times webpage on 2014.09.12.

really hard public officials. As a consequence, anti–money laundering authorities are dealing with a 'target' that is almost impossible to recognize.[63] Furthermore, anonymity doubled by the 'currency's' high volatility can help justify huge incomes and disguise the origins of money obtained through illegal activities, know–how which is also used to launder money.

Moving forward with the analysis, the lack of information on the payer and the payee allows large amounts of money to be moved cross border without hindrance to undetected areas, method that is perfect for terrorist financing.[64] In the same time, this transaction typology provides a secure service for black market commerce (e.g. narcotics) by assuring a safe way of payment between retailers and costumers from different parts of the world.[65] In both cases, the virtual currency can be transformed in fiat money by either using centralized exchanges, selling them to individual users, withdrawing from digital money ATMs or using to purchase goods and services.

As it can be deduced, besides the many benefits that virtual currencies bring into the consumer's life, there are also several issues regarding to the fact that so far, the modern, decentralized ones have evaded the European Union or worldwide regulatory frameworks. The next section is intended to present the recent reactions and legal developments in this resort, which came as a response to all the above-mentioned problems.

7. The next steps

On the European Union scale, the most important point of view, besides the ones presented by the European Central Bank ever since 2012 is being assumed by Michel Barnier whom, very recently, from his posture of financial services commissioner communicated that 'it is imperative to move quickly on this issue [...] the potential for money laundering and terrorist financing is too serious to ignore.'[66]

However, at a first sight, the European Union finds itself only at a political declaration level due to the fact that none of the ongoing negotiations for recasting the current relevant directives (i.e. payment service directive, the anti–money laundering/terrorist financing directive and the one on information accompanying transfer of funds)[67] are not having on their agenda the virtual currency issue. Anyhow, it should be expected that initiatives regarding this

[63] Danton Bryans, op. cit. p.447
[64] KPMG, Virtually Unregulated, *Countering Virtual Currency Money Laundering in the 21st Century* (2013) pp. 3–4, seen on KPMG's webpage on 2014.08.21
[65] Raj Samani, François Paget, Matthew Hart, op. cit., pp. 14–16.
[66] *EU Banks Must Shut Bitcoin Until Rules in Place, EBA Says* (2014), seen on Bloomberg's webpage on 2014.08.22.
[67] Directive 2007/64EC, Directive2005/60EC and Regulation 1781/2006.

area of interest will soon be presented. They might just take the form of new pieces of secondary legislation (i.e. Regulation, Directive) or come as amendments to the currently negotiated acts.

On the other hand, considering what is happening in the United States it can be said that things are more dynamic at a federate and not federal level. The first authorities to take initiative and try to regulate decentralized virtual currencies are the ones from the state of New York. In this matter, at the end of July current year, the New York Department of Financial Services proposed a licensing scheme that would also cover the new models of virtual coins. By defining virtual money as 'any type of digital unit that is used as a medium of exchange or a form of digitally stored value that is incorporated into payment system technology', its intention is to create a new regulatory framework. As it can be seen, the term is constructed in an extensive way and as it is meant to encompass both centralized and decentralized repositories and administrators.[68]

Furthermore, the proposed regulations goes beyond the money transmitter rules (i.e. the ones applying to centralized virtual currencies) and it *expresis verbis* imposes the duty of designation of a compliance officer and a chief information security officer.[69]

From the other measures imposed it can be said that virtual currency companies will have to 'maintain capital amounts set by the law and have audited annual financial statements, enforce written policies, including refund, anti–fraud, anti–money laundering, cyber security, privacy and information security.'[70]

In the same time, such undertakings will be obliged to keep for ten years books and records regarding all transactions and give public officials 'immediate access to all records of licensee or affiliates', 'wherever located.' Also, the anonymity problem is being dealt with as virtual currency firms will have to make sure that each transaction is being followed by information on amount date and 'precise time', 'payment instructions', 'names, account numbers, and physical addresses of the parties to the transaction.'[71]

This kind of legal policy looks very energetic and, *prima facie*, solves all the above-mentioned problems. Even though bringing more discipline and transparency into the system is very desirable, the cost at which this might occur can endanger the existence of the system

[68] *New York State forges ahead in the virtual currency arena with proposed licensing requirements* (2014) seen on Regulation Tomorrow webpage seen on 2014.09.15.
[69] Ibid.
[70] Proposed Codes, Rules and Regulations, NY State, Dept. of Financial Services seen on New York Department of Financial Services's webpage on 2014.08.22
[71] Ibid.

per se, fact that might cause other problems (i.e. innovation hindrance, consumer welfare damage).

On the European level, legislative action will for sure take place on the short run. As the anti–money laundering and terrorist financing policies are internationally harmonized[72], it is more than legitimate to expect measures increasing transactional transparency. Also, as the Union institutions have a very cautious approach on consumer protection, there will for sure be measures taken to assure refund policies, enhanced security and legal certainty.

On the other hand, it should be expected that the virtual coins companies will invest in protecting their actual interest; some of their tactics might refer to lobbying in Brussels for not as restrictive legislation and investing in media campaigns that would assure their users of the network's strength. However, such kind of actions must be seen legitimate as far as virtual currency undertakings admit the system's vulnerabilities and plead for suitable measures that would not go beyond what is needed to efficiently regulate the system. As the danger of excessive regulation exists, the need for compromise represents a must.

8. Conclusion

It is certain that we live in a dynamic world based on technological change and permanent development. Because of this, legislators must keep pace with it and deliver the best regulatory frameworks meant to sustain progress and not hinder innovation. In order to do so, they must first understand the system's way of functioning, its desirability for the society and the way it can be protected from miss usage. Once this level of understanding and planning is being reached, the premises for a solid regulation are being established.

However, this is not always the case; as it has been developed in this case–study, legislators are sometimes one step behind as the understanding process takes time and normative bargains are lengthy. Moreover, the need to change legislation can occur most of the times due to the fact that it lacks visionary character and, as in our case, it allows new technologies to evade their application.

Besides the timing issue, there is another problem, which relates to the substance of the norm to be enforced. In this particular resort, a proportionality test between the benefits of the invention and the costs of regulating it must always take place in order to reach the perfect compromise. Exemplifying, what makes the whole decentralized virtual currency really cheap nowadays is the fact that the functioning costs are at a minimum level. Once all of the regulatory

[72] *Countries* seen on Financial Action Task Force's webpage on 2014.09.15.

requirements from the United States example will be enforced (e.g. book keeping, maximum transparency, surveillance, accountability etc.) the administrative and financial burden might be too heavy for the system and prices for services might rise at the detriment of the average consumer, fact which will 'chase away' users.

In the same time, as there are two categories of users: the ones being attracted by the anonymous or facile way of sending money and another one speculating exchange rates, it is for sure that once most jurisdictions will impose maximum transparency standards, the networks will not be desirable any more for most of the persons from the first category and as a result the second one will suffer as well. As the currency power or fragility is a matter of supply and demand it is certain that if the supply increases and there is not demand, the unit price will lower.

Having this interlinked system, it can be seen that an action that is being taken on any level has implications upon several other aspects and agents. Because of this, it is very important to give primacy to a proportionality type of logic in which only feasible measure that do not go beyond what is needed are being enforced and in which the effects of the regulatory endeavour are not depriving the final consumer from novel and more efficient products.

However, as in order to solve refund, security and criminality problems there is a strong need to bring more transparency, the fact that some users might abandon the network (i.e. the ones aiming for anonymous transfer) represents a loss that, on the long run can prove to be beneficial for the system's legitimacy and reputation. Continuing, it can be said that, at this point, the perfect compromise would be transparency at very few costs as the system would still conserve its benefits for consumers and, in the same time, fraudulent and penal abuses would be avoided.

For example, one solution to reach such an outcome can be the usage of the e–identification method. By basing their logic on the fact that 'building trust in the online environment is key to economic and social development', the European Union institutions have adopted in July 2014 the Regulation on electronic identification and trust services for electronic transactions in the internal market.[73] This piece of secondary legislation defines electronic identification as 'the process of using person identification data in electronic form uniquely representing either a natural or a legal person'[74] and has the main scope of assuring a 'coherent

[73]Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257

[74] Regulation No 910/2014, art. 3 (1).

framework with a view to providing a high level of security and legal certainty of trust services' at affordable prices.[75] Anyhow, this might be just one solution in order to reach the perfect balance between the need to abolish anonymity and the imperative of keeping costs as low as possible.

Summing up, as today virtual currencies are more and more popular among consumers – important currency exchanges list virtual coins alongside other currencies, Visa and MasterCard offer virtual currency debit cards and Lamborghini accepts virtual coins for its cars[76]– it is very important to make sure that the regulations fold on the market tendencies and do not obstruct them in a brutal way.

[75] Regulation No 910/2014, recital 44.
[76] *So You Know Nothing About Bitcoins? Here's 50 Things That'll Make You Sound Like An Expert* (2014) seen on Bluntbit's webpage on 2014.08.10

A BRIEF HISTORY OF THE FINNISH DATA PROTECTION AUTHORITIES

With an Eye towards the Future[1]

Juhana Riekkinen

Researcher, University of Lapland, Faculty of Law, juhana.riekkinen@ulapland.fi

1. Introduction

The first Finnish general act on data protection, the Personal Data File Act (471/1987; hereinafter PDFA) entered into effect on January 1, 1988. Already before this date, two new national authorities had been founded to supervise and enforce compliance with the provisions of the Act: the Data Protection Ombudsman (*tietosuojavaltuutettu*) and the Data Protection Board (*tietosuojalautakunta*). The basic distribution of tasks and duties was such that the Ombudsman, supported by an organization known as the Office of the Data Protection Ombudsman, was to provide guidance, to consult, to control and to supervise; the Board, on the other hand, was given a decision–making role in relation to permissions, prohibitions and orders as provided in the PDFA.[2]

The PDFA has since been replaced by the Personal Data Act (523/1999; hereinafter PDA), which was drafted mainly in order to accommodate the requirements of the EU Data Protection Directive[3] adopted in 1995, as well as the increased emphasis on fundamental rights. The volume of both domestic and European specialized statutes and provisions on data protection issues has also increased dramatically, but the basic roles of the two Finnish data protection authorities have remained the same to this date.

Another thing that has remained the same since the beginning is that both of these two authorities are based in Helsinki, and they have jurisdiction in the entire country. In Finland, there are no regional data protection authorities, with the exception of *Datainspektionen*, the data protection authority of the autonomous region of Åland.[4] When talking about Finnish data protection authorities, notion must also be made of the somewhat problematic role of the

[1] This paper is a summarized account of a Finnish–language report written in the course of the NETSO research project.
[2] The background of this supervisory model will be discussed in chapters 2 and 3 of this paper.
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[4] See <http://www.di.ax> [20.5.2014].

Finnish Communications Regulatory Authority (FICORA).[5] However, *Datainspektionen* and FICORA are not the topic of this paper. The focus is on the Ombudsman and the Board.

As regards the Ombudsman and the Board, their exact responsibilities, powers and especially workloads have seen some significant changes. The purpose of this paper is to draw a picture on the history and development of the two authorities through over a quarter of a century of drastic technological, societal and legislative changes and advancements. Reference is frequently made to statistical information, which has been derived mainly from the annual reports of the Office of the Data Protection Ombudsman. In addition, the paper draws heavily on decisions and various other materials produced by the authorities, as well as court cases, law drafting documents, and interviews.

2. Drafting and development of Finnish Data Protection legislation

Finland was not among the very first countries to draft or approve legislation on data protection. Already in the late 1960s and 1970s, discussion concerning data files, processing of personal data and data protection had started in organizations such as the OECD and the Council of Europe. While it took until the early 1980s for these discussions to materialize in the OECD Recommendation[6] and the Council of Europe Convention[7], national data protection legislation was approved in certain countries several years earlier. The *Datenschutzgesetz* of the West German state of Hesse, which was approved and entered into effect in October 1970, is considered the first act on data protection. Other examples of the first generation of data protection laws include the Swedish *datalag* (SFS 1973:289) and *kreditupplysningslag* (SFS 1973:1173) as well as the *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* (approved in 1977 and entered into effect on January 1, 1978), a federal act applying to the whole of West Germany.[8]

Despite the strong tradition of Nordic co–operation and collaboration in law drafting, in data protection matters the Nordic countries saw fit to find their own, separate ways. In Finland, drafting of data protection legislation began in November 1971 with the appointment of the so–

[5] FICORA, an agency operating under the Ministry of Transport and Communications, has some tasks relating to the supervision of the provisions of the Information Society Code (917/2014) that replaced the Act on Privacy in Electronic Communications (516/2004). Due to its organization and other tasks, FICORA can hardly be considered a genuine, independent data protection authority.

[6] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data, 23.8.1980.

[7] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (108/1981).

[8] The background of *datalag* is discussed extensively in Söderlindh, *Personlig integritet som informationspolitik* (2009).

called Data Protection Commission (*Tietosuojatoimikunta*).[9] Its report[10] and the documents produced by its successors, the Information System Committee (*Tietojärjestelmäkomitea*)[11] and the Personal Data File Working Group (*Henkilörekisterityöryhmä*)[12], did not lead to legislative action in the 1970s. This was largely due to the controversial and at the time highly politicized nature of the matter. In fact, the Information System Committee was disbanded in May 1975 for political reasons before it could finish its assignment. In 1980, the new Data Protection Committee (*Tietosuojakomitea*) was given the assignment of drafting a bill on data protection in the form of a Government Proposition. The Data Protection Committee completed its report[13] in 1981, but it took an additional five years of drafting at the Ministry of Justice before the Government Proposition on the Personal Data File Act and related legislation (HE 49/1986 vp) was finally given. In February 1987, the bills were passed by the Parliament with some minor amendments. The President approved the bills on April 30, 1987. Simultaneously, related decrees were issued by the Government.[14]

Internationally, the PDFA can be classified as a second generation data protection law. It was in effect for over 11 years, during which time it was amended three times, most significantly in 1994 when, i.e., sections governing the processing of personal data for the purposes of direct marketing, genealogical research and public registers were included in the act.[15] Concurrently, data files maintained for journalistic purposes were largely excluded from the scope of the act. Soon after this, in 1995, the need for a new general data protection act was brought on by two events: the reform on fundamental rights, and the adoption of the EU Data Protection Directive.

---

[9] The assignment was preliminary and preparatory in nature: to map the problems relating to gathering, distribution and disclosure of data in relation to private individuals, public sector and business sector, with the aim of drafting a commission for a committee.

[10] KM 1972:B 31.

[11] KM 1974:110.

[12] Sinisalo & al., *Henkilörekisterityöryhmän väliraportti* (1977).

[13] KM 1981:66

[14] In the Data Protection Committee report and the Government Proposition, the ombudsman–like authority was called *tietosuoja–asiamies*. The title was amended in the course of the parliamentary proceedings, and in the final act the authority was called *tietosuojavaltuutettu*. — For a more detailed description of the early history of data protection in Finland (in Finnish), see Konstari, *Henkilörekisterilaki* (1992) pp. 3–9, 15–35, Wallin & Nurmi, *Tietosuojalainsäädäntö* (1991) pp. 1–7, 16–20 and Korhonen, *Perusrekisterit ja tietosuoja* (2003) pp. 112–116. In English, see also Saarenpää, 'Finland' in Blume (ed.), *Nordic Data Protection* (2001) p. 42

[15] As regards genealogical research (and many other things), it is important to notice that the PDFA applied, as does the current PDA, to personal data of deceased persons, at least to some extent. By contrast, the Data Protection Directive does not apply to deceased persons. See WP 29, *Opinion 4/2007 on the concept of personal data* p. 22–23 (referencing Minutes of the Council of the European Union, 8.2.1995, document 4730/95). See also Saarenpää, 'Data protection in the network society – the exceptional becomes the natural' in *Galindo* (ed.), *El derecho de la sociedad en red* (2013) pp. 116–117.

Finland's ratification of the European Convention on Human Rights in October 1990 paved way for the 1995 reform on fundamental rights, which can be seen as a major legislative milestone also from the point of view of data protection. The reform added, without much discussion in the drafting documents,[16] a new constitution–level provision on the *right to privacy*, which was later transferred to the new Constitution of Finland (731/1999). Currently located in section 10 of the Constitution, the provision states that everyone's private life, honor and the sanctity of the home are guaranteed, and that more detailed provisions on the protection of personal data are laid down by an Act. This provision elevated the right to data protection to the status of a fundamental right, albeit only as a part of privacy, not as an independent right as it is nowadays understood.[17]

In Finland, the 1990s were marked by European integration on two separate but related fronts. As regards the Council of Europe, in addition to the ECHR, Finland ratified the aforementioned Personal Data Convention in December 1991.[18] As regards the European Union, Finland's accession came into effect on January 1, 1995. In October of the same year, the Data Protection Directive (95/46/EC) was adopted. Member states were given three years to implement the directive in their national legislation. In Finland, a new committee called the Personal Data Commission (*Henkilötietotoimikunta*) was trusted with preparing this implementation.[19] The Commission was also instructed to take into account the reform on fundamental rights and the Personal Data Convention. Largely based on the Commission's report[20], the Government Proposition on the Personal Data Act and certain related legislation (HE 96/1998 vp) was given to the Parliament in July 1998. The time limit for the implementation of the Directive could not be met; the bills were approved in 1999 and the new Personal Data Act replaced the old PDFA on June 1, 1999.

The PDA, a third–generation general data protection law, has now been in effect for 15 years. It has been updated six times, but the amendments have been largely technical and of little significance. The general principles of the Act have stood the test of time in a changing, developing, increasingly technological and networked society. However, the development of data protection legislation has been marked by the ever–increasing amount of special laws and

[16] See KM 1992:3 and HE 309/1993 vp.
[17] Cf. Charter of Fundamental Rights of the European Union (2010/C 83/02), Articles 7 and 8.
[18] The ECHR entered into force in Finland simultaneously with the ratification on May 10, 1990, and served as an inspiration for the aforementioned reform on fundamental rights. The Personal Data Convention entered into force on April 1, 1992.
[19] The committee consisted of a chairperson, eight members and nine permanent experts. The implementation was prepared nationally. Again, Nordic co–operation was not pursued, save for one meeting in Norway. Saarenpää, 'Finland', in Blume (ed.), *Nordic Data Protection* (2001) pp. 46–47.
[20] KM 1997:9.

provisions. Notable, current Finnish data protection special laws include the Act on the Protection of Privacy in Working Life (759/2004) and the Credit Data Act (527/2007). A further noteworthy special law, the Act on Privacy in Electronic Communications (516/2004)[21], was replaced by largely corresponding provisions incorporated in the new, massive Information Society Code (917/2014), which entered into effect on January 1, 2015. Provisions on the processing of personal data can be found in dozens of other acts and decrees, including a large amount of legislation concerning various national registers, among them the most important basic registers of the Finnish society, e.g., the Population Information System[22]. However, none of the special laws override all the provisions of the general law, and therefore the PDA must be taken into account in all data processing activities.

3. Statutes and Provisions on the Authorities

The first two committee reports did not address the question of supervisory authorities. In the Personal Data File Working Group report, alternatives for supervision were discussed based on foreign examples.[23] Based on this, the Working Group asked for opinions on three different organizational models. The first model was based on founding new national, dedicated data protection authorities. The second model would have tasked some existing sectoral supervisory authorities with new responsibilities. The third model was to leave the supervision and enforcement of data protection legislation to the general courts. In the feedback that was collected, the second alternative proved the most popular.[24]

The Data Protection Committee, however, came to a different conclusion. As data protection legislation had already been approved in other countries, the Committee compared solutions adopted abroad and endorsed a centralized approach with dedicated data protection authorities.[25] Without much visible argumentation, apparently drawing from the Finnish

[21] What was to become Amendment 125/2009 of the Act on Privacy in Electronic Communications, commonly dubbed *Lex Nokia* or *prying law*, raised considerable privacy concerns and public debate in 2008 and 2009. Among other things, the Amendment granted corporate and association subscribers wide powers to process identification data (e.g., e–mail headers of employee e–mails) in cases of suspected misuse. The proposal elicited criticism from a number of interest groups, the Chancellor of Justice, the Data Protection Ombudsman and several legal experts. Contrary to the opinions of numerous law professors heard in the Constitutional Law Committee of the Parliament, the amendment was deemed constitutional and consequently approved in the ordinary legislative procedure. The new provisions entered into effect on June 1, 2009. In practice, however, organizations have made little use of their new powers.

[22] See <http://www.vrk.fi/default.aspx?id=39> [20.5.2014].

[23] See Sinisalo & al., *Henkilörekisterityöryhmän väliraportti* (1977) pp. 4 (Sweden), 8–9 (Denmark), 11 (Norway), 13–14 (Germany), 16 (Austria), 18 (Netherlands), 19–20 (Belgium), 20–21 (France), 22 (Spain), 25 (Canada and England).

[24] See Virtanen, *Lausunnot henkilörekisterityöryhmän väliraportista* (1977) pp. 53–62.

[25] See KM 1981:66 pp. 39–44.

experiences in the fields of consumer protection and accounting,[26] it proposed an internationally unique, twofold model with the responsibilities divided between a supervisory and consultative ombudsman and a decision–making entity in the form of a 7–member board, which were seen as balancing each other. This basic model was later transferred to the Government Proposition (HE 49/1986 vp), which, in addition to the proposed PDFA, contained a separate bill on the Data Protection Board and the Data Protection Ombudsman. In contrast to the PDFA, which entered into effect in the beginning of the following year, the Act on the authorities took effect already on October 1, 1987. On that day, the Office of the Data Protection Ombudsman began its operation. The Data Protection Board convened for its first meeting on December 7, 1987.

The first act concerning the data protection authorities (474/1987; hereinafter DPB–DPO Act of 1987) consisted of 12 sections and contained provisions on the Board's composition, tasks and duties, competency requirements and liability for acts in office, as well as the Ombudsman's competency requirements, appointment procedure, and office personnel. Furthermore, the Act contained provisions on the authorities' right to obtain expert opinions, the duty of the police to provide executive assistance, and secrecy obligations.

The DPB–DPO Act of 1987 contained only general provisions on the tasks and duties of the authorities. According to section 3, the duty of the Data Protection Board was to solve matters that were to be decided by it under the PDFA, and to deal with questions of principal importance in relation to the scope of application of the PDFA. Section 7 stated that the Ombudsman was to solve the matters that were to be decided by her or him as provided in the PDFA, and to supervise and guide the collection and storage of personal data to data files, the use and protection of data files, and the disclosure of data contained in a data file. While the PDFA itself largely determined the tasks of the authorities, more specific norms were contained in a lower level decree (477/1987; hereinafter DPB–DPO Decree of 1987).

The DPB–DPO Act and Decree of 1987 were replaced in July 1994 with new pieces of legislation bearing the same titles (Act 389/1994; hereinafter DPB–DPO Act of 1994, and Decree 432/1994; hereinafter DPB–DPO Decree of 1994). The content of the two statutes remained largely the same, but specific provisions on the duties of the authorities were moved from the Decree to the Act, and provisions on the Board's composition, appointment procedure

[26] Some years earlier, an expert board (*kuluttajavalituslautakunta*, nowadays *kuluttajariitalautakunta*) and an ombudsman (*kuluttaja–asiamies*) had been founded to take care of the supervision and enforcement of the Consumer Protection Act (38/1978). The Accounting Board (*kirjanpitolautakunta*) had been founded already in 1974 with the entry into effect of the Accounting Act of 1974 (655/1973).

of the members of the Board, and competency requirements of the members and the Ombudsman were moved from the Act to the Decree.

The Act and Decree of 1994 are still in effect, although they have been amended several times, notably along with the approval of the PDA in 1999. In its current form, section 2 of the DPB–DPO Act states that the Board's task is 1) to process and make decisions on matters that are to be decided by it under the PDA; and 2) to monitor the need of development of legislation concerning the processing of personal data, and to issue initiatives it deems necessary. Section 5 lists four tasks for the Ombudsman: 1) to process and make decisions on matters concerning personal data and credit data as provided in the PDA and the Credit Data Act, and to perform other duties resulting from them; 2) to monitor the general development of the processing of personal data and credit data, and issue initiatives she or he deems necessary; 3) to take care of information services related to her or his scope of authority; and 4) to take care of international co–operation related to the processing of personal data.

Chapter 9 of the PDA concerns direction and supervision of the processing of personal data and is important in determining the tasks of the authorities. Further provisions on the tasks of the authorities—in particular the Ombudsman—are issued in special laws, including the Credit Data Act but also approximately 30 acts and decrees not mentioned in the DPB–DPO Act, most notably the Information Society Code and the Act on the Protection of Privacy in Working Life. Contrary to some foreign data protection authorities, the Finnish Data Protection Ombudsman has no duties relating to the interpretation or supervision of openness legislation, and makes no decisions on the publicity or disclosure of documents held by state or municipal authorities.[27] The somewhat complicated legislative framework is illustrated in the following figure.

[27] In practice, openness and data protection matters are often connected to each other, and the Ombudsman may not fully avoid questions relating also to openness. On EU level, the relationship between data protection and openness is partly, if not clearly, defined by Recital 72 of the Data Protection Directive—added on request of Sweden and Finland – which states that the Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in the Directive.

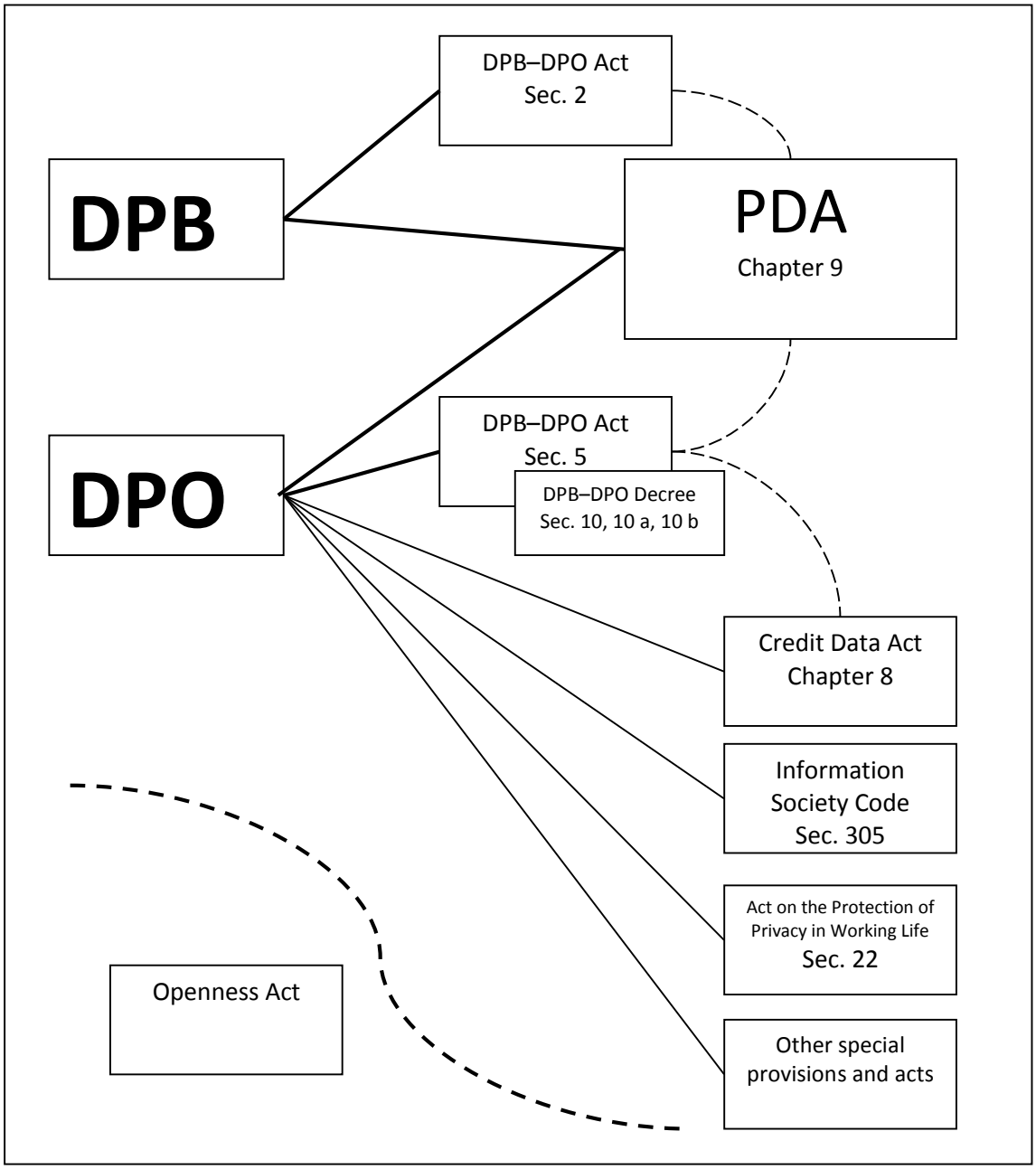


Figure 1. Duties of the Finnish Data Protection Authorities in Legislation.

So far, tasks and duties of the authorities have been determined chiefly by domestic legislation as opposed to EU law, which has imposed few specific demands regarding the organization of supervision. This will, in part, change with the new EU General Data Protection Regulation.[28] Concerning the authorities, the key requirement of the current EU legislation is that the supervisory authorities must act with *complete independence* in exercising the functions entrusted to them (Article 28(1) of the Data Protection Directive). The Court of Justice of the

[28] See COM(2012) 11 final, proposed Articles 52–54.

European Union has clarified the meaning of this independence in three judgments,[29] in which it has declared that the member states in question have failed to fulfil their obligations under the Directive. The Court has highlighted that while the operational independence of supervisory authorities, in that their members are not bound by instructions of any kind in the performance of their duties, is an essential condition, it is not sufficient in itself to protect supervisory authorities from all external influence. The authorities must remain above all suspicion of partiality. While the independence of the Finnish data protection authorities could be called into question based on the links that both of these authorities have to the Ministry of Justice, the institutional model has been considered to adequately fulfil the independence requirement of Article 28(1). The new General Data Protection Regulation will contain more specific provisions on the independence of the supervisory authorities.[30]

4. The Data Protection Ombudsman

4.1 General Information

The Data Protection Ombudsman is a public official nominated by the Government for a renewable period of no more than five years.[31] So far three different people have acted as the Ombudsman: *Anna–Riitta Wallin* (1987–1992), *Jorma Kuopus* (1992–1997) and the current Ombudsman, *Reijo Aarnio* (since 1997).

The Ombudsman is supported by the Office of the Data Protection Ombudsman, an expert organization under his direction. There is no Vice– or Assistant Data Protection Ombudsman; when needed, the Office Manager acts as the Ombudsman's substitute. In the end of 1988, the number of personnel was 8. During the 1990s the Office gradually gained some more resources and the number of staff could be increased. In the early 2000s the number stabilized around 20.[32] This was made possible by the increase in funding, but to this day the Office remains considerably smaller than the comparable Nordic data protection authorities.[33] In 1988, the entire budget for both the Office and the Board was 2.349.000 FIM (approximately 670.000

[29] Cases C–518/07 (Commission v Germany, Judgment of 9 March 2010), C–614/10 (Commission v Austria, Judgment of 16 October 2012) and C–288/12 (Commission v Hungary, Judgment of 8 April 2014).
[30] See COM(2012) 11 final, proposed Articles 47–49. About independence of the supervisory authorities, see Saarenpää, 'Data protection in the network society – the exceptional becomes the natural' in *Galindo* (ed.), *El derecho de la sociedad en red* (2013) pp. 108–113.
[31] Before 2000, the Ombudsman was nominated by the President of the Republic.
[32] In addition, during the 2000s and early 2010s, the Office made rather heavy use of trainees and other temporary workers, amounting to over 4 FTEs at highest. The use of trainees for fulfilling the legally mandated duties of the Office was considered problematic, and the policy has been discontinued.
[33] The Swedish, Norwegian and Danish data protection authorities all have approximately twice as many employees. See Datainspektionen (Sweden), *Årsredovisning 2012* p. 47, Datatilsynet (Norway), *Årsmelding for 2013* p. 69, and Datatilsynet (Denmark), *Datatilsynets årsberetning 2012* p. 15. It should be noted, however, that the organizational structures of these authorities differ from the Finnish model.

euro). In 2000, the budget for the Office was 3.900.000 FIM (approximately 1.300.000 euro), and in 2012 1.764.502 euro.[34]

4.2 The Ombudsman and the Office in Statistics

In the Government Proposition for the PDFA, it was estimated that the Ombudsman would receive approximately 200 statutory notifications from data controllers yearly. In addition, 250 one–time notifications were expected to immediately follow the Act's entry into effect. It was also estimated that the Ombudsman would carry out approximately 50 inspections per year. No numbers were given for other activities.[35]

During its first full year of operation, 1988, the Office of the Data Protection Ombudsman received a total of 716 and concluded a total of 287 cases. In the 1990s the case–load varied between approximately 600 and 1000 cases. Since the adoption of the PDA, the number of cases has risen quickly and is currently at well over 3000 per year, as illustrated in the following figure.

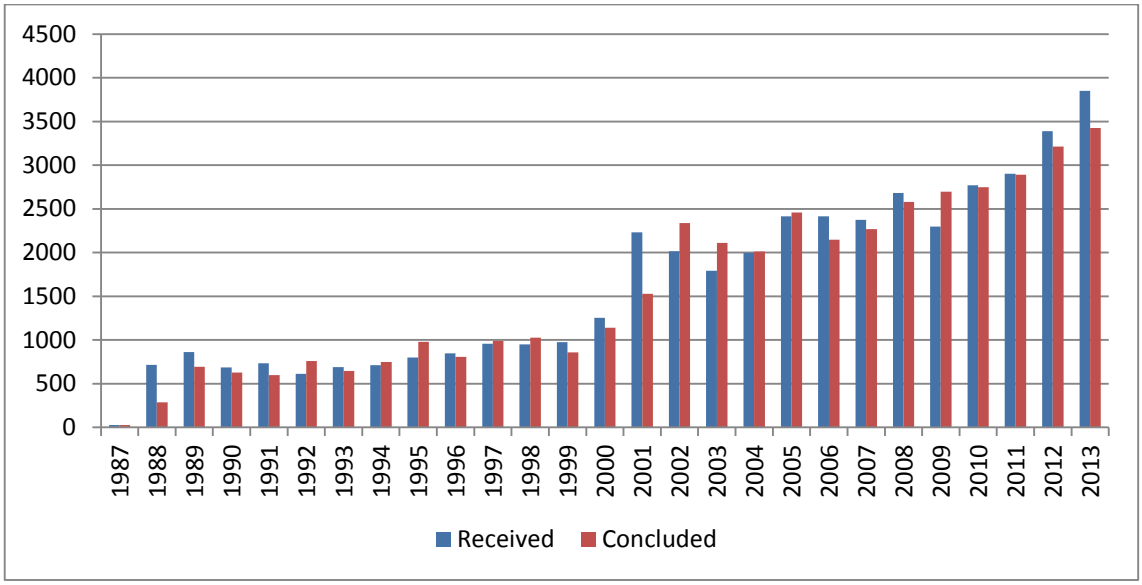


Figure 2. Received and concluded cases at the Office of the DP Ombudsman, 1987–2013.

The numbers depict all kinds of cases and matters including, e.g., statutory notifications by data controllers, complaints and requests for action by data subjects, investigations initiated by the Ombudsman, and expert opinions given to prosecutors, courts, law drafters etc. The numbers also include matters relating to the administration and operation of the office itself.

[34] The FIM values have been converted to 2012 value using a table provided by Statistics Finland, available at <http://www.stat.fi/til/khi/2012/khi_2012_2013–01–15_tau_001.html> [3.4.2014].
[35] The effective operation of the office was expected to require a budget of 1.200.000 FIM (approximately 370.000 euro) and a minimum of nine office personnel.

These administrative matters have comprised approximately 5–10 percent of all statistical cases.

The largest categories of cases have been requests for action by data subjects (private citizens), and consultation and guidance of data controllers. Request for action have on average made up for one third of all cases, whereas cases relating to consultation and guidance of data controllers have made up for one fifth. The number of cases in both of these categories has significantly increased in the 2000s, but proportionally the share of requests for action has been on a downward trend whereas the share of consultation and guidance of data controllers has been considerably larger in the 2000s than it was in the 1990s.

In 1988, the office received 226 statutory notifications from data controllers. In the 1990s, there were on average 50 notifications per year, a much lower figure than estimated in the Government Proposition. During the PDA era, the numbers have been considerably higher, averaging above 250 even excluding the transitional period which saw a sudden albeit temporary rise. Compared to the overall numbers of received cases, the share of notifications has generally been below 10 percent, but with the entry into effect of both the PDFA and the PDA, has temporarily risen to approximately one third of all cases. The changed legal requirements concerning notifications were indeed the cause for the sudden increase of all received cases in 2001, when the transitional period of the PDA drew to its close. The following figure depicts the development of the major categories starting from the final years of the PDFA.

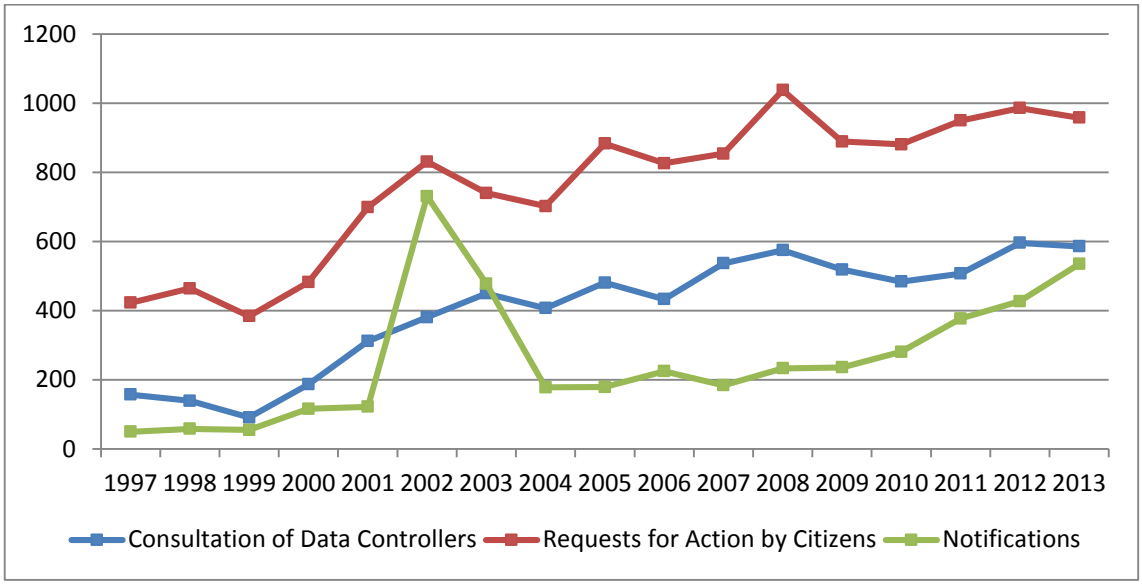


Figure 3. Concluded cases by category, top 3 categories, 1997–2013.

Inspections, which were originally believed to play a major part in the Ombudsman's activities, chronically suffered from a lack of resources throughout the 1990s. On average, less

than 10 inspections per year could be carried out. During the 2000s there have been on average slightly more investigations, although in the last few years the focus has shifted from traditional inspections at the premises of a single data controller to sector–wide electronic mass inspections and online queries.

When looking at different sectors or branches of activity, it can be noted that most matters brought to the Ombudsman by data subjects have to do with work life, healthcare and direct marketing. Data protection issues concerning these sectors, especially work life and healthcare, have also drawn high numbers of consultation requests by data controllers. When looking at other sectors, data subjects have been particularly active in contacting the Ombudsman in relation to the processing of personal data in law enforcement and the processing of credit data. It is also noteworthy that from very early on, citizens have been seemingly concerned with matters that have to do with the use of the personal identity code (*henkilötunnus*). By contrast, cases relating to insurance industry, education and associations have much more commonly been initiated by the data controller than the data subject. These things, among other things, can be observed from the following two figures.

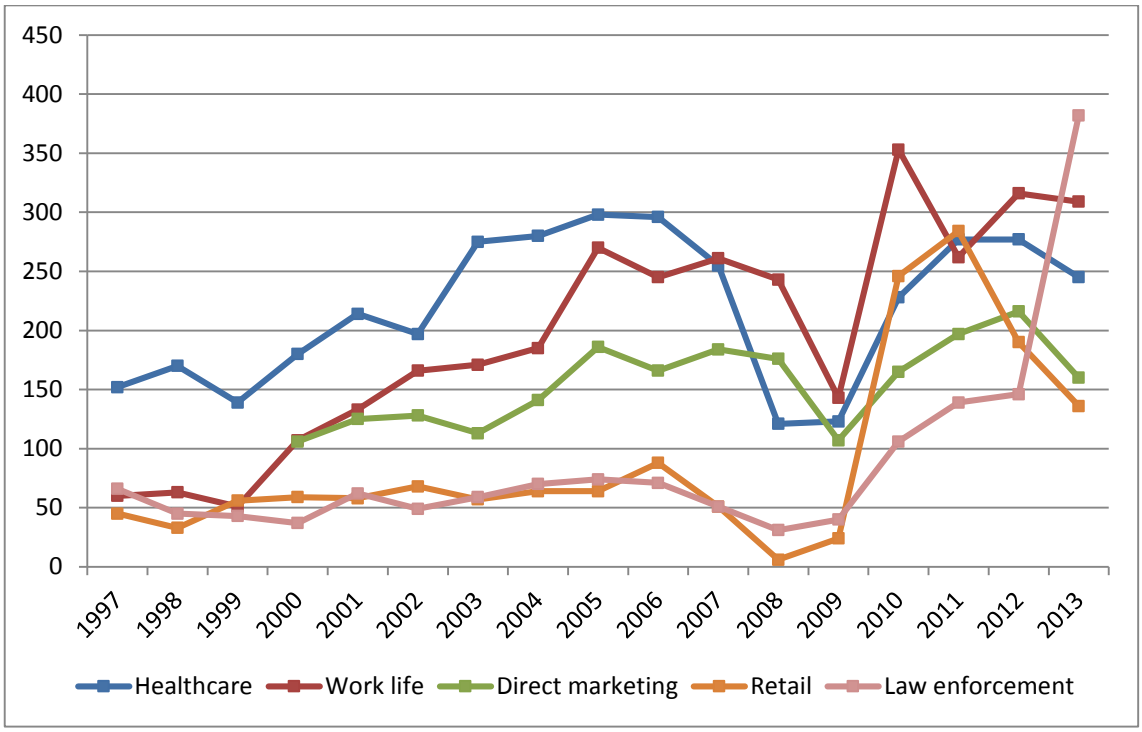


Figure 4. Received cases by sector, top 5 sectors, 1997–2013.

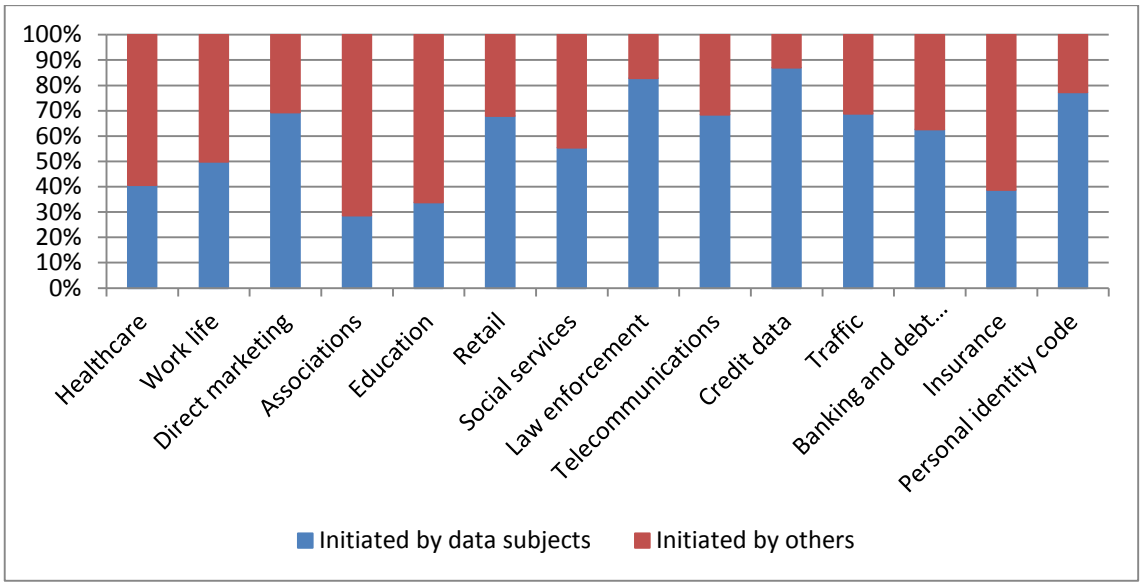


Figure 5. Received cases initiated by data subjects and by others by sector, 2000–2007.[36]

The only cases in which the PDA gives the Ombudsman the power to make binding decisions are the data subjects' requests concerning the realization of their right of access to their own personal data under PDA section 28, and their right to request rectification of erroneous data under PDA section 29. According to PDA section 40(2), the Ombudsman may order a data controller to realize the right of access of the data subject or rectify an error. The numbers of these cases are illustrated by the following figure.

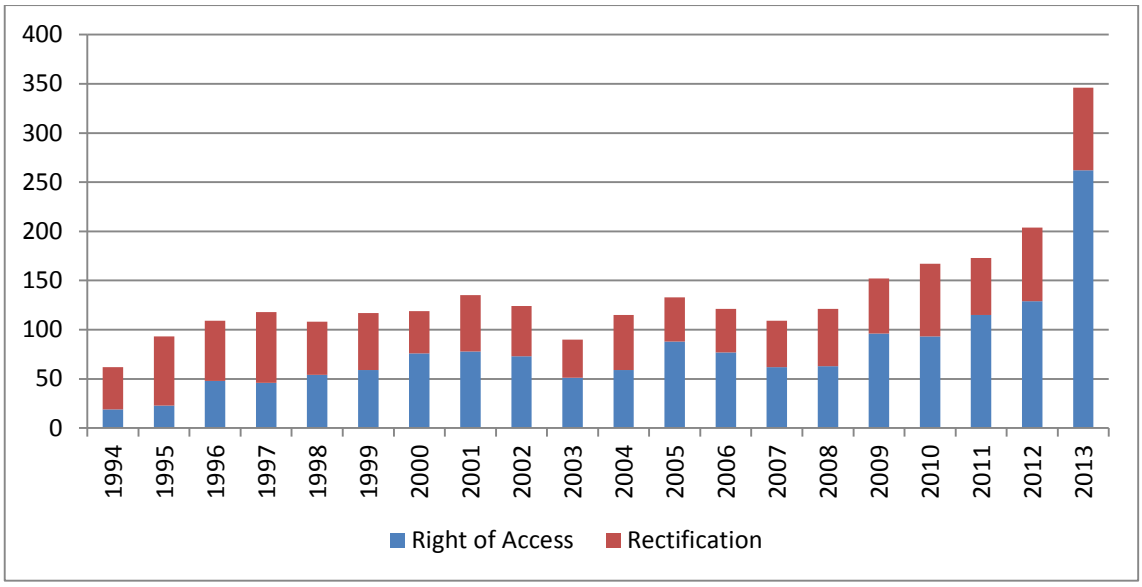


Figure 6. Received Requests from Citizens on Right of Access and Rectification Matters, 1994–2013.

[36] The data for matters concerning the personal identity code is limited to years 2000–2005. Matters initiated by "others" have almost exclusively been initiated by data controllers, but include investigations initiated by the Ombudsman.

The share of these cases is relatively low compared to the overall number of cases (lately approximately 6 percent, in the 1990s slightly more than 10 percent). As can be observed, in particular the number of requests concerning the realization of right of access has been on an upward trend. The increase is focused at the statistical subcategory "other registers".[37] Out of the 129 received requests in 2012, 59 fell in this category, while 40 concerned healthcare and 30 law enforcement. In 2013, also requests concerning law enforcement registers increased dramatically, most likely in connection with the media coverage on certain specific cases. As a result, the total number of right of access requests doubled to 262 (119 other, 112 law enforcement and 31 healthcare). The number of rectification requests has stayed more stable. Nevertheless, during the 2000s, rectification requests regarding personal data in the healthcare sector have increased. In 2013, out of the 84 received rectification requests, 49 concerned healthcare, 3 credit data and 32 other registers.[38]

Under PDA section 45(1), the Ombudsman's decisions can be appealed to an Administrative Court and further to the Supreme Administrative Court. In its published decisions, the Supreme Administrative Court has generally upheld the Ombudsman's decisions,[39] but in two cases it has decided otherwise, interpreting the right of access and right to rectification more restrictively than the Ombudsman.[40]

4.3 Communication, Information Services and General Guidance

The Office of the Data Protection Ombudsman has two main channels of communication towards the general public. One of them is the magazine *Tietosuoja*, which has appeared quarterly since 1989. *Tietosuoja* is nowadays published in co–operation with the Data Protection Board, the Finnish Communications Regulatory Authority and the National Board of Patents and Registration of Finland. The magazine currently has approximately 3.500 subscribers, most of which are organizations, and is aimed mainly at professionals working in the field of data processing, data protection and data security. An Internet version of the magazine is available for subscribers. In addition, some open–access articles have been published on the magazine website for non–subscribers.[41]

[37] In the statistics, both of these case groups have been divided into three categories by sector. The statistical categories for right of access matters are healthcare, credit data and other. The statistical categories for rectification matters are healthcare, law enforcement and other.
[38] During and in the aftermath of the 1990s depression, the bulk of rectification requests concerned credit data, in particular default of payment entries.
[39] See KHO 23.4.2001 T 926, KHO 27.2.2007 T 457, KHO 13.11.2008 T 2861 and KHO 2012:51.
[40] See KHO 18.8.2006 T 1976 and KHO 27.9.2013 T 3084.
[41] The Internet version can be accessed at <http://www.tietosuoja–lehti.fi> [8.4.2014].

The second and perhaps currently the most significant channel of communication is the *Tietosuoja.fi* website[42], opened in 1997. The website, available in Finnish, Swedish, and to a very small extent in English, serves as the home site of the Office and is aimed both at citizens and data controllers, and reaches a much larger audience than the magazine. During the last few years the site has been viewed by approximately 500.000 visitors per year. The long–serving site version from 2004 was upgraded in May 2014. Even with an added blog and a new poll function, the website functions mainly as a traditional one–way information channel. Basic information for both data subjects and controllers is provided, as well as answers to frequently asked questions and a collection of decisions of the Ombudsman; there is, however, no comprehensive database of these decisions.

Additionally, a collection of guides, models and forms is available on the website. Since the beginning of its operation, the Office has spread information by publishing various guides aimed at data subjects, data controllers and other professionals working with data processing. Nowadays these are mainly distributed via the website in PDF format rather than as traditional paper copies.

For providing general information and consultation, the Office also maintains a phone service, usually attended by two employees at a time. The numbers and topics of phone calls have not been recorded, but according to information given in the annual reports of the Office, the role of the phone service has been significant.[43]

4.4 Co–operation with Interest Groups and Codes of Conduct

The Ombudsman and the Office participate in dozens of committees, working groups and other groups that facilitate communication, consultation and co–operation with different interest groups. Permanent sectoral working groups handle matters relating to data processing in, e.g., education, healthcare, social services, telecommunications and marketing. The Office also organizes lectures and seminars in co–operation with different interest groups.

According to PDA section 42, the Ombudsman may check if the sectoral *codes of conduct* drafted by data controllers are in conformity with the PDA and other provisions relating to the processing of personal data. Section 42 has its roots in Article 27 of the Data Protection Directive; no such provision was contained in the PDFA. The Ombudsman does not formally

[42] <http://www.tietosuoja.fi> [15.5.2014].
[43] A standard statement in the annual reports estimates the number of answered calls at approximately 7.500 per year.

approve codes of conduct. Instead, she or he issues an opinion, which does not legally validate the code. However, checked codes of conduct may be influential in defining the exact content of general PDA provisions[44] or good processing practice in the processing of personal data on the sector in question.

Although not stated in the Act, the Ombudsman provides guidance and feedback to the drafters also in earlier stages. Therefore codes of conduct can be seen as co–regulation between data controllers and the Ombudsman. Because the Ombudsman does not approve the codes and has no power to formally order drafters to modify them, not all codes submitted to be checked necessarily reflect the Ombudsman's interpretation of the law. In addition, the drafters of sectoral guidelines have no legal obligation to consult the Ombudsman. However, if the drafted code is not submitted for checking, it cannot be considered a code of conduct in the sense of PDA section 42 or Article 27 of the Directive.

Since 2000, the Ombudsman has checked over 50 codes of conduct for different sectors, drafted by various state and municipal authorities, interest groups, associations and even single private companies. The most prolific drafter has by far been the Population Register Center, which had asked for the Ombudsman's opinion 17 times by October 2013.

4.5 International Co–operation

The Ombudsman's statutory duty for international co–operation has always formed a significant part of the operation of the Office. [45] In the early years, the co–operation could be divided into Nordic co–operation and wider, worldwide international co–operation. After Finland's accession to the European Union in 1995, co–operation within the Union has gained a more and more pronounced role. This is also evident in the following figure, although the nature and significance of international co–operation cannot be fully depicted by mere numbers of statistical "cases".

[44] For example, the duty of care (section 5) or the necessity requirement (section 9).
[45] Originally, the duty was stated in section 2 of the DPO–DPB Decree of 1987. In 1994, the provision was moved – with a slightly altered wording—to section 5 of the new DPO–DPB Act.

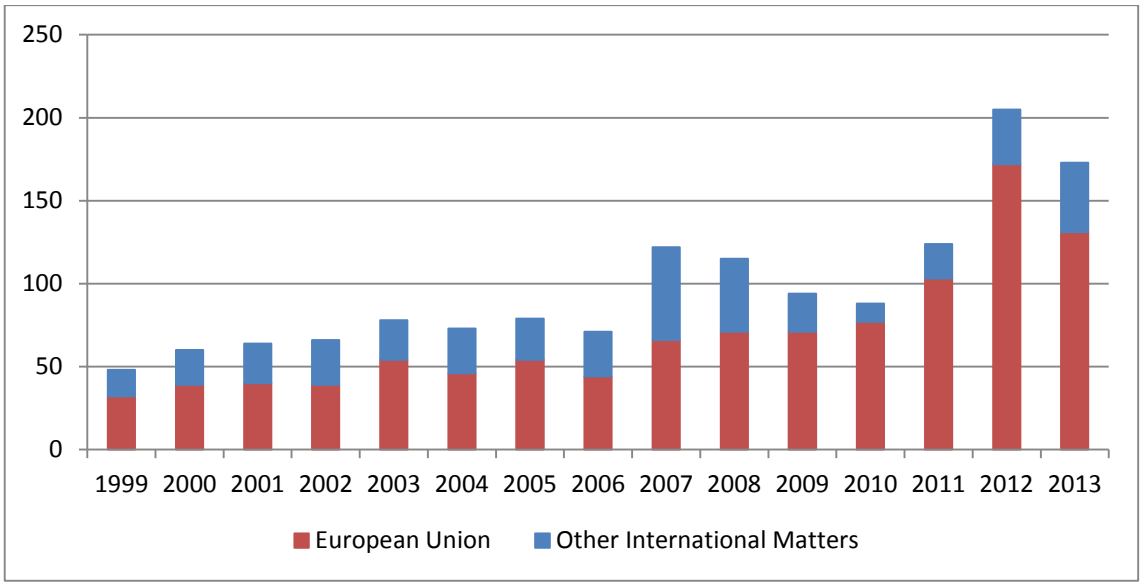


Figure 7. Distribution of matters relating to the EU and other international matters, 1999–2013.

The Nordic data protection authorities organize regular meetings with each other. In these meetings—earlier usually three per year, nowadays a single yearly meeting with the program divided into sub–meetings—actual matters relating to data processing and data protection have been discussed. The Nordic data protection authorities have also organized several inspections and surveys on selected target branches or topics together with each other. Because Finland, Sweden and Denmark are EU member states, the Nordic co–operation partly intertwines with co–operation on the EU level.

The annual international conferences of data protection and privacy commissioners have served as the most important forums of worldwide co–operation in data protection matters. The first conference was organized in 1979, and the Ombudsman has participated in them ever since the late 80s. Members of the Office staff and representatives of the Data Protection Board have often attended the conferences, as well. The Ombudsman and the Office have also participated and lectured in various other international seminars, conferences and meetings.

The European Union facilitates many types of communication and co–operation between national data protection authorities. As provided in PDA section 38(3) and Article 28(6) of the Data Protection Directive, the Finnish authorities co–operate with the data protection authorities in other Member States, providing executive assistance, where necessary. In addition to executive assistance and other direct co–operation between authorities, a key arena for discussion is the Article 29 Working Party (WP 29).[46] WP 29 is an independent, advisory

[46] See <http://ec.europa.eu/justice/data–protection/article–29/index_en.htm> [16.4.2014].

group composed of representatives of national supervisory authorities, the European Data Protection Supervisor and a representative of the Commission.[47] The Ombudsman also participates in the operation of various other EU working groups and several joint supervisory bodies, e.g., those of Europol, SIS and EURODAC.

The volume and significance of EU co–operation has been on a constant rise, and the new General Data Protection Regulation will surely contribute to this development. Among other things, the Regulation will replace the WP 29 with a new European Data Protection Board, which will be trusted with ensuring the consistent application of the Regulation and given new instruments for achieving this purpose.

4.6 Hearings and Expert Opinions

One significant activity of the Ombudsman is to provide expert opinions to different authorities and the Parliament in relation to proposed legislative and administrative reforms. The authorities' duty to hear the Ombudsman is stated in PDA section 41(1). Although this kind of a duty was not mentioned in the PDFA, in practice the Ombudsman was heard already before the PDA when drafting legislation that concerned personal data.[48]

The aim of the hearings is to give the Ombudsman a chance to promote good data processing practices, privacy and data protection issues in advance before any reforms are made. On average, during the 2000s the Ombudsman has given approximately 40 opinions on legislative reforms per year. The numbers of Parliamentary hearings and opinions on administrative reforms have been slightly lower.

In addition, PDA section 41(2) provides that before bringing charges for conduct contrary to the Act, the public prosecutor shall hear the Ombudsman, and when hearing a case of this sort, the court shall reserve the Ombudsman an opportunity to be heard. This provision corresponds to PDFA section 47. Conduct contrary to the Act is sanctioned in the Criminal Code of Finland (39/1889) and PDA section 48.[49]

---

[47] The legal basis for the operation of WP 29 is provided in Articles 29 and 30 of the Data Protection Directive. Additionally, Article 15(3) of Directive 2002/58/EC (Directive on privacy and electronic communications) states that WP 29 shall also carry out the tasks laid down in Article 30 of the Data Protection Directive with regard to matters covered by that Directive.

[48] Section 41(1) was included in the PDA due to the requirements of Article 28(2) of the Data Protection Directive.

[49] PDA section 48(1) contains references to following provisions of the Criminal Code: chapter 38, section 9 (data protection offence); chapter 38, section 8 (computer break–in); chapter 38, sections 1 and 2 (secrecy offence and secrecy violation); and chapter 40, section 5 (breach and negligent breach of official secrecy). Data protection offence, computer break–in, secrecy offence and breach and negligent breach of official secrecy are punishable with a fine or imprisonment. Secrecy violation and personal data violation, defined in PDA section

Since the turn of the millennium, the number of these hearings has been on a rapid rise. During the first half of the 1990s there were only a few of these cases per year, and during the second half of the same decade on average 15. The PDA era average is well above 60 per year, with a record number of 233 opinions issued in 2013. This development can be attributed to the change of society and increased publicity and media coverage of data protection crime, not a legislative amendment, as the current provision corresponds to the old PDFA provision.

A third group of hearing matters is related to permissions to use data from the national healthcare registers for research purposes. Before granting such permission, the designated authorities must reserve the Ombudsman an opportunity to be heard. Although there has been some variation between different years, since the mid–1990s the overall level of these matters has remained rather stable, averaging approximately 60 cases per year. The record number from 2011 was 89.

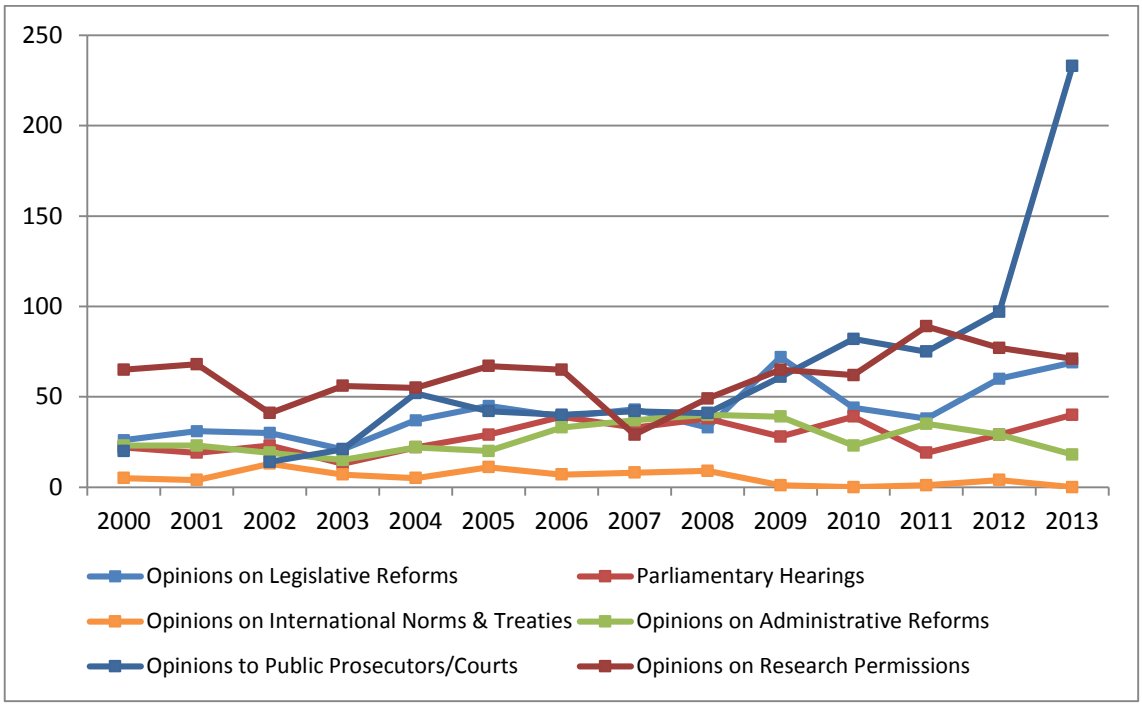


Figure 8. Opinions and Hearings of the Data Protection Ombudsman, 2000–2013.

5. The Data Protection Board

5.1 General Information

The Data Protection Board consists of a chairman, a vice–chairman and five regular members, who all have personal alternate members. The Government nominates the members

48(2), are punishable with a fine only. For example, a violation of PDA section 32 concerning data security is punishable under the last provision and can therefore not lead to imprisonment.

for a 3–year period, which can be renewed multiple times.[50] The terms have, in fact, been renewed quite often and the composition of the Board has therefore remained rather stable. Illustratively, the Board has been chaired by *Pekka Nurmi* ever since 1988.

According to the current DPB–DPO Decree, all members of the Board must be familiar with data file activities. The chairman, vice–chairman and one regular member are required to hold a law degree, and IT expertise must be represented in the Board.[51] The Board may have a full–time secretary and part–time secretaries who are required to hold law degrees.

5.2 Duties and Powers

The Data Protection Board is an entity with a decision–making role.[52] The Board convenes when necessary and decides on matters as provided in the PDA. The decisions can be grouped into two main categories: 1) permissions and 2) orders and prohibitions.

In permission cases, the data controller applies for a permission to derogate from certain provisions that set limits on the processing of personal data. Under the PDFA, section 37 gave the Board a very wide mandate to grant permissions to derogate from practically any provision of the PDFA. The PDA, however, lays much stricter boundaries on the situations in which the Board may grant permissions. The current key provision is PDA section 43.

> ***Section 43 — Power of the Data Protection Board to grant permissions***
>
> *(1) The Data Protection Board may grant a permission for the processing of personal data, as referred to in section 8(1)(9), if the processing is necessary, otherwise than in an individual case, in order to protect the vital interests of the data subject, or in order to use the public authority of the controller or a third person to whom the data is to be disclosed. The permission may be granted also in order to realise a legitimate interest of the controller or the recipient of the data, provided that such processing does not compromise the protection of the privacy of the individual or his/her rights.*
>
> *(2) The Data Protection Board may grant a permission for the processing of sensitive data, as referred to in section 12(13), for a reason pertaining to an important public interest.*
>
> *(3) The permission may be granted for a fixed period or for the time being; it shall contain the rules necessary for the protection of the privacy of the data subject. These rules*

[50] The selection of members is prepared at the Ministry of Justice. Members are chosen from different kinds of background organizations in order to make use of wide experience and maintain a certain amount of balance in the board. However, members are to act impartially and they do not formally represent their respective interest groups when the Board makes decisions.

[51] Section 2 of the DBP–DPO Act of 1987 specifically required *two* members of the board to be experts on IT matters.

[52] Sometimes it has been characterized as a quasi–tribunal.

may be amended or supplemented at the request of the Data Protection Ombudsman or the data subject, if this is necessary owing to a change in circumstances.

In effect, the Board may use its discretion to grant an exception from only two specific provisions of the PDA, which concern the general prerequisites for processing and derogations from the prohibition to process sensitive data.

While permission applications are lodged by data controllers, orders and prohibitions are sought by the Data Protection Ombudsman when she or he considers the processing of personal data unlawful, and when consultation and other "soft" methods are not effective. The Board's power to give orders and prohibit unlawful processing of personal data is regulated in PDA section 44.

Section 44 — Orders of the Data Protection Board

At the request of the Data Protection Ombudsman, the Data Protection Board may:

(1) prohibit processing of personal data which is contrary to the provisions of this Act or the rules and regulations issued on the basis of this Act;

(2) in matters other than those referred to in section 40(2), compel the person concerned to remedy an instance of unlawful conduct or neglect;

(3) order that the operations pertaining to the file be ceased, if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interests or rights, provided that the file is not set up under a statutory scheme; and

(4) revoke a permission referred to in section 43, where the prerequisites for the same are no longer fulfilled or the controller acts against the permission or the rules attached to it.

The PDA limited the Board's duties and powers also otherwise. The Board no longer grants permissions for archiving, disclosure of personal data to abroad, or storage of credit data.[53] Under the PDFA, cases concerning the data subject's right of access to her or his own personal data and rectification of inaccurate data could also be brought to the Board if the data controller objected to the Ombudsman's initial decision in such a matter. These cases were relatively common in the Board, especially in the late 1990s as the Board processed—and turned down—numerous data subjects' requests for removal of registry entries concerning default of payment. Under PDA sections 40(2) and 45(1), the Ombudsman's decisions in these matters are binding, and can be appealed to an Administrative Court and further to the Supreme

[53] The permits for disclosure to a foreign country were replaced by free movement of personal data within the European Union and the new PDA provisions concerning transfer of personal data to outside of the European Union. Archiving permits are nowadays granted by the National Archives Service, and the processing of credit data is regulated in the Credit Data Act.

Administrative Court. Therefore, the Board no longer deals with cases coming directly from data subjects.

In addition to decision–making in individual cases, under PDA section 38(2) the Board deals with questions of principle relating to the processing of personal data, where these are significant to the application of the PDA. The exact meaning of this provision is debated, and the Board itself has been rather reluctant to provide general answers to these questions of principle in its binding decisions. Instead, it has seen the provision to be connected principally to its role in giving statements and opinions to authorities and other organizations. Further, DPB–DPO Act section 2 states that the Board is also to monitor the need of development of legislation concerning the processing of personal data and to issue initiatives it deems necessary. However, the Board has not been particularly active in doing so. Therefore, it can be noted that decision–making has always formed and still clearly forms the bulk of the Board's operations.

5.3 Case Statistics

The change from the almost limitless, discretionary exceptions of the PDFA to the strictly regulated, specific permissions of the PDA and the otherwise diminished duties of the Board have had a significant impact on the workload of the Board. Immediately prior to the entry into effect of the PDA, the Board decided 30–40 cases per year, most of which concerned permissions. In 1993, prior to an amendment in which provisions on processing of personal data for the purposes of genealogical research and public registers were included in the PDFA, the Board decided a record number of 59 cases. Since the PDA entered into effect, the highest number of decisions per year has been 17 in 2011, with the average staying well below 10 decisions per year. The permission applications still account for a majority of the cases. However, the spike in 2011 was caused by the Ombudsman seeking prohibitions on several pay–day loan providers that utilized inadequate practices for identification of loan–seekers. The development of the case–load is illustrated by the following figure.

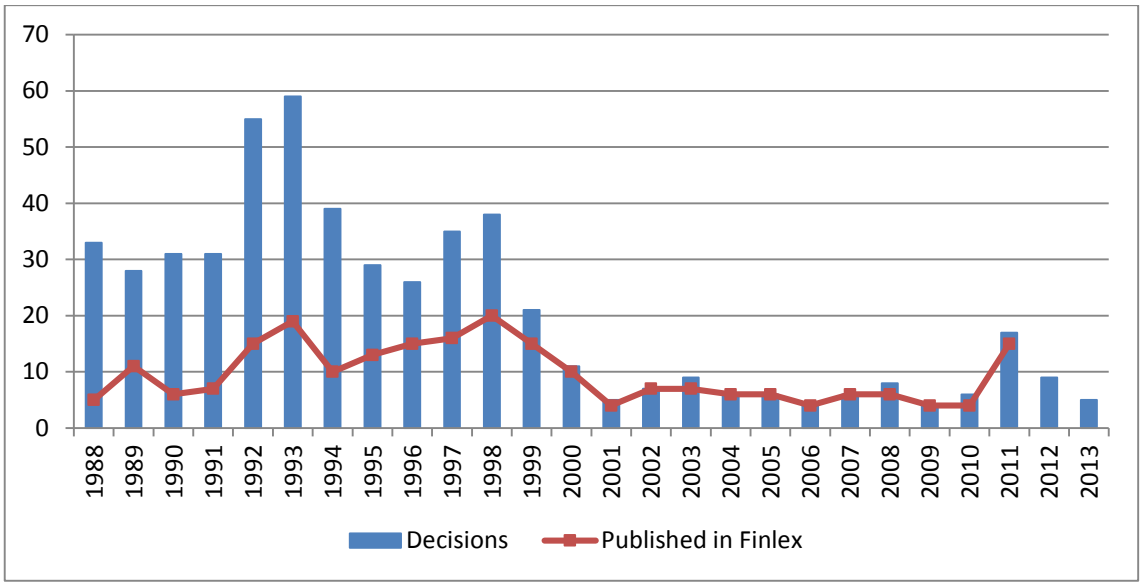


Figure 9: Decisions of the Data Protection Board, 1988–2012.

Because the Board only convenes when needed, the noticeable drop in the number of cases has also brought a decrease in the number of Board meetings and expenses. Whereas the Board's expenses were close to half a million FIM (approximately 113.000 euro) in the mid–1990s and the Board convened over 20 times a year, in the 2000s the expenses have averaged approximately 15.000 euro per year, and there have been 4–8 meetings per year. This has also led to average processing times getting longer.

Since 2000, almost all of the decisions of the Board have been published in Finlex[54], the freely available online database containing legislative and other judicial information. In contrast, only a limited number of the PDFA era decisions have been published.

5.4 Typical Cases

The early years of the Board were marked by permission applications regarding public registers and genealogical research. In a typical application, numerous exceptions were sought simultaneously, for example from the requirement of exclusivity of purpose, connection requirement, and the provisions concerning necessity, mass disclosure, and transfer of data to outside Finland. In 1994, provisions on processing of personal data for the purposes of genealogical research and public registers were included in the PDFA, which removed the need for many of these applications, resulting in a decrease in their numbers. In the late 1990s, a large group of permission applications concerned different kinds of blacklists and documentation of defaults and misuse. During the PDA era, a typical permission application

[54] <http://www.finlex.fi> [7.4.2014].

has concerned direct access to the so–called THS identification query system.[55] These applications have been pursued by numerous insurance companies and professional debt collectors, and have generally been accepted.

Although even in the early years of the Board there were some applications regarding computer–based data files and data processing, a major part of the cases concerned manual data files throughout the 1990s, and very seldom was the actual legal question even remotely related to the use of computers. In the 21st century, however, the development of IT and networks has been clearly visible from the evolution of the Board's cases. In 2006, for example, the Board was asked to rule on whether or not IP addresses are personal data.[56] In the last few years the Board has also decided on permissions to collect of street imagery and WiFi information for the purposes of Internet–based location and map services—which the Board has granted, under certain conditions. Furthermore, during the PDA era, order and prohibition cases initiated by the Ombudsman have almost exclusively had to do with Internet or mobile phone services. A majority of these cases have concerned the identification practices employed by various pay–day loan providers.

5.5 Appeals

Under PDFA section 38, the Board's decisions could be appealed directly to the Supreme Administrative Court (hereinafter: SAC). As provided in PDA section 45(1), the path of appeal now goes through an Administrative Court. The longer path may be problematic in two ways: the time to final decision may become too long, and fewer court cases are likely to be published as the SAC publishes its decisions far more actively than the regional Administrative Courts. With the longer path, fewer cases reach the SAC.

The Finlex database currently lists 21 decisions on appeals against the Board's decisions. Out of these published decisions, 18 are from the PDFA era and mere three concern the PDA. Another factor contributing to the decrease of the number of court cases are the diminished powers of the board, which have led to fewer cases in the Board, as well.

Out of the 18 PDFA era cases, 15 concerned permissions.[57] In 11 cases, the appeal was filed by the data controller, in three cases by the Ombudsman. One case concerned the right of

[55] Direct use of this system does not fall within the general prerequisites for processing because the system operates in such a way that the queries may also return personal data of persons to whom the data controller has no connection.
[56] According to the Board, they are.
[57] See KHO 1989–A–9, KHO 1989–A–10, KHO 1989–A–12, KHO 1990–A–3, KHO 1990–A–4, KHO 1990–A–5, KHO 1990–A–6, KHO 6.3.1991 T 770, KHO 1992–A–10, KHO 1992–A–11, KHO 1992–A–29, KHO 1993–A–4, KHO 1995–A–11, KHO 1996–A–6 and KHO 3.3.1999 T 339.

appeal of a data subject and a third party, which was found to be lacking. In eight cases, the SAC upheld the Board's decisions, whereas in the remaining seven it either altered or overturned the decisions, in part or in full. Most of these cases were returned to the Board.

Two of the PDFA era cases concerned prohibitions issued by the Board on request of the Ombudsman.[58] One of the two decisions was overturned in part, the other one in full. In the remaining PDFA era case the SAC dismissed an appeal against the Board's decision not to investigate a request for rectification of corporate credit data due to lack of jurisdiction.[59]

One of the three published PDA era decisions concerned the scope of the Board's power to grant permissions, which the SAC interpreted in the same way as the Board and dismissed the appeal.[60] The other two SAC decisions concerned the same case in which a company published personal tax information in magazines and transferred the data to another company to be published via an SMS service. Following complaints, the Ombudsman requested the Board to prohibit such activities. The Board rejected the request, whereupon the Ombudsman brought proceedings before the Helsinki Administrative Court, which also rejected his application, and consequently an appeal before the SAC. The SAC, having consulted the Court of Justice,[61] returned the case to the Board for issuing the prohibition.[62]

In almost a half of the published decisions on appeals, the Board and the SAC have not seen eye to eye. However, the published decisions do not really tell much; this already because of the fact that there are very few of them.[63] There are no comprehensive statistics on how the Administrative Courts have treated the appeals, but in general, the decisions of the Board are appealed against rarely, and even more rarely do the decisions get overturned.[64]

6. Concluding Remarks

While the legislative reforms have certainly played a role in the development of the Finnish data protection authorities, technological advancements and the change of society towards a network society have affected what kind of questions, requests and legal problems

[58] See KHO 1992–A–6 and KHO 1995–A–13.
[59] See KHO 1998:35.
[60] See KHO 2011:16.
[61] See Case C–73/07 (Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, Judgment of 16 December 2008).
[62] See KHO 2007:9 and KHO 2009:82.
[63] Looking at just published cases is not illustrative also because there is likely to be a selection bias: decisions dismissing baseless appeals are not published as often as decisions concerning the "hard cases" where the courts might see the legal question differently and where they wish to send a signal.
[64] Interview of Pekka Nurmi, 14.10.2013, Helsinki.

the authorities have to deal with. When the authorities began, manual data files and local, non–networked computer–based data files still formed the main regulatory field of data protection. Since then, computerized data processing has become the standard, and the sheer amount of data processed has been rapidly increasing—even if we are not talking about *big data*. Networks have become the standard gateway for transferring data, which is regularly crossing national and regulatory borders. Networks and surveillance of online behavior of individuals are also used for large–scale gathering of personal data, data mining, and flat–out spying. Therefore, the threats and risks concerning privacy and personal data in the 2010s are much different in nature and in volume from those faced in the 1980s. This is evident in the everyday operation of the data protection authorities. All in all, the statistics as well as the cases also make it clear that the development has been more evolution than revolution: change hasn't happened in one night. It has not been slow, either: the entire timespan is barely over quarter of a century, after all.

This being said, statistics make it clear that the entry into effect of the PDA also contributed to increasing the workload of the Ombudsman and especially to decreasing the number of cases decided by the Board. This is consistent with the goals of the reform: to shift focus from decisions and reactions to consultation and forethought, a strategy which is necessary to secure the best possible realization of fundamental rights in a rapidly changing world. The Ombudsman and the Office are clearly in the driver's seat, although the Board still has its own, strictly limited and regulated role and function.

While the current, proven Finnish model is not the only option, the evident need for dedicated data protection authorities can hardly be called into question nowadays.[65] However, the Finnish authorities have to continue to adapt and evolve. The next major challenge they are facing seems obvious: the EU Data Protection Reform. As of the time of writing, the division of the new duties provided in the upcoming General Data Protection Regulation—or the final content of the Regulation—has not been set in stone yet. While predicting the future is known to be perilous, I feel tempted to claim that for the authorities, especially the Ombudsman and the Office, the trend towards more and more EU–level co–operation and other international activities will not only continue but also intensify in the near future.

[65] As mentioned in chapter 3 of this paper, initially the establishment of dedicated data protection authorities was not deemed necessary by everyone. Even in the early 1990s, the abolishment of the data protection authorities was suggested in a report ordered by the government and prepared by Juhani Kivelä. However, such action was apparently never seriously considered.

THE PRIVACY RISKS OF BIOMETRIC IDENTIFICATION

Juhani Korja

Dr. of Law, University of Lapland, Finnish Police super indendant, juhani.kuparinen@jippii.fi

Keywords: ***Biometrics, privacy, surveillance***

Abstract: *Heightened security concerns arising from the growth of various forms of crimes have led to increased interest in the development and application of the technologies of surveillance. A prominent form of these new surveillance technologies is biometric identification. The term biometrics has traditionally stood for the statistical study of biological phenomena. Because of the growing usage of automated systems for person identification by government and industry, biometrics is now commonly referring to the automated methods of identification to determine the identity of a person based on physiological or behavioral characteristics. Biometric identification raises multiple rational concerns wherever it is applied. The increasing use of biometrics has led to fears that a surveillance society will be created, with scant room for personal privacy and autonomy. With the growing use of biometrics, it is paramount importance that discussions about the ethical, social and legal implications relating to the technology take place. Because of the basic nature of biometric technology, the issue of privacy is a central concern. In this article, I will examine biometric identification as the technology of surveillance. Related to this analysis, I will discuss the privacy concerns biometric identification raises. As a part of this analysis, I will view the informatization of the human body, which can be seen as the basis of biometric identification.*

1. Introduction

A billboard advertising a new science fiction miniseries towers above Manhattan. Although it is unremarkable at first glance, those who stop to look at the ad unknowingly relinquish significant personal information. How is this possible? “Billboards that look back” are the latest in high–tech advertising. Each contains a tiny biometric camera that analyzes the viewer´s facial features for gender and age.[1]

This example is to demonstrate how surveillance is increasing in the modern society. The main reason for the increase in surveillance is said to be security. Heightened security concerns arising from the growth of various forms of crimes have led to increased interest in the development and application of technologies of surveillance.[2]

[1] Clifford, ”Billboards That Look Back”. News article in New York Times.

[2]The term “technology of surveillance” refers to technologies that facilitate the collection and processing of personal data for the purposes of influencing or managing those whose data have been collected. Liu, Bio–privacy, p. 3

A prominent form of these new surveillance technologies is biometric identification. It should be pointed out that biometric identification cannot solely be seen as a surveillance technology. Biometric identification has a practical application in both the public and private sectors, and the technology can be applied across several areas. But the surveillance and control potential of the technology is the reason why biometrics is attracting controversy. This technology has advanced to the point where it possesses the capability to threaten the most basic democratic notions of individual autonomy and privacy. Because of these reasons, biometric identification should be considered as a technology of surveillance.

The tragic experiences of terrorism, especially 9/11, have made us pay more attention to security. One way to increase security is the use of devices that utilise biometric data, such as a fingerprint, to identify an individual. In today´s discussion, the technology that utilises biometric data is also seen as a silver bullet for terrorism. The utilisation of biometric technology enables automation in the identification process thus making the identification more accurate and effective. Using biometric information in documents such as passports and ID cards is therefore an effective way to prevent identity theft. It also makes it very difficult to exploit lost and stolen documents. As a part of the efforts to enhance security, governments around the world are investing large sums of money and human resources in biometric technology. This also acts to accelerate the use of biometrics among the private sector entities.

2. Surveillance as a means of power

Earlier the word "surveillance" was reserved for highly specific scrutiny of suspects. From this, the situation has changed. Surveillance nowadays occurs routinely, locally and globally. One might even say that surveillance has become an unavoidable feature of everyday life in the modern society. As the example in the Introduction shows, organizations of all kinds engage in surveillance, and citizens, consumers and employees generally comply with this surveillance[3].

But what is meant by the term "surveillance"[4]. The Concise Oxford Dictionary equates surveillance with "supervision, close observation and invigilation of individuals who are not trusted to work or go about unwatched"[5]. While this definition has a traditional sounding ring to it, it captures a dimension of surveillance, which is increasingly discussed in current debates

[3] There are three different roles in which an individual comes across with biometrics: 1) citizen, 2) employee and 3) consumer / customer. See further i.e.: Nanavati, S. – Thieme, M. – Nanavati, R.:Biometrics. Identity Verification in a Networked World, p. 147.
[4] Surveillance can also be seen as a form of social sorting. See further: Lyon, Surveillance as Social Sorting.
[5] Fowler, H.W. – Fowler, F.G., The Concise Oxford Dictionary, p. 1302.

– trust. Trust is the traditional element of and a motive for surveillance: surveillance is practiced because those in positions of authority do not trust those below them. It should be reminded, however, about the other definition of surveillance. In addition, surveillance can be defined as the collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered, and does not usually involve embodied persons watching each other[6]. Surveillance can therefore be considered as the practice of gathering and sorting data with one explicit purpose: to influence and manage the data target. Surveillance can therefore be seen as a means of power[7] in the modern surveillance society[8].

When talking about surveillance, one distinction must be made. Surveillance is not only the act of the government. As the example shows, also the private sector is very active in the field of surveillance. Therefore, it is necessary to make a distinction between public and private surveillance. Public surveillance is surveillance actions the government does in the name of i.e. national security. Private surveillance, on the other hand, refers to the surveillance activities of the private sector, such as advertising agencies and other consumer related companies, and is executed in many different ways in order to influence in and gain control over i.e. consumer habits. In these surveillance sectors, the methods of surveillance are very similar, but they differ in the motive of the surveillance activities.[9] As the proportion of private sector surveillance is expanding, the threat to privacy and other fundamental freedoms comes not, with few exceptions, from the state but from the private sector. This is why the aforementioned distinction between private and public surveillance is important.

But when talking about surveillance there seems to be one question above all that arises: How much surveillance is too much? The answer to this question is actually quite simple. Like Benjamin Goold has said: we know that there is too much surveillance when citizens begin to fear the surveillance activities, and no longer feel free to exercise their lawful rights[10].

---

[6] Lyon, Surveillance Society: Monitoring Everyday Life, p. 2

[7] The term "power" is defined as "capability of acting or of producing an effect" or "authority or capacity to act that is delegated by law or constitution". Merriam–Webster´s Dictionary of Law, p. 366.

[8] Surveillance societies are societies which function, in part, because of the extensive collection, recording, storage, analysis and application of information on individuals and groups in those societies as they go about their lives. *Surveillance Studies Network*, An introduction to the surveillance society. Available at: http://www.surveillance–studies.net/?page_id=119. See further on surveillance societies i.e. Lyon, Surveillance Society: Monitoring Everyday Life. *Issues in Society.* Open University Press. Buckingham. 2001.

[9] It should be mentioned that the principal motivator for these two modes of surveillance is the same: to influence and manage the data target.

[10] Goold, B: How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy and the Political Value of Privacy, p. 46

3. What is Biometrics?

Identification[11] is, and has always been, a fundamental component of human interaction. The traditional means of identification, i.e. ID cards and passports, have been the most widely used, and are likely to remain as such for years to come. These traditional means of identification no longer match the need of accuracy expected from identification in the modern society. This is why stronger identification technologies are becoming commonplace. Biometric identification is one such technology of identity.

Because biometric identification refers to such a broad range of technologies, systems and applications, it is essential to discuss the terminology, classifications and unique processes that define biometrics.

According to the American Heritage Dictionary, the term biometrics has traditionally stood for "the statistical study of biological phenomena."[12] Because of the growing usage of automated systems for person identification by government and industry, biometrics now commonly refers to automated methods of identification to determine the identity of a person based on physiological or behavioral characteristics.[13] Several aspects of this kind of definition require elaboration.

Automated use: Biometric technologies are automated: computers or machines are used to verify or determine identity through behavioral or physiological characteristics.

Physiological or behavioral characteristics: Biometric identification is based on the measurement of distinctive physiological and behavioral characteristics. Physiological biometrics are based on direct measurements of a part of the human body. Behavioral biometrics, on the other hand, are based on measurements and data derived from an action and therefore indirectly measure characteristics of the human body.[14]

Identification: Identification can be seen to consist of three different terms: 1) identification, 2) authentication and 3) verification. These terms are closely related but still separate. Authentication is the act of confirming the truth of an attribute of a single piece of data or entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the

[11] Identification is the action to attribute "identity" to an item. Mordini – Tzovaras – Ashton, Introduction, p. 1
[12] The American Heritage Dictionary. Available at:
http://www.ahdictionary.com/word/search.html?q=biometrics
[13] It is said that biometrics is the application of modern statistical techniques to measure the human body and is therefore defined as the science of using biological information for the purposes of identification.
[14] Compare with Russell and Gangemi who have said that only the technologies based on physiological characteristics can be called biometrics. See further Russel, D. – Gangemi, G.T. Sr.: Computer Security Basics. O´Reilly and Associates, Inc. USA 1991.

process of actually confirming that identity. In contrast with authentication and identification, verification can be defined as an act of confirmation of truth or authority.[15]

Identity: Identity is often misunderstood in the context of biometrics. It is, therefore, important to draw a distinction between an individual and an identity. An individual is a singular, unique entity, but an individual can have more than one identity[16]. This distinction between an individual and identity is important because it establishes limits on the type of certainty that a biometric system can provide. It can also have significant bearing on biometrics and privacy. Biometric identity verification and determination are only as strong as the initial association of a biometric with an individual. A user who enrolls in a biometric system under a false identity will continue to have this false identity verified with every successful biometric match.

With a range of available attribute choices, a question arises: What are the desirable characteristics of a biometric attribute for automatic identification? The answer is distinctiveness, robustness and measurability. These characteristics are deemed the most important. Distinctiveness implies that the attribute must show great variability over the general population so as to yield a unique signature for each individual. Robustness determines how the attribute varies over time. Ideally, it should not change over time. The measurability refers to the ease with which it can be sensed.[17]

In addition, it is desirable that the attribute is acceptable and universal. The acceptability implies that no negative connotation is associated with it. The universality of an attribute determines the fraction of the general population that possesses it in multiples.[18]

---

[15] Also the terms determining and verifying identity represent a fundamental distinction in biometric usage. The reason for this is that some biometric systems can determine the identity of a person from a biometric database without that person first claiming an identity. The traditional use of fingerprints in crime investigations is a good example of an identification deployment. This kind of an identification system stands in contrast to verification systems, in which a person claims a specific identity and the biometric system either confirms or denies that claim.

[16] Saarenpää distinguishes six different legal viewpoints into identity:

1. identification data
2. surveillance
3. data protection
4. the market
5. the media
6. information security

Saarenpää, Tietoturva ja tietosuoja, identiteetin näkökulma, p. 39–47.

[17] Wayman, J.L.: Fundamentals of Biometric Technologies, available at http://www.engr.sjsu.edu/biometrics/publications_tech.html. See also Sethi, I: Biometrics: Overview and Applications (2006).

[18] Wayman, J.L.: Fundamentals of Biometric Technologies, available at http://www.engr.sjsu.edu/biometrics/publications_tech.html. See also Sethi, I: Biometrics: Overview and Applications (2006). ibid.

3.1 When and how? – The development of biometrics

Biometric identification, as we know it today, has become a part of the network society in a few decades because of the advances in computing technology. Biometric identification as an idea, however, is not new.[19] The technology is based on the same basic principles and thoughts laid down centuries ago.

Just like every technology, biometrics has its own history and generations, which have affected on the present form of the technology. Even though biometrics is not new, it is still in its technological infancy, taking the first real steps towards being a mature technology.

The first generation of biometrics began when an anthropologist Alphonse Bertillon started to identify criminals using their distinctive physiological features, such as the structure and shape of the scull and shoulders.[20] This method, called bertillionage, was developed for the increasing needs for stronger and better method of identification. This system was called anthropometrical signalment and was very basic in its implementation.[21] But Bertillon's system was not without flaws. It failed to answer the accuracy demands required from the system. As an example is a case from 1903 in which the system failed to distinguish identical twins from one another.

Because of the flaws, the Bertillon system was short–lived. Soon after its introduction, the distinctiveness of human fingerprints was established. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records as Bertillon's method did but was based on fingerprint patterns and ridges. This system was developed in India by Edward Henry, Inspector General of Police, Bengal, India. This system, named after its creator, the Henry System, is still in use for classifying fingerprints.

The first true applications of the biometric identification as known today began to emerge in the latter half of the twentieth century, coinciding with the giant leaps taken in the computing technology. In the 1970s the first automatic fingerprint identification systems became available.[22] This can also be seen as the end of the first generation of biometrics, because the older methods of biometric identification, such as the Bertillon system and the Henry System,

[19] Quantitative measurement of biological human traits for the purpose of identification dates back to at least the 1880s, though the use of human characteristics to recognize people has arguably always been an integral part of human interaction.
[20] Bertillon was probably the first to realize that certain elements of the human body did not change over time. Garfinkel, Database Nation: The Death of Privacy in the 21st Century, p. 39.
[21] Liu, Bio–Privacy, s.4. Although the bertillionage system cannot be considered as a biometric system because of its lack of automation, it has nevertheless laid the foundation for modern day biometric systems.
[22] Jain, A.K. – Kumar, A.: Biometric Recognition: An Overview, p. 55–56.

could not anymore answer the needs of identification in the technologically and digitally developing network society.

Since late 1990s – four factors, reduced cost, reduced size, increased accuracy and increased ease of use – have combined to make biometrics an increasingly feasible solution.[23] The terrorist act of September 11 has been another major factor spurring innovation in biometric applications. The unfortunate events of 9/11 forced governments all around the world pay more attention to robust identification documents. The reason for this is the inability of the traditional methods of human identification to meet the growing demands for stringent security in applications such as national ID cards and border crossings.

Because of the aforementioned reasons and because of the digitization of the society, the second generation of biometric identification started to develop in the late 1990s. And since the early 2000s biometric identification systems have been a part of everyday life in the modern society. Examples of these second generation biometrics are the US–VISIT –system (based on fingerprints), the Privium System used at Schiphol Airport (based on iris) and the SmartGate –system at Sydney Airport (based on face).[24]

These aforementioned reasons alone do not explain enough the rapid growth of biometric technologies. In addition to these reasons explained above, there is a real need for stronger identification in the society, which is derived from the societal, political and technological developments in the society[25]. As the society develops, there is a growing need for stronger, faster and more accurate methods for identification in the new digital environment. The next generation, or the third generation, of biometric identification will have to answer the legal and technological challenges of this new technology.

But nowadays biometrics are much more than a replacement for the traditional identification methods. Millions of people use biometric technology in applications as varied as time and attendance, voter registration, international travel and benefits dispersal. Biometrics can be used for security, for fraud reduction, for convenience, even as an empowering technology, depending on the application.[26]

---

[23] According to Ishwar Sethi, a number of factors have led to the unprecedented growth of biometrics. Chief among them are decreasing hardware costs, growth in networking and e–commerce, and greater emphasis on security and access control. Sethi, I: Biometrics. Overview and applications (2006), p. 118.

[24] Jain, A.K. – Kumar, A.: Biometric Recognition: An Overview, p. 56.

[25] New information technologies and improved transportation, have enabled many things, i.e. commerce, to be done at a distance in the past half century. This has led to the need for stronger methods of identification in the society.

[26] India has deployed the world´s largest biometric identification program. The idea of the program is to register every citizen´s fingerprint into a registry, and replace passports and other ID cards as an identification method. BBC News, available at http://www.bbc.co.uk/news/world–asia–india–16979875.

3.2 The Human Body as a Source of Information

The human body has been largely invisible on the horizon of law and discourse on data privacy. Much more prominent on that horizon has been the computer. The main concern within the field of data privacy has been the impact of this computing technology on the privacy and related interests of human individuals. In this context, concern for the body as such has manifested itself mainly as anxiety over what might be visited upon one's physical self as a result of the gathering and further processing of personal data. At the same time, one should not forget that the discussion about the nature and value of privacy has often had, as a point of departure, concern for the integrity of the physical self.[27] One development is the merger of information and communication technology with biotechnology to create i.e. biometrics.

All biometric applications have one thing in common: in each one, parts or aspects of human bodies are represented in digital form, enabling new ways of performing identities and embodiment. This has been a catalyst for the emergence of a new body ontology.[28] This new ontology redefines bodies in terms of, or even as, information.[29]

The notion of body ontology enables us to describe the way the human body is implicated in a process of co–evolution with technology. Over the past century, various developments have resulted in a set of body ontologies that quite explicitly construe the body in terms of flows of information and communication patterns.[30]

The co–evolution of various information technologies and bodies generates confusions, casts doubts, and generates needs for explication of issues previously considered self–evident. This comes to the surface in particular when normative implications of contemporary technological developments are considered. The growth in generation and processing of this body data regularly generates public controversy, for the recognition of the enormous potential for misuse of these types of information is widely shared. In trying to draw lines, and separate legitimate use from misuse, concepts and values are invoked and applied in contexts and

---

[27] Bygrave, The body as data? Reflections on the relationship of data privacy law with the human body, p. 1–2.

[28] The sciences and practices of genetics have generated a body ontology that takes the building blocks of the body to be ”information”. For example, the human DNA itself is a code to be broken in order to enable us to read the blueprints of life. Genetics can also be regarded as the epitomization of a more general development to which all biometric technologies contribute. A development that can be characterized as the *informatization of the body*, a relatively new phenomenon in which the human body appears to be redefined as an entity made of information.
Ploeg, Genetics, biometrics and the informatization of the body, p. 44.

[29] Ploeg, Biometrics and the body as information, p. 64. In the fields of informatics and computer science, the notion of 'data' usually denotes signs, patterns, characters or symbols which potentially represent some thing (a process or object) from the 'real world' and, through this representation, may communicate information about that thing. The 'information' as such denotes the semantic content of the data communicated to a person.
Bygrave, The body as data? Reflections on the relationship of data privacy law with the human body, p. 2.

[30] Ploeg, Biometrics and the body as information, p. 64

discursive spaces they were not invented for. The ensuing discursive exercises sometimes reveal how the ontologies implied in these concepts and values do not entirely match with the informatization and digitization processes currently evolving.[31]

According to Ploeg, today, the socio–technical production of social categories and identities through IT–mediated surveillance relies increasingly on a gradually extending intertwinement of individual physical characteristics with information systems.

In the light of these facts, it could be argued that there is a distinction to be made between the body itself and information about, or digital representations of that body, in the context of the rapidly extending practices of registration and processing of digital data on physically identified individuals.

3.3 Privacy Concerns associated with Biometrics

Biometric identification raises multiple rational concerns wherever it is applied. Most forms of technology inspire, however, not only hope but also fear. Biometrics is no exception. The development of innovative technology has almost always raised new legal concerns, and especially in the case of biometric technology. The increasing use of biometrics has led to fears that a surveillance society will be created, with scant room for personal privacy and autonomy. With the growing use of biometrics, it is paramount importance that discussions about the ethical, social and legal implications relating to the technology take place.

Because of the basic nature of biometric technology, the issue of privacy is a central concern. It is unnecessary to engage here in an extensive debate over the exact meaning of privacy as a concept.[32] It suffices to note that there are two main zones of privacy[33] that are directly pertinent. The first zone is informational privacy and concerns the control of personal information. These interests give rise to attempts to establish rules governing the collection and handling of personal data. The ability to control personal information about oneself is closely related to the dignity of the individual, self–respect and sense of personhood. Informational

[31] Ploeg, Biometrics, p. 65–66.
[32] In Merriam–Webster´s Dictionary of Law the term "privacy" is defined as "freedom from unauthorized intrusion: state of being let alone and able to keep certain especially personal matters to oneself". Merriam–Webster´s Dictionary of Law, p. 379.
[33] Zone of privacy is an area or aspect of life that is held to be protected from intrusion by a specific constitutional guarantee or is the object of an expectation of privacy. Merriam–Webster´s Dictionary of Law, p. 536. Saarenpää has divided privacy as a concept into ten different zones: 1) physical privacy, 2) spatial privacy, 3) social privacy, 4) media privacy, 5) anonymity, 6) data protection, 7) informational ownership, 8) right to be evaluated in the correct light, 9) patient privacy and 10) communicational privacy. Saarenpää, Oikeusinformatiikka, p. 311–317. One zone of privacy could be added to this list: genetic privacy.

privacy is the concern that lies at the very heart of the discussion over the risks and benefits of biometrics.

The second, and often forgotten, zone falls under the rubric of physical privacy with respect to the body itself. This form of privacy is aimed essentially at protecting the dignity of the human person. In the case of biometrics this concerns protection from intrusive searches and seizures, particularly the protection of persons´ physical bodies against invasive procedures. The widespread use of biometric technologies may invade our physical privacy in several ways.

3.3.1 Informational Privacy

Today´s computing technologies allow both public– and private–sector institutions to gather, store and compare a broad range of information about individuals. This ability to compile and share information about individuals can be very easily abused. For this reason, informational privacy is a major concern of privacy advocates.

Biometric technology raises some of the same issues that arise when any personal information about individuals is collected. In the case of biometrics, however, such loss can occur in specific ways that distinguish biometric data from losses involving other personal data. This difference makes concerns about biometric technology of particular importance with regard to privacy protection. For this reason, it is important to explore the types of special risks that the technology poses.

Informational privacy concerns associated with biometric technology, basically, revolve around five issues. These are unnecessary collection, unauthorized collection, unauthorized use, identity theft and decreasing of anonymity.

3.3.1.1 Unnecessary collection

A central principle of rules grounded in informational privacy is that the collection of personal information should be limited to those data that are necessary and relevant to a legitimate purpose. One of the primary privacy concerns with respect to the potential massive use of biometric technology is that more personal information than is necessary and relevant will be collected, used and disclosed. The concern therefore is that the excessive collection of biometric information will result in heightened monitoring of individuals. Biometric identification is normally deployed in order to address a specific identity verification problem, i.e. controlling physical access. From privacy perspective, deploying biometrics in environments in which they provide ill–defined or nominal benefits can undermine

informational privacy.[34] Like Prins has said: "Fundamental rights are likely to be violated in case biometrics is used for applications merely requiring a low level of security. In the end, organizations and government agencies must demonstrate that there is a compelling interest in using biometric technology and that an obligatory fingerprint requirement is reasonably related to the objective it is required for."[35]

3.3.1.2 Unauthorized collection

Biometric information, like other personal data, can be gathered or stored easily and surreptitiously without the subject having control or knowledge of this process. These data can then be collected, tracked and profiled without the data subject´s knowledge. The deployment of facial–recognition technology by the Tampa police at the 2001 Super Bowl in Florida and the possibility of scanning passports from a distance are good examples. Given the indiscriminate nature of a number of surveillance systems, covert surveillance of the general public may become the norm. The use of biometric technology has the great potential to enhance law enforcement´s ability to gather data without the participation or even awareness of the individual. This necessarily involves the collection and analysis of various body characteristics.[36]

Although only certain biometric technologies, such as facial–scan and voice–scan, are capable of collecting biometric information without the subject´s knowledge, the increased deployment of biometric technologies does bring with it the possibility that institutions could gather and process biometric information without consent.[37] The use of biometric information without the free consent of the data subject is a serious derogation of an individual´s right to privacy.[38]

3.3.1.3 Unauthorized use

Unauthorized uses of the biometric technology can be seen to present the greatest risk biometrics pose to privacy. It is not normally intended uses of biometrics that are seen as problematic. It is the risk of unauthorized use of biometric data, however, that defines many informational privacy fears. The unauthorized uses can be divided into three categories:

---

[34] Liu, Bio–Privacy, p. 72–73.
[35] Prins, Biometric technology law, making our body identify for us: legal implications of biometric technologies, p. 161 Computer Law & Security Report, 14(3), p.159–165
[36] Liu, Bio–Privacy, p. 74
[37] Nanavati, S. – Thieme, M. – Nanavati, R., Biometrics. Identity Verification in a Networked World, p. 241.
[38] See also Liu, Bio–Privacy, p. 75

a) Unauthorized disclosure

Unauthorized disclosure is a violation of a fundamental privacy principle: individual has the right to exercise control over his / her own personal data. If biometric information is shared without an individual´s authorization, the potential uses which the data will be put, the information with which it is linked and the security measures used to protect biometric information are all unknown.

b) Tracking / surveillance

Tracking refers to the possibility of linking different transactions to build profiles. Biometric data offer strong evidence of one´s identity since they represent relatively unique biological characteristics which distinguish one person from another. As biometric data can usually be linked to only one individual, they therefore act as a powerful, unique identifier that brings together disparate pieces of personal information about an individual.

Biometric data not only allow individuals to be tracked, but create the potential for the collection of an individual´s information and its incorporation into a comprehensive profile by linking the databases together. Because some biometric technologies can be used covertly, it is also possible that individuals could be tracked clandestinely. One such case occurred in 2001 during Super Bowl in Tampa Bay, Florida. Law enforcement authorities scanned the crowd using facial recognition technology in an attempt to identify criminals and terrorists.[39]

Biometric technology is seen as especially threatening since the technology is often positioned as the identifier that cannot be lost. This unchangeable, unique identifier could be used to track information about an individual across databases. Unique identifiers can be used by malicious parties to monitor, link and track a person´s daily activities across disparate databases and information.

c) Function creep[40]

The threat to privacy arises not from the positive identification that biometrics provide. The problem is the ability of third parties to access this in an identifiable form and link it to other information. This results in secondary use of that information

[39] Woodward, J.D, Jr: Super Bowl Surveillance: Facing up to Biometrics, Rpt. IP–209 (Rand Publications, 2001), available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP209.pdf. See also Woodward, J.D, Jr: Biometrics – Facing up to Terrorism, Rpt. IP–218 (Rand Publications 2001), available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP218.pdf.

[40] Function creep can be defined as the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. Nanavati, S. – Thieme, M. – Nanavati, R., Biometrics. Identity Verification in a Networked World, p. 242. See more about function creep i.e. Greenleaf, G.: Function creep – defined and still dangerous. Submission on the revised ID Card Bill. Available at: http://www.cyberlawcentre.org/ipp/id_card/DHS_submission_CLPC.pdf

without the consent of the data subject. This erodes the personal control of an individual over the uses of his or her information. For this reason function creep is unavoidable. It has been claimed that any high–integrity identifier, such as biometrics, represents a threat to civil liberties, because it represents the basis of a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. This kind of power is opposite to the idea that an individual should have some expectation of privacy in the society.[41]

3.3.1.4 Identity theft

Identity theft stands for the unauthorized use of another´s means of identification for the purpose of committing theft or another crime.[42] The heightened concern of identity theft has been one motivator to the development of biometric technology. The reason for this is the technology´s capability to stronger identification, which is to protect the identity of the individual. Biometric information makes it harder to commit identity theft. In France, for example, identity theft protection has been used to justify the collection of fingerprints. The European Court of Human Rights overruled such a ground in the case M.K. v. France (no.19522/09, 18.7.2013) stating it would enable fingerprint collection of all citizen without an acceptable reason.

Despite the fact that biometric identification can be used to prevent identity theft, the unintelligent and irresponsible use of biometrics might cause spoofing. A system based solely on biometrics is therefore very vulnerable to identity theft, especially if the same biometric data is used in several independent systems. Losing the biometric to an identity thief would therefore be harmful to the individual. In such a case, the individual would have two choices: 1) either he will void the biometric identifier in all of these systems and thus excludes himself (partly) on the outside thereof, or 2) he takes the risk that the identity may at any time be used by the identity thief.[43]

[41] Expectation of privacy can be defined as a belief in the existence of freedom from unwanted intrusion in some thing or place. Merriam–Webster´s Dictionary of Law, p. 179.
[42] Merriam–Webster´s Dictionary of Law (2011), p. 489.
[43] This view is shared by Kindt. *Kindt*, Privacy and Data Protection Issues of Biometric Applications, p. 346. See also *Gripjink*, Trend report on biometrics: Some new insights, experiences and developments, p. 262.

3.3.1.5 Decreasing of anonymity

The word **"**anonymity" is derived from the Greek word *anonymia*, which means "without a name" or "namelessness". In colloquial use, the word "anonymity" typically refers to the state of an individual's personal identity, or in the case of biometrics personally identifiable information, being publicly unknown.

In the network society anonymity is a central concept. The ever increasing collection of personal information, especially biometric information, is gradually leading to the loss of anonymity. In the modern society anonymity can therefore be seen decreasing.

Anonymity is linked with autonomy and a person´s sense of freedom. The increasing collection of personal data is making tracking and profiling of individuals more and more convenient for government and private organizations. Anonymity can be seen as the only effective tool available against this profiling and tracking. In the network society, anonymity is highly appreciated simply because it is fundamental to the sense of freedom and autonomy. The ever–increasing identification in the society can be seen as demeaning, or implicit recognition that the society´s organizations are exercising power over them. But will the deployment of biometric technology undermine anonymity? Liu has stated that despite the fact that there exist many methods of eroding anonymity, it cannot be denied that biometric systems are detrimental to anonymity.[44] Biometric systems are also created to identify people, and it will not be difficult to link a biometric identifier to other personal information. If personal information could be linked and identified using biometric data, the ability to remain anonymous would be severely diminished. In the case of biometrics, it will be almost impossible to have absolute anonymity, or even semi–anonymity[45] due to the technology´s ability to identify people.

3.3.2 Physical / Personal Privacy

In addition to the aforementioned informational privacy concerns, biometrics raises concerns also from the physical / personal privacy viewpoint.

Physical privacy can be defined as the right to be free from unwanted, unreasonable intrusions or searches of one´s body. Physical privacy is concerned with bodily integrity and is indirectly concerned with emotional integrity together with human dignity. What should be

[44] Liu, Bio–Privacy, p. 78.
[45] According to Liu, semi–anonymity could be possible, if biometric systems are carefully designed from the start. Liu, Bio–Privacy, p. 79.

noted is that physical privacy can also be defined as freedom from contact or monitoring by others. This might include searches, video surveillance and other forms of monitoring.

Physical or personal privacy as it relates to biometrics is not usually in the focus of the privacy discussion. But there cannot be drawn a clear line between an individual´s bodily integrity and information. The new intensive forms of linking, tracking, controlling and manipulating of persons through their biometric information therefore become possible indications that some form of physical privacy is at stake. Such forms of surveillance may not violate bodily integrity in the traditional sense associated with physical intrusion, but physical privacy might still be jeopardized, especially once the collection of body–related biometric information such as DNA becomes easy and inconspicuous[46]. Despite the fact that informational privacy is the main concern associated with biometric identification, at least some methods of biometric identification are a serious breach of physical privacy and bodily integrity.

The reason for these physical or personal privacy concerns is that the use of biometric technology can be seen inherently offensive, invasive, or disturbing. While some personal privacy fears may be derived from inchoate informational privacy concerns, this reaction is often attributable to cultural, religious or personal beliefs.[47]

4. Conclusion

As of today, biometric identification is gaining significant attention due to the technology´s ability to protect humans and resources from potential non–legitimate user attacks in high security environments. It is a well–known fact that humans have used body and other characteristics for recognizing each other long before biometric identification technology appeared. But during these past few decades, the biometric technology has emerged as a viable solution for a range of applications where a person's identity must be verified or determined. This technology is no longer a science–fiction solution: biometric technologies are being deployed to solve security problems, to help companies generate revenues, and to protect personal information. The reason for the vast growth of biometric technologies is simple. Biometrics has been made possible by the explosive advances in computing power.

The legal issues and concerns associated with new technologies quite often are overrun by the technological hype. The challenge, therefore, is to break this hype and ensure intelligent

[46] Liu, Bio–Privacy, p. 79. In the case of DNA, for example, there cannot be found a clear point at which bodily matter becomes information.
[47] Nanavati, S. – Thieme, M. – Nanavati, R., Biometrics. Identity Verification in a Networked World, p. 243–244 and Liu, Bio–Privacy, p. 79–81.

and responsible use of biometrics as the technology moves into the mainstream. The unintelligent and irresponsible use could have severe repercussions to the individual´s rights.

In the EU, any collection and processing of personal data, such as biometrics, must comply with fundamental rights laid down in the Charter of Fundamental Rights of the EU and with the relevant EU secondary legislation. The main challenge is, however, to put these legal safeguards in practice and to render them effective. This implies that the introduction of any new instruments requiring the collection and exchange of personal data pass both the necessity and proportionality tests.

EU data protection law sets out robust principles ensuring that the use of biometrics respects fundamental rights of individuals. This is an essential part in building trust of individuals with regard to the processing of their biometric personal data and respect for their dignity.[48]

The use of biometric technologies is becoming increasingly prevalent in individuals´ lives. Biometrics can prove to be a useful tool for recognizing or verifying the identity of a person based on physical or behavioral characteristics.

Technologies often have, however, an inherent logic or bias which may strongly influence the way in which they are being used. The bias of these technologies of surveillance is essential to augment surveillance capabilities. Therefore the development of surveillance has also been driven by new forms of technology.[49] It could almost be said that surveillance is a self–sustaining engine where the technological development is the fuel.

The realization of an Orwellian future can´t be excluded, in particular if security remains the major driver for this technological area. It is unlikely that new methods to look underneath the skin can be restricted to protective or purely supportive applications. Once the knowledge is created, it will be used for all the purposes we might be afraid of.

The subject can also be approached from a more theoretical point of view. There is a political and philosophical discussion about the use of biometric technology. This discussion aims to understand how diverging assessments of biometrics function in the public construction of the technology involved.[50] This discussion is not seeking to counter the constructions of technology by claiming that technology in itself is neutral, or that the degree of its threat to privacy depends on the specific use to which it is being put. In the case of biometrics, it can be claimed that the technology is highly political and normative. This is because technology can

[48] Reding, Privacy Implications of Biometrics, p. V–VI.
[49] Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, p.
[50] See Ploeg, The Machine–Readable Body. Shaker Publishing. Maastricht 2005.

be seen as the outcome of social processes and choices, and is continually in the process of being made.[51]

The deployment of biometric technology has raised radical, diverging positions on the issue of whether biometric technology is dangerous to individual privacy and democracy in general. On the one hand, biometrics is seen as one of the most serious among many technologies of surveillance that are threatening the freedom of individuals and of societies.[52] This technology enables the bringing together of disparate pieces of personal information about an individual. On the other hand biometrics constitutes a potential solution to privacy by safeguarding identity and integrity, and could even be privacy–enhancing when combined with cryptography techniques.[53]

At the heart of the debate on biometric identification´s role in the surveillance age, however, is the balance between human rights and civil liberties and the intrusion on these rights in the name of safety.[54] In the surveillance age and especially in the case of biometrics, this balance might have to be given another thought. Like the history has shown, the balance between security and privacy has never been static. It has been shifting in favor of security whenever the society is faced with significant threats to public safety. And this is why we have ever expanding surveillance.

Because biometric technologies are based on measurements of physiological or behavioural characteristics of the human body, the increasing use of biometrics raises questions about the technology´s impact on privacy. The one responsible for the deployment of the biometric system should therefore address the following questions, which are necessary to ensure that biometric system design and deployment does not undermine or threaten personal or informational privacy, before deploying biometric systems.[55]

What are the major privacy concerns associated with biometrics?

What types of biometric deployments require stronger protections against privacy invasiveness?

What biometric technologies are more susceptible to privacy–invasive use?

What types of protections are necessary to ensure that biometrics are not used in a privacy–invasive fashion?

[51] See i.e. Ploeg, The Machine–Readable Body.
[52] See i.e. Clarke, Biometrics and Privacy. Available at: http://www.rogerclarke.com/DV/Biometrics.html.
[53] See i.e. Woodward, Biometrics: Identifying law & Policy concerns.
[54] Cavoukian, Public Safety is Paramount – But Balanced Against Privacy, p. 1
[55] Nanavati, S. – Thieme, M. – Nanavati, R.:Biometrics. Identity Verification in a Networked World, p.237.

Taking in to account all that has just been said, the role of biometrics in the surveillance age will remain to be seen. Biometric technology, as a tool, has a great potential in protecting privacy. But, unfortunately it can also be seen as a threat to the freedom of individuals. Whilst recognizing the benefits of biometrics, the principal question is: How to ensure that biometric technologies are designed and used in a way that respects fundamental rights? When answering the question, one should remember that we as individuals and citizens have the right to go about our lives anonymously from the eyes of the government and other organizations, and that we as a society should highly value individual privacy, both physical and informational. Because biometrics is perceived to impinge upon privacy, it should be viewed with suspicion. No matter what the benefits of biometrics are, it is therefore very important to keep in mind the many risks and concerns this technology poses to the fundamental rights. These are especially the risk to the right to privacy and to data protection.

This technology should therefore not be taken lightly. We should avoid getting caught up in the technological hype surrounding biometrics. The decision of deploying biometric identification should be based on careful and strict consideration, in which the fundamental rights are the starting point.

In a world of identity politics and risk management, surveillance is turning decisively to the body as a document for identification, and as a source for prediction. When this is combined with the fact that in the 20th century biometric identification has become the technology of the future, which is an ever developing area of technology. For these reasons there is a real need for the legal expertise in the field of identification.

TIETOTURVALLISUUDEN SÄÄNTELY TAUSTA, TEKIJÄT JA TULEVAISUUS MISSÄ MENNÄÄN NYT?

Eija Alavesa

OTM Lapin yliopisto, Trainee District Judge at District Court of Vantaa, eija.alavesa@oikeus.fi

1. Johdanto – tietoturvasääntelyn taustaa

Elämme digitalisoitumisen aikakautta, jonka tieto– ja viestintäteknologia on mahdollistanut.[1] Tiedosta on tullut tärkeä resurssi. Muutos on vaikuttanut siihen, kuinka yksilöt ja organisaatiot toimivat ja kuinka tietoa käytetään, liikutetaan ja jalostetaan. Tiedon määrä kasvaa räjähdysmäisesti, jolloin tietoa on käytettävissä koko ajan enemmän. Kehitys pitää sisällään sekä mahdollisuuksia että uhkia.[2]

Tietoyhteiskunnan säädöspuitteet mukaan lukien tietoturva otettiin esille jo 1970–luvulla.[3] Euroopan yhteisön kiinnostus tietokoneistumiseen liittyviin ongelmiin alkoi samoihin aikoihin. Tietosuojaa koskeva lainsäädäntökeskustelu 1970–luvulta liittyi myös osaltaan tietoturvaan.[4] Tietoturvallisuus on kuitenkin paljon vanhempaa perua. Se on yksi turvallisuuden muoto, joka on ollut mukana yhteiskunnan kehityksessä jo paljon pidempään. Tietoa on suojeltu eri tavoin muun muassa lukoin ja salaisuuksin.[5]

Osana informaatioinfrastruktuurin kehitystä tietoturvallisuus on tullut hitaasti yhdeksi tärkeimmistä kysymyksistä verkkoyhteiskunnassa, jossa tietoliikenteet ja –verkot ovat keskeisessä osassa yhteiskunnan toimintoja.[6] Yhteiskunnan, yritysten ja organisaatioiden keskeisimmät toiminnot ovat nykyään sidoksissa tieto– ja viestintätekniikan (ICT, Information and Communication Technology) järjestelmien toimintaan. Tieto– ja viestintätekniikan moitteeton toiminta on nykyään liiketoiminnan ehdoton edellytys. ICT:n hyödyntäminen on toisaalta tuonut mukanaan tietoriskit. Nämä tietoriskit ovat globaaleja ja nopeasti muuttuvia.

[1] Puhutaan digitalisaatiosta, joka on sekä kokonaisvaltaista toimintatapojen uudistamista, sisäisten prosessien digitalisointia että palveluiden sähköistämistä (Digitalisaatio, valtiovarainministeriö 2015).
[2] Andreasson & Koivisto 2013, s. 11.
[3] Huuhtanen 2001, s. 10.
[4] Still 1997, s. 109.
[5] Saarenpää 2012b, s. 531.
[6] Råman 2006, s. 818.

Internet on tuonut mukanaan myös ammattimaisen rikollisuuden, haittaohjelmat ja luvattoman tunkeutumisen tietojärjestelmiin.[7]

Tietoturvallisuutta pidettiin pitkään, jopa 1990–luvun puoliväliin asti, toisarvoisena teknisenä kysymyksenä tietojärjestelmien suojaamisessa.[8] Hyvin ominaista tietoturvan kehityksessä on ollut myös se, että tietojärjestelmien ja tekniikan kehittyessä tietoturvallisuus on hoidettu jälkijunassa.[9] Toisaalta 1990–luvun alussa tietojärjestelmät oli rakennettu erillisiksi järjestelmiksi. Järjestelmien välillä ei ollut tuolloin yhteentoimivuutta. Turvallisuuskysymykset keskittyivät lähinnä sisäisiin uhkiin. Järjestelmiä suojattiin ulkomaailmalta pitämällä ne suljettuina. 1990–luvun puolivälissä alettiin puhumaan avoimista verkoista. Tämän muutoksen taustalla oli internetin kehittyminen. Kehitys johti tietojärjestelmien yhteenliittymiseen. Kehitystä joudutti erityisesti taloudellisten ja sosiaalisten hyötyjen tavoittelu. Vuonna 2008 myös OECD (Organisation for Economic Co–operation and Development, taloudellisen yhteistyön ja kehityksen järjestö) tunnisti internetin taloudellisen kehityksen yhdeksi tekijäksi, joka mahdollisti kasvun, vaurauden ja elämän laadun parantumisen koko yhteiskunnassa. 1990–luvun puolivälin jälkeen tietovarantojen kasvu, yhteiskunnan riippuvuus tietotekniikasta ja internetistä nostivat tietoverkkorikollisuuden ja muut ulkoiset uhkat suurimmiksi turvallisuutta vaarantaviksi tekijöiksi organisaatioissa.[10]

Verkkoyhteiskunnassa tietoturvallisuus on paljon enemmän kuin ohjeiden tasoinen tekninen tai rikosoikeudellinen kysymys. Tietoturvallisuus on esimerkiksi yksilön näkökulmasta eräänlainen metaperusoikeus eli tietoturva on perusoikeuksien toteutumisen edellytys. Ilman tietoturvaa tietotuoja perusoikeutena ei voisi toteutua. Yksilöllä on oikeus tietoturvalliseen informaatioinfrastruktuuriin.[11] Käytännön toimijat näkevät usein tietoturvan osana yrityksen toiminnan välttämätöntä edellytystä. Kun taas puolestaan oikeudellinen näkökulma tietoturvaan lähtee yksilöstä ja yhteiskunnasta. Tietoturvallisuudessa on ennen kaikkea kyse yksilön oikeuksien ja yhteiskunnan toiminnan turvaamisesta.[12] Tietoturvallisuuden sääntely koskee samalla tavoin sekä yksityisen että julkisen sektorin toimintaa.

Sähköinen viestintä ja sähköiset infrastruktuurit ja palvelut ovat nykyään taloudellisen ja yhteiskunnallisen kehityksen olennaisia tekijöitä. Niillä on yhteiskunnassa merkittävä rooli ja

[7] Porvari 2012, s. 1.
[8] Råman 2006, s. 818.
[9] Porvari 2012, s. 8.
[10] The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy, OECD Digital Economy Papers No. 209, s. 5–8.
[11] Saarenpää 2012b, s. 449–450 & Råman 2006, s. 818.
[12] Råman 2006, s. 818.

niistä on itsessään tullut kaikkialla läsnä olevia hyödykkeitä. Viestintäverkot toimivat lisäksi sosiaalisten muutosten ja innovaatioiden käynnistäjinä. Häiriöt viestintäverkoissa voivat aiheuttaa huomattavia fyysisiä, yhteiskunnallisia ja taloudellisia haittoja. Tarvitaan toimia, joilla parannetaan viestintäverkkojen suojaa ja häiriönsietokykyä.[13] Internetin verkko– ja tietoturvasta on tullut yhä tärkeämpi. Jos internet ei toimi, seuraukset voivat olla erittäin vakavat.

Tässä kirjoitelmassa ensimmäisenä selvitetään, mitä tietoturvallisuus tarkoittaa. Tämän jälkeen selvityksen kohteena ovat tietoturvan erilaiset näkökulmat, joista käydään läpi muutama. Esiteltävät näkökulmat eivät ole tyhjentäviä, mutta ehkäpä keskeisimpiä, kuten yksilön, valtion, organisaation ja teknologian näkökulmat. Osana yksilön näkökulmaa esitetään myös lyhyesti tietoturvan ja tietosuojan välinen suhde, jota tarkennetaan myöhemmin selvitettäessä tietoturvan metaperiaate luonnetta. Tietoturvatyössä erityisen tärkeää on kansainvälinen yhteistyö, josta kerrotaan tietoturvan näkökulmien jälkeen. Tämän jälkeen päästäänkin luontevasti selvittämään Euroopan unionin toimijoita ja tietoturvaan liittyvää unionin sääntelyä. Seuraavaksi piiriä pienennetään entisestään ja katsannon kohteeksi tulevat Suomen tietoturvasääntely ja suomalaiset tietoturvan toimijat. Lopussa kerrotaan vielä tietoturvasääntelyn tulevaisuudesta ja sääntelyn vaihtoehdoista sekä nykypäivän ja tulevaisuuden haasteista.

2. Tietoturvallisuus

2.1 Luottamuksellisuus, eheys ja käytettävyys

OECD:n neuvoston tietoturvallisuusperiaatteita koskevassa suosituksessa vuodelta 1992 tietoturvallisuuden päämääränä on suojella tietojärjestelmiä käyttävien tahojen intressejä haitoilta, jotka syntyvät informaation ja tietojenkäsittelyn luottamuksellisuuden (confidentality), eheyden (integrity) ja käytettävyyden (availability) puutteesta johtuvista vahingoista.[14]

Tietoturvallisuudessa on kysymys informaation ja tietojenkäsittelyn luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvista riskeistä. Informaatioon, sen

[13] Verkko– ja tietoturva voidaan osaksi ymmärtää verkon ja tietojärjestelmien kyvyksi kestää onnettomuuksia ja ilkivaltaa (Komission tiedonanto neuvostolle, Euroopan parlamentille,
Talous– ja sosiaalikomitealle ja Alueiden komitealle, Verkko– ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi (KOM(2001)298 lopullinen), s. 3.

[14] OECD:n neuvoston tietoturvallisuusperiaatteita koskeva suositus 26.11.1992, kohta IV: ”The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.”.

käyttöön tai informaatioväyliin kohdistuvat uhkat ovat lähtökohtana arvioitaessa tietoturvallisuutta ja sen suojaamistarvetta.[15] Yleinen ongelma kuitenkin on, että tietoturvauhkiin ei aina osata varautua, sillä ne eivät tunnu arkipäiväisiltä tai konkreettisilta asioilta sen vuoksi, että riskit eivät välttämättä ole vielä toteutuneet.[16]

Luottamuksellisuus liittyy siihen, että tiedot ovat vain niihin oikeutettujen henkilöiden käytössä. Luottamuksellisuutta pyritään suojaamaan muun muassa käyttäjätunnuksin ja salasanoin. Käytettävyys sen sijaan tarkoittaa, että tiedot ovat saatavissa tietojärjestelmässä oikeassa muodossa ja riittävän nopeasti. Käytettävyyttä ylläpidetään huolehtimalla siitä, että tieto– ja tietoliikennejärjestelmien laitteet ovat tarpeeksi tehokkaita ja käytettävät ohjelmistot soveltuvat mahdollisimman hyvin käyttötarkoitukseensa. Eheydellä puolestaan tarkoitetaan tietojen paikkaansa pitävyyttä ja virheettömyyttä. Eheyteen pyritään pääasiassa ohjelmistoteknisin keinoin. Sovelluksiin voidaan ohjelmoida esimerkiksi erilaisia syöttörajoitteita tai syötteen tarkastuksia.[17]

2.2 Määritelmä Suomen lainsäädännössä

Perinteisesti uhkia ja riskejä on pyritty hallitsemaan myös oikeudellisen sääntelyn avulla. Keinoina on nähty muun muassa toimintoja koskevien sääntöjen sekä niiden rikkomista koskevien sanktioiden asettaminen. Sääntöihin ei automaattisesti kuulu valvovankoneiston asettaminen, vaikka nykyään keskeisenä tekijänä myös tietoturvallisuuden sääntelyssä on nähtävillä erilaisten valvontaviranomaisten asettaminen.[18] Yksi lainsäätäjän toimenpiteistä on perustaa asiantuntijaviranomainen edistämään tietoturvaa ja tätä mahdollisuutta lainsäätäjä on käyttänyt.[19]

Suomen lainsäädännössä tietoturvan määritelmät sisältyvät tietoyhteiskuntakaareen (TYK, 516/2004) ja valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (tietoturvaA, 681/2010).[20] Tietoyhteiskuntakaaressa (1:3 § 28 k) tietoturva on määritelty seuraavasti: ”Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä”. Määritelmä tarkoittaa tietojen luottamuksellisuuden, eheyden ja

[15] Saarenpää–Pöysti (toim.) 1997, s. xxxv.
[16] Andreasson & Koivisto 2013, s. 237.
[17] Hakala et al. 2006, s. 4.
[18] Pöysti 1997b, s. 19.
[19] Pöysti 1997b, s. 43.
[20] Saarenpää 2012b, s. 533–534.

käytettävyyden varmistamista teknisin ja hallinnollisin toimin. Tällaisia tietoturvatoimia voivat olla esimerkiksi laitteille ja järjestelmiin lisätty pääsynvalvonta, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen (esim. loki), tietoliikenteen alkuperävalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpidon asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta, kuten viruksilta ja haittaohjelmilta. Tietoturvatoimia ovat lisäksi tietoliikenteen häirinnän valvonta ja sen estäminen.[21]

Asetuksessa valtionhallinnon tietoturvallisuudesta puolestaan tietoturva–käsite määritellään 1:3 §:ssä 2 kohdassa. Asetuksessa tietoturvallisuudella tarkoitetaan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä. Sähköisen viestinnän tietosuojalakiin verrattuna asetuksessa mainitaan sana ”salassapitovelvollisuus”. Salassapitovelvollisuuden laajuus on riippuvainen siitä, mitä kukin tilanne, säädös, sopimus tai kansainvälinen tietoturvallisuusvelvoite kulloinkin edellyttää.[22]

2.3 Laajennettu määritelmä – kiistämättömyys ja pääsynvalvonta sekä autenttisuus

Perinteistä tietoturvallisuuden määritelmää voidaan pitää osin riittämättömänä, sillä se ei huomioi tiedon tuottajan tai omistajan identiteettiä, eikä laitteistojen tai tieto– ja tietoliikennejärjestelmien arvoa. Perinteistä määritelmää onkin laajennettu lisäämällä siihen käsitteet kiistämättömyys (non–repudiation) ja pääsynvalvonta (access control).[23]

Kiistämättömyys tarkoittaa tietojärjestelmän kykyä tunnistaa ja tallentaa luotettavasti järjestelmää käyttävän tiedot. Samalla halutaan varmistaa tiedon alkuperä tai tunnistaa tietojen luvaton käyttö tilanteissa, joissa tietojärjestelmän omistaja joutuu harkitsemaan esimerkiksi oikeudellisia toimia järjestelmän käyttäjää vastaan. Kiistämättömyys pyritään varmistamaan esimerkiksi käyttämällä salausmenetelmiin liittyviä tunnistusmekanismeja tai biometrisiä tunnisteita. Salausmenetelmiä ovat muun muassa älykortit. Biometriseen tunnistukseen voidaan käyttää sormenjälki– tai silmänpohjantunnistuslaitteita. Pääsynvalvonta puolestaan tarkoittaa niitä menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä.

[21] HE 221/2013 vp, s. 90–91.
[22] HE 53/2010 vp, s. 1.
[23] Hakala et al. 2006, s. 5.

Organisaatiot voivat muun muassa tarvittaessa estää ulkopuolisia tai omaa henkilökuntaansa käyttämästä sen laitteita tai tietoliikenneyhteyksiä henkilöiden omiin tarkoituksiin.[24]

Joskus tietoturvaan voidaan liittää myös kuudes osa–alue, autenttisuus (authentication). Autenttisuudella tarkoitetaan tietojärjestelmän käyttäjien ja siihen osallistuvien laitteiden luotettavaa tunnistusta. Autenttisuus on luottamuksellisuuden ja kiistämättömyyden perusedellytys.[25] Autenttisuus voidaan suomentaa myös todentamiseksi tai oikeaksi todistamiseksi.

2.4 Tietoturvan osa–alueet

Tietoturvallisuus on laaja alue, jota luonnollisesti on helpompi käsitellä, kun se pilkotaan helpommin käsiteltäviin osiin. Tavallisin tapa jaotella tietoturvan osa–alueet on seuraava: hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, laitteistoturvallisuus ja tietoliikenneturvallisuus.[26] Jaottelu on osaltaan keinotekoinen, sillä kaikki osa–alueet vaikuttavat toisiinsa ja niissä on paljon yhteisiä tekijöitä.[27]

Hallinnollisella turvallisuudella pyritään varmistamaan tietoturvan johtaminen ja kehittäminen. Siihen liittyy myös lainsäädännön ja erilaisten yksityisoikeudellisten sopimusten vaikutusten arviointi. Fyysinen tietoturvallisuus merkitsee rakennuksen tilojen ja niihin sijoitettujen laitteiden suojaamista erilaisilta fyysisiltä uhkilta, kuten ilkivallalta tai murroilta sekä ympäristöuhkilta. Henkilöturvallisuuteen kuuluu puolestaan ne toimet, joilla varmistetaan tietojärjestelmän käyttäjien toimintakyky ja heidän mahdollisuudet käyttää tietoja ja tietojärjestelmiä. Henkilöturvallisuuteen liittyy myös henkilöstön kouluttaminen. Tietoaineistoturvallisuus käsittää tietojen säilyttämiseen, varmistamiseen, palauttamiseen ja tuhoamiseen liittyvät toimet. Ohjelmistoturvallisuus liittyy nimensä mukaisesti ohjelmistoihin. Ohjelmistojen testaus kuuluu osaksi ohjelmistoturvallisuutta. Testauksessa varmistetaan ohjelmiston sovellusten sopivuus suunniteltuun käyttötarkoitukseen, ohjelmistojen keskinäinen yhteensopivuus sekä toiminnan luotettavuus ja virheettömyys. Ohjelmistoturvallisuudessa tärkeää on myös ohjelmistojen versiohallinta ja lisenssien hallinta. Laitteistoturvallisuuteen liittyy tietokoneiden ja muiden tietojärjestelmään kytkettyjen laitteiden tarkoituksenmukainen mitoitus, toiminnan testaus, huollon järjestäminen ja

[24] Hakala et al. 2006, s. 5.
[25] Hakala et al. 2006, s. 6.
[26] Hakala et al. 2006, s. 10.
[27] Hakala et al. 2006, s. 12.

varautuminen laitteiden kulumiseen ja vanhentumiseen. Tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisujen turvallisuudesta.[28]

3. Näkökulmia tietoturvaan

3.1 Yksilö

Riippuen näkökulmasta tietoturva voidaan nähdä yksilön näkökulmasta yksityisyyteen sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen liittyvänä asiana. Lisäksi tietoturvaa voidaan yksilön näkökulmasta arvioida esimerkiksi siten, kuinka tietoturva toteuttaa tietosuojan perusoikeutena.

Yksityisen henkilön näkökulmasta tietoturvallisuus on merkittävä tekijä, sillä yksityisten henkilöidenkin tietoja siirretään yhtä enenevässä määrin verkossa. Nämä tiedot saattavat sisältää myös arkaluonteisia henkilötietoja, kuten potilastietoja ja lääkemääräyksiä. Myös verkkokaupan ja sähköisen asioinnin tulee olla luotettavaa.[29] Henkilötietolaki (HeTiL 523/1999) velvoittaa rekisterinpitäjät suojaamaan henkilötiedot asianmukaisesti. Henkilötietolain esitöissä kerrotaan, että rekisterinpitäjän on toteutettava henkilötietojen suojaaminen laittomalta käsittelyltä, erityisesti silloin, kun käsittely muodostuu tietojen siirtämisestä verkossa[30].

Yksilön näkökulmasta arvioitavaksi voi tulla myös yksittäisen henkilön omia mahdollisuuksia edistää tietoturvaa. Tietoturvallisuus on usein pikemminkin ihmisongelma kuin tekninen ongelma.[31] On esimerkiksi varsin tavallista, että yksilöt käyttävät samaa salasanaa ja käyttäjätunnusta useissa eri palveluissa. Saman salasanan käyttö eri verkkopalveluissa avaa mahdollisuuksia verkkorikollisille. Siksi onkin tärkeää, että organisaatiot antavat ohjeistuksia hyvistä salasanakäytänteistä ja muutoinkin neuvovat toimimaan tietoturvallisesti eri järjestelmissä.[32]

3.2 Tietoturva ja tietotuoja

Termit tietoturva ja yksityisyydensuoja sekoittuvat yllättävän usein puheessa toisiinsa. Ne tarkoittavat eri asioita, mutta ovat samalla vahvasti toisiinsa kytköksissä.

[28] Hakala et al. 2006, s. 10–12.
[29] Porvari 2012, s. 3.
[30] HE 96/1998 vp, s. 66.
[31] Porvari 2012, s. 2.
[32] Password reuse opens doors for cyber criminals, InfoWorld 15.2.2011.

Tietosuoja on vakiintunut käytetyksi ilmaisuksi puhuttaessa henkilötietojen suojan oikeudellisesta sääntelystä.[33] Tietosuojalla on ymmärretty perinteisesti henkilötietolain henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista henkilöiden yksityisyyden ja oikeusturvan varmistamiseksi.[34] Käsite tietosuoja on kuitenkin osittain harhaanjohtava. Ensisijaisena tavoitteena on suojata luonnollisia henkilöitä ja heidän oikeuksiaan, ei tietoja.[35] Tietosuojan tarkoituksena on turvata tiedon kohteen yksityisyys, edut ja oikeusturva.[36]

Tietoturvalla tarkoitetaan kaikkia hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys. Tietoturvatoimilla pyritään suojaamaan sekä viestinnän luottamuksellisuutta että yleisemminkin kansalaisten yksityisyyttä ja henkilötietoja. Tietoturvallisesti toimimalla pyritään siis vahvistamaan yksityisyydensuojaa. Voidaan hyvinkin sanoa, että ilman tietoturvaa ei ole olemassa yksityisyydensuojaa.

3.3 Valtio ja lainsäätäjä

Julkisen vallan velvoitteena turvallisuuden takaamiseksi nähdään yhteiskunnan jäsenten suojaaminen rikoksilta ja muilta heihin kohdistuvilta oikeudenvastaisilta teoilta.[37] Yhteiskunnan tasolla tietoturva–asiat voidaan nähdä myös osana kansallista turvallisuutta, osana verkkoturvallisuutta. Lisäksi on aiheellista, että tietoturvallisuutta säädellään lainsäätäjän toimesta.[38]

Yksi informaatiohallinnon keskeisimpiä kysymyksiä on tietoturvallisuuden taso. Hallinnon tietoturva ja hallinnon avoimuus ovat olennaisella tasolla erilaisia asioita. Julkisuus tai avoimuus on yksi hallintoa ohjaava periaate, joka on kirjattu myös julkisuuslakiin (JulkL, 1999/621). Avoimuutta ei saisi toteuttaa kuitenkaan ilman tietoturvaa.[39] Viime aikoina on puhuttu paljon Big Datasta ja Open Datasta (avoin data)[40]. Avoimen datan tarkoituksena on, että erityisesti julkisen sektorin hallinnassa olevaa tietoa jaetaan kaikkien halukkaiden maksuttomaan käyttöön yksityisyyden ja tietosuojan mahdollistamisissa rajoissa. Euroopan

[33] Saarenpää 2012a, s. 318
[34] Ylipartanen 2010, s. 18.
[35] Saarenpää 2012a, s. 318.
[36] Ylipartanen 2010, s. 18.
[37] HE 309/1993 vp, s. 47.
[38] Porvari 2012, s. 3.
[39] Saarenpää 2012b, s. 464.
[40] Nykyään puhutaan myös My Datasta eli omadatasta, jolla viitataan ihmiskeskeisiin henkilötiedon organisointitapoihin. My Datassa yksityisyydensuojan ja tiedon pirstaleisuuden haasteita pyritään ratkaisemaan asettamalla ihminen tiedon hallinnan keskiöön. Lue lisää My Datasta esim. Poikola, Kuikkaniemi & Kuittinen 2014.

unioni on antanut asiaan liittyvän PSI– eli Public Sector Information –direktiivin (2003/98/EY)[41]. Direktiivissä säädellään nimensä mukaisesti julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä.

3.4 Organisaatiot ja johtaminen

Tieto ja tietoturvallisuus ovat nykyisessä yhteiskunnassa ehdottomia edellytyksiä organisaatioiden toiminnalle.[42] Useissa organisaatioissa tietojärjestelmien toiminta ja tietoturvallisuus ovat elintärkeitä tekijöitä organisaation eri toiminnoissa. Tietoturvallisuuden ja tietoriskien seuraaminen ja kehittäminen ovat nykyään merkittävässä asemassa organisaatioiden johtamisessa.[43]

Tietoturvallisuus tulee organisoida ja toteuttaa siten, että se tukee parhaalla tavalla organisaation perustehtävää ja strategian mukaisten tavoitteiden saavuttamista. Tietoturvallisuus on osaltaan sekä lain toteuttamista että hyvää hallintotapaa. Tietoturvallisuuden tulee olla luonteva osa organisaation toimintaa ja kokonaisvaltaista riskien hallintaa.[44]

Tietoturvallisuus on tärkeä liikesuhteissa. Liikesuhteissa tulee täyttää asiakkaiden, sidosryhmien ja viranomaisten antamat määräykset. Tietoturvallisuus ei kuitenkaan ole pelkästään organisaation toimintaan liittyvä asia vaan sen tulisi sisältyä usein myös organisaation tuotteen tai palvelun ominaisuuksiin. Tietoturvallisuudesta huolehtiminen kuuluu osaksi yritysten johtamista, sillä tietoturvavahingoista aiheutuu liiketoimintariskejä. Organisaatioiden tulisi myös säännöllisesti arvioida tietoturvallisuuden tilaa, tunnistaa ainakin suurimmat puutteet ja korjata tilanteet.[45]

Usein, tai ainakin parhaassa tapauksessa, yrityksen johto asettaa tietoturvallisuudelle tavoitteita ja vaatimuksia.[46] Organisaation johto onkin keskeisessä asemassa tietoturvallisuuden kehittämisessä, suunnittelussa, organisoinnissa ja ylläpitämisessä. Erityisesti johdon ja vastuuhenkilöiden sitoutumista vaaditaan tietoturvan toteuttamiseen. Vaatimuksia tietoturvasta voivat esittää omistajat, asiakkaat, sopimuskumppanit, käyttäjät ja lainsäätäjä.[47]

---

[41] Euroopan parlamentin ja neuvoston direktiivi 2003/98/EY, annettu 17 päivänä marraskuuta 2003, julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (EUVL nro L 345, 31.12.2003).
[42] Andreasson & Koivisto 2013, s. 32.
[43] Porvari 2012, s. 59.
[44] Andreasson & Koivisto 2013, s. 32.
[45] Porvari 2012, s. 1–2.
[46] Porvari 2012, s. 3.
[47] Porvari 2012, s. 3.

Asianmukaisella tietojen salassapidolla suojataan organisaation toimintaympäristöä, asiakkaiden liike– ja ammattisalaisuuksia sekä lisäksi turvataan kansalaisten yksityisyyden suoja. Tarkoituksena ei ole suojata pelkästään organisaation omaan toimintaan liittyviä tietoja.[48]

Tietoturvatoiminta tulee myös organisoida siten, että organisaation koko henkilöstö saadaan toimintaan mukaan. Säännöllinen tietoturvakoulutus ylläpitää tehokkaasti henkilöstön tietoturvaosaamista ja –tietoisuutta. Isoissa organisaatioissa hyvä vaihtoehto perinteisille koulutuksille on myös verkkopohjaiset tietoturvakurssit. Kurssien suorittamista voidaan seurata esimerkiksi esimiesten ja alaisten välisissä kehityskeskusteluissa.[49]

3.5 Teknologia

Nykyään tietoturvaa ei nähdä enää pelkästään teknologisena tai vain fyysisen tietoturvan asiana. Tietoturvaa voidaan toki kehittää myös teknisin turvatoimin. Tietoturvalla kuitenkin tarkoitetaan kaikkia hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.[50] Tekniset keinot ovat vain osa keinovalikoimien joukkoa.

4. Kansainvälinen yhteistyö

Nykyisessä globaalissa maailmassa erityisesti kansainvälinen yhteistyö tietoturvallisuuteen liittyvissä asioissa on nähty tärkeänä. Toimijoita kansainvälisessä tietoturvallisuudessa ovat muun muassa OECD, YK, NATO, WEU, EU, G8, CERT –organisaatiot, kansainväliset poliisiviranomaiset (EUROPOL, INTERPOL), tietotekniikan, tietoliikenteen ja tietoturvan standardointiorganisaatiot (IETF, W3C, ISO, BSI, EESSI, ETSI, CEN/ISSS, ITU–T). Lisäksi kansainväliset ICT– ja tietoturvayritykset ovat mukana kansainvälisessä toiminnassa.[51]

Seuraavaksi tarkastellaan erityisesti OECD:n, YK:n, G8:n ja WEU:n tietoturvatyötä. Lisäksi myöhemmin esitellään lyhyesti CERT/CC:n toimintaa sekä kerrotaan tietoturvallisuuteen liittyvästä standardoinnista.

[48] Andreasson & Koivisto 2013, s. 32–33.
[49] Andreasson & Koivisto 2013, s. 33.
[50] HE 221/2013 vp, s. 90–91.
[51] Valtionhallinnon kansainvälisen tietoturvayhteistyön hallintamalli, 2009.

4.1 OECD

OECD (Organization for Economic Cooperation and Development, taloudellisen yhteistyön ja kehityksen järjestö) on kansainvälinen yhteistyöjärjestö. Järjestö perustettiin 1961 ja sen päämaja sijaitsee Pariisissa. Tällä hetkellä OECD:ssa on 34 jäsenmaata. Päämääränään järjestöllä on kestävän taloudellisen kasvun ja työllisyyden edistäminen ja hyvinvoinnin lisääminen jäsenmaissa sekä maailmantalouden laajeneminen ja kaupan kasvu monenkeskiseltä pohjalta.[52]

OECD on merkittävä toimija tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteiden kehittäjänä. OECD laati vuonna 1992 tietoturvallisuusperiaatteet (Guidelines for the Security of Information Systems). Vuoden 1992 tietoturvallisuusperiaatteet syrjäytettiin vuonna 2002 uudemmilla tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteilla (Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security), joita käsitellään myöhemmässä kappaleessa. [53]

Tietoturvallisuusperiaatteiden lisäksi OECD on laatinut useita periaatesuosituksia maailman tietoyhteiskunnalle tärkeistä asioista. Nämä suositukset koskevat muun muassa tietosuojaa (1980 OECD:n suositus yksityisyyden suojaa ja henkilötietojen kansainvälisiä virtoja koskeviksi periaatteiksi, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) ja salakirjoitustekniikkaa (1997 OECD:n suositus salauspolitiikan periaatteiksi, Guidelines for Cryptography Policy). Myöhemmin esitellään lyhyesti myös OECD:n tietosuojaperiaatteet erityisesti tietoturvanäkökulmasta. Lisäksi OECD:n sihteeristö raportoi jo vuonna 1989 Tietoverkkojen turvallisuudesta (Information Network Security). Tietoturvallisuusperiaatteet tulisi lukea muiden suositusten kanssa samassa yhteydessä.[54]

[52] Tietoa OECD:stä, Suomen pysyvä edustusto OECD:ssä ja Unescossa, 2015.
[53] OECD:n neuvoston suositus, Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet: Turvallisuuskulttuurin kehittäminen, OECD:n Neuvoston suositus 1037.
[54] OECD:n neuvoston suositus, Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet: Turvallisuuskulttuurin kehittäminen, OECD:n Neuvoston suositus 1037, s. 11.

4.1.1 OECD:n tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet

OECD:n tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteiden pääsanoma on, että tietoturvallisuusnäkökohdat tulisi huomioida jo tietojärjestelmien suunnitteluvaiheessa. Turvallisuusriskit tulee tunnistaa ennakolta ja niiden varalta tulee olla myös ehkäisykeinoja.[55] OECD:n jäsenmaille tietoturvallisuusohjeet edustavat yhteistä turvallisuuskäsitteistöä ja tietoturvallisuuden määrittelyä oikeudellisena ja teknisenä instituutiona.[56]

Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteita on yhdeksän ja ne ovat toisiaan täydentäviä. Periaatteet ovat seuraavat:

1. Turvallisuustietoisuus: Tahojen tulisi olla tietoisia tietoturvallisuuden tarpeesta ja siitä, mitä ne voivat tehdä turvallisuuden edistämiseksi.
2. Vastuullisuus: Kaikki tahot ovat vastuussa tietoturvallisuudesta.
3. Vastatoimet: Tahojen tulee toimia viipymättä ja yhteistyössä ehkäistäkseen ja havaitakseen turvallisuuden loukkaukset ja vastatakseen niihin.
4. Eettisyys: Tahojen tulee kunnioittaa toisten oikeutettuja etuja.
5. Demokratia: Tietoturvallisuuden tulee sopeutua demokraattisen yhteiskunnan olennaisiin arvoihin.
6. Riskien arviointi: Tahojen tulee suorittaa riskien arviointia.
7. Turvallisuuden suunnittelu ja toimeenpano: Tahojen tulee sisällyttää turvallisuus tietojärjestelmien ja verkkojen olennaiseksi osaksi.
8. Turvallisuuden hallinta: Turvallisuuden hallinnan tulee olla kokonaisvaltaista.
9. Uudelleenarviointi: Tahojen tulisi arvioida uudelleen tietoturvallisuuttaan ja tarpeen mukaan tarkistaa sitä koskevat politiikkansa, toimensa ja menettelynsä.[57]

4.1.2 OECD:n tietosuojaperiaatteet

OECD perusti vuonna 1978 tilapäisen asiantuntijaryhmän ”Group of experts on transborder data barriers and privacy protection”, jonka tarkoituksena oli kehittää yleisohjeita ja –sääntöjä tietosuoja–asioihin liittyen. Kyseiseen asiantuntijaryhmään kuuluivat muun muassa puheenjohtajana Justice Kirby ja asiantuntijana Peter Seipel.[58]

---

[55] OECD:n neuvoston suositus, Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet: Turvallisuuskulttuurin kehittäminen, OECD:n Neuvoston suositus 1037, s. 10.
[56] Saarenpää–Pöysti (toim.) 1997, s. xxxiii.
[57] OECD:n neuvoston suositus, Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet: Turvallisuuskulttuurin kehittäminen OECD:n Neuvoston suositus 1037, s. 11–14.
[58] OECD:n neuvoston suositus, Tietosuojasäännöt – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

OECD julkaisi 1980 asiantuntijaryhmänsä kehittämät tietosuojaperiaatteet, joihin viitataan vielä tänäkin päivänä kirjallisuudessa (OECD:n suositus yksityisyyden suojaa ja henkilötietojen kansainvälisiä virtoja koskeviksi periaatteiksi, recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data).[59] Nämä periaatteet sisälsivät jo alkuperäisessä muodossaan kohdan, jonka mukaan suositellaan, että henkilötiedot tulisi suojata kohtuullisin keinoin tietojen luvatonta käyttöä, tuhoamista, muuttamista, luovuttamista tai muuta käyttöä varten (turvatoimien periaate, Security safeguards principle).[60]

Tietoturva oli jo OECD:n asiantuntijaryhmässä kiistelty aihe. Tietoturva nähtiin paljolti teknisenä seikkana, joka liittyi tietosuojan toteuttamiseen. Tietoturvan nähtiin lähinnä liittyvän tiedon suojaamiseen muun muassa valtuudettomalta käyttämiseltä ja tulipalolta. Asiantuntijaryhmällä oli myös hankaluuksia rajata kuinka laajassa määrin tietoturva tulisi määritellä osaksi tietosuojaan liittyvää kokonaisuutta. Ryhmän tarkoituksena oli rajata alemman tason koneistoon liittyvät asiat pois tietosuojaperusperiaatteista ja –tavoitteista.[61] Tietoturva nähtiin tietosuojan yhtenä toteuttajana, osana alemman tason koneistoa, teknisenä asiana.

OECD:n tietosuojaperiaatteita päivitettiin syyskuun 9. päivänä 2013. Uusiin periaatteisiin sisällytettiin muun muassa sääntö, jonka mukaan tietoturvaloukkauksen sattuessa olisi tehtävä ilmoitus tietosuojaviranomaiselle (Data security breach notification). Lisäksi päivityksessä korostettiin muun muassa kansallisten yksityisyydensuojastrategioiden merkitystä. [62] Ehdotetussa tietosuoja–asetuksessa[63] on myös otettu huomioon rekisterinpitäjän tietoturvaloukkausilmoitusvelvollisuus. Rekisterinpitäjät velvoitetaan asetusehdotuksessa ilmoittamaan henkilötietojen tietoturvaloukkauksista toimivaltaiselle viranomaiselle.[64]

[59] Alapuranen 2005, s. 20.
[60] OECD:n neuvoston suositus, Tietosuojasäännöt – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.
[61] OECD:n neuvoston suositus, Tietosuojasäännöt – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.
[62] OECD:n tietosuojatyö – OECD work on privacy, 2015.
[63] Ehdotus Euroopan parlamentin ja neuvoston asetukseksi: yksilöiden suojelusta henkilötietojenkäsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja–asetus) COM(2012) 11 Final, annettu 25.1.2012.
[64] Ks. tarkemmin asetus–ehdotuksen (COM(2012) 11 Final) 31 artikla.

4.2 YK:n suuntaviivat

YK:n tietokoneistettujen henkilötiedostojen sääntelyä koskevissa Yhdistyneiden kansakuntien suuntaviivoissa kohdassa 7[65] esitetään, että jokaisen maan tulisi säätää lailla tieturvan perusperiaatteista. Kohdan mukaan organisaatioiden tulisi huolehtia siitä, että tietoja suojataan luonnollisilta vaaroilta. Luonnolliset vaarat liittyvät vahinkoihin ja tietojen tuhoutumiseen esimerkiksi tulipalossa. Lisäksi organisaatioiden tulisi varautua ihmisten aiheuttamiin vaaroihin, kuten luvattomaan tiedon käyttöön, petolliseen tiedon käyttöön (fraudulent misuse of data) ja tietokonevirusten levittämiseen.[66]

YK:n suuntaviivoilla on lähinnä historiallista merkitystä ja ne voidaan nähdä taustalla vaikuttavina tekijöinä nykyisessä tietoturvasääntelyssä. Suuntaviivat kuvaavat kuitenkin hyvin yhteenvetona perusperiaatteita, jotka liittyvät tietojen automaattiseen prosessointiin.[67] YK:n ohjeistukset ovat myös hyvin konkreettisia ja luonteeltaan teknisiä.

YK on lisäksi julkaissut tietokonerikollisuuden ehkäisemistä ja valvontaa koskevan käsikirjan vuonna 1994 (Manual on the prevention and control of computer–related crime). Käsikirjassa tietoturvallisuuden osa–alueina on mainittu muun muassa valtion turvallisuus, henkilökohtaisten tietojen suojaaminen, taloudellinen ja tieteellinen tietoturvallisuus ja tietokonelaitteiden turvallisuus.[68]

4.3 G8 (Group of Eight)

1970–luvun maailmantalouden vaikeuksien seurauksena järjestettiin ensimmäinen maailman johtavien teollisuusmaiden huippukokous Ranskassa vuonna 1975. Kokoukseen osallistuivat Iso–Britannian, Italian, Japanin, Ranskan, Länsi–Saksan (nykyään Saksa) ja Yhdysvaltojen päämiehet. Kanada hyväksyttiin ryhmään vuonna 1976. EU pääsi ryhmään tarkkailijaksi 1977 ja on sen jälkeen ollut ryhmässä mukana kyseisessä roolissa. Venäjä on osallistunut huippukokouksiin vuodesta 1994 lähtien. 1998 jälkeen Venäjä on ollut täysipainoisesti mukana ryhmän toiminnasta. G8:n päätavoitteena on häiriöttömän maailmantalouden kehityksen turvaaminen. Huippukokouksissa käsitellään ajankohtaisia

[65] Kohta 7 on englanniksi: ” Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.”.
[66] YK:n yleiskokous, suuntaviivat tietokoneistettujen henkilötietojen sääntelyyn. UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files. 14 Joulukuuta 1990.
[67] YK:n suuntaviivat tietokoneistettujen henkilötietojen sääntelyyn, ENISA:n www–sivut, UN Guidelines.
[68] International review of criminal policy – United Nations Manual on the prevention and control of computer–related crime & Saarenpää–Pöysti (toim.) 1997, s. xivii.

maailmantalouden kysymyksiä, jotka liittyvät muun muassa kauppapolitiikkaan, työllisyyteen, terrorismiin ja rikollisuuteen.[69]

Vuonna 2003 G8–ryhmä julkaisi elintärkeiden infrastruktuurien suojaamisen periaatteet, joiden mukaan informaatioinfrastruktuurit ovat merkittävä osa elintärkeistä infrastruktuureista. G8:n elintärkeiden infrastruktuurien 11 periaate sisältää säännön, jonka mukaan valtioiden tulee edistää kansallista ja kansainvälistä tutkimusta ja kehitystä sekä rohkaista turvallisuuteen liittyvän kansainvälisesti sertifioidun teknologian käyttöä (XI Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards).[70]

Toukokuussa 2011 G8–maat julkaisivat myös uudistetun vapautta ja demokratiaa koskevan sitoumuksen. G8–ryhmä totesi samalla, että internetillä on ainutlaatuinen merkitys demokratian ja talouskasvun edistämisessä. Vapautta ja demokratiaa koskevaan sitoumukseen liittyi yhtenä laajana osiona kohta ”Internet”, jossa korostetaan yhteentoimivuutta, tietosuojaa, turvallisuutta sekä teollis– ja tekijänoikeuksia.[71]

4.3 WEU, Länsi–Euroopan unioni

Länsi–Euroopan yhteisen ulko– ja turvallisuuspolitiikan ”väline” oli aikaisemmin Länsi–Euroopan unioni (WEU, West–European Union). Länsi–Euroopan unionin tehtävänä oli valmistella ja toteuttaa puolustukseen liittyviä EU:n toimenpiteitä. Perusluonteeltaan Länsi–Euroopan unioni oli siihen kuuluvien jäsenvaltioiden solmima sotilasliitto. Suomi ei koskaan liittynyt Länsi–Euroopan unioniin ja pysyi siinä vain tarkkailijajäsenenä vuodesta 1995 heinäkuun 2010 alkuun asti, jolloin WEU:n toiminta päättyi.[72]

Sotilaspolitiikan alalla pyrkimys integroida Länsi–Euroopan unioni Euroopan unionin yhteyteen ei koskaan onnistunut. NATO:n suunniteltu laajeneminen Itä–Eurooppaan saattoi vaikuttaa Eurooppa–neuvoston varovaisuuteen Länsi–Euroopan unionin aseman vahvistamisen osalta.[73] WEU:lla oli toiminnassaan oma tietoturvallisuussäännöstä. Myös Suomi allekirjoitti 22.4.1997 turvallisuussopimuksen WEU:n kanssa (ei enää voimassa oleva SopS 41 ja 42/1998).[74]

---

[69] Taloudellisia ryhmittymiä, G7/G8, Ulkoasiainministeriön www–sivut, taloudellisia ryhmittymiä.
[70] G8 Principles for Protecting Critical Information Infrastructures, toukokuu 2003.
[71] G8 Declaration, Renewed Commitment for Freedom and Democracy, G8 Summit of Deauville, toukokuu 26.–27.2011 & G8 Principles for Protecting Critical Information Infrastructures, toukokuu 2003.
[72] Still 1997, s. 165.
[73] Raitio 2010, s. 54.
[74] Still 1997, s. 166.

4.4 Voimassaolevia tietoturvallisuussopimuksia

Tietoturvallisuustarpeiden painottumista myös taloudelliseen toimintaan ilmentää lisäksi Suomen ja Euroopan avaruusjärjestön (ESA, European Space Agency) välinen yhteistyösopimus vuodelta 2004 (SopS 94 ja 95/2004). Sopimuksen eräs keskeinen tavoite on turvata Suomen elinkeinoelämän mahdollisuudet osallistua tasavertaisesti muiden jäsenmaiden kanssa ESA:n turvallisuusluokiteltuihin tarjouskilpailuihin.

Lisäksi Suomi on solminut tietoturvasopimuksia useiden eri valtioiden kanssa. Nämä sopimukset luovat puitteet Suomelle ja suomalaisyrityksille osallistua hankkeisiin, jotka edellyttävät turvallisuusluokitellun tiedon vaihtamista.[75]

4.5 Muita kansainvälisiä tietoturvaorganisaatioita

CERT Coordination Center (CERT/CC, Computer Emergency Response Team/Coordination Center) on perustettu vuonna 1988 Carnegie Mellon yliopiston yhteyteen. CERT/CC perustettiin Morris –madon ”innoittamana”. Morris –mato oli ensimmäisiä internetissä levinneitä tietokoneviruksia.[76] CERT/CC:llä on nykyään yli 150 työntekijää, jotka pyrkivät kehittämään ja ylläpitämään tietoturvallisuutta. Lisäksi CERT/CC:ssä ollaan tutkittu muun muassa kuinka estetään, tunnistetaan ja vastataan organisaation sisäisiin uhkiin. Organisaation sisäisen uhkan aiheuttaja saattaa olla kuka tahansa niin sanottu sisäpiiriläinen, kuten entinen tai nykyinen työntekijä tai sopimuskumppani. CERT/CC:n tutkimukset ovat osoittaneet, että neljäsosa tietoverkkorikoksista tehdään sisäpiiriläisen toimesta. CERT/CC julkaisee tietoturvaohjeita, jotka ovat saatavilla CERT/CC:n verkkosivuilla.[77]

SANS Institute (SysAdmin, Audit, Networking and Security) on vuonna 1989 perustettu tutkimus– ja koulutusorganisaatio, joka järjestää tietoturvakoulutusta sekä tarjoaa GIAC–turvasertifikaattiohjelmaa (Global Information Assurance Certification). SANS:in www–sivuilla on lisäksi yli 2000 tietoturvaan liittyvää julkaisua, joita pääsee lukemaan maksutta SANS:in lukuhuoneessa (Reading room).[78]

[75] Lisätietoa voimassaolevista tietoturvallisuussopimuksista löytyy ulkoasiainministeriön www–sivuilta: Voimassa olevat tietoturvasopimukset, 7.9.2015.
[76] Boettger 2000, s. 2–3 & CERT/CC:n www–sivut: www.cert.org (viitattu 16.11.2015).
[77] CERT/CC:n www–sivut: www.cert.org (viitattu 16.11.2015).
[78] SANS:n (SysAdmin, Audit, Networking and Security) www–sivut: www.sans.org, about & reading room, 2015.

Yhdysvaltojen hallituksen alainen organisaatiot NSA/CSS (National Security Agency/Central Security Service, kansallinen turvallisuusvirasto) on vuonna 1972 perustettu organisaatio, joka kehittää ja tutkii salausmenetelmiä ja suorittaa tietoteknistä tiedustelua.[79]

4.6 Standardointi

Maailma on täynnä erilaisia standardeja. Sanalla standardi voidaan tarkoittaa useita eri asioita. Jotkut standardit voivat olla pakollisia viranomaismääräyksiä, kuten esimerkiksi liikennemerkit. Niin sanotusta de facto –standardista on puolestaan kyse, kun standardia ei ole laatinut standardoimisjärjestö vaan siitä on muodostunut hiljalleen yleinen käytäntö. Standardit, joita tehdään standardoimisjärjestöjen toimesta ovat yhteisiä sääntöjä, joiden tarkoituksena on muun muassa lisätä tuotteiden yhteensopivuutta ja turvallisuutta, suojella ympäristöä sekä helpottaa kansallista ja kansainvälistä kauppaa. Standardit laaditaan usein yhteistyönä erilaisissa työryhmissä ja komiteoissa. Standardityön tulokset julkaistaan asiakirjoina. Standardit ovat yleensä luonteeltaan suosituksia, joiden käyttö on vapaaehtoista ja ilmaista.[80]

Tietoturvaan liittyy useita kansainvälisiä ja kansallisia standardeja. Niitä kutsutaan yleisesti tietoturvastandardeiksi. Tietoturvastandardit eivät useimmiten aseta vaatimuksia itse tietoturvalle vaan sen suunnittelun menettelytavoille. Standardit antavat erityisesti tietoturvasuunnittelun dokumentointiin apuvälineitä. On kuitenkin hyvä muistaa, ettei standardien noudattaminen yksin takaa riittävää tietoturvallisuutta. Standardi määrittelee ainoastaan, mitä suunnittelutyöhön sisältyy ja missä muodossa suunnittelutyön tulokset tulisi esittää.[81]

IT–standardoimistyö on Suomessa jaettu siten, että Suomen Standardisoimisliitto (SFS) huolehtii IT–standardisoinnista, SESKO sähkö– ja elektroniikka–alan standardisoinnista ja Viestintävirasto tietoliikenteen standardisoinnista. Tietotekniikan kansainvälistä standardoimistyötä tehdään puolestaan ISO:n (International Organization for Standardization, kansainvälinen standardointijärjestö) teknisissä komiteoissa. [82] Suomessa julkisyhteisöjen tietoturvallisuuden kehittäminen ja valvonta puolestaan kuuluvat valtiovarainministeriölle (VM). Käytännön ohjeistuksesta vastaa viestintävirasto.[83]

[79] NSA:n www–sivut: www.nsa.gov, About NSA, marraskuulta 2011.
[80] SFS–käsikirja, standardit ja standardointi 2013, s. 7.
[81] Hakala et al. 2006, s. 46.
[82] Yleistä IT–standardisointityöstä, SFS:n www–sivut: www.sfs.fi (viitattu 16.11.2015).
[83] Hakala et al. 2006, s. 46.

On olemassa lukuisia organisaatioita, jotka tekevät standardointia omista lähtökohdistaan.[84] Tällaisia organisaatioita ovat muun muassa IETF (The Internet Engineering Task Force)[85], W3C (World Wide Web Consortium)[86], BSI (British Standards Institution)[87], EESSI (Electronic Exchange of Social Security Information, Sosiaaliturvatietojen sähköinen vaihtojärjestelmä)[88], ETSI (European Telecommunications Standards Institute)[89], CEN/ISSS (European Committee for Standardisation/ Information Society Standardisation System)[90] ja ITU–T (Telecommunication Standardization Sector of International Telecommunication Union)[91].

Muun muassa ISO (International organization for Standardization, kansainvälinen standardointijärjestö) on laatinut tietoturvaan liittyviä kansainvälisiä standardeja. Erityisesti ISO 27000–sarjan standardit on erityisesti varattu tietoturvan alueelle. Sarja tarjoaa suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin.[92] Tietoturvastandardeja kehitetään koko ajan, jotta standardi pystyy vastaamaan muuttuviin olosuhteisiin tekniikan kehittyessä.[93] ISO standardeihin liittyy vapaaehtoisuus. Organisaatiot saavat halutessaan ottaa standardin mukaiset velvoitteet käyttöönsä. ISO–standardit eivät kuitenkaan ole julkisesti saatavilla ja ovat maksullisia.[94]

5. Toimijat Euroopassa ja unionin sääntely

Euroopan unionin sääntelyn taustalla on usein yhteismarkkinoiden toimivuus ja esteettömien yhteisten sisämarkkinoiden toteuttaminen. Luottamus markkinoihin vaatii myös tietoturvallisuuden asianmukaista sääntelyä. Hyvällä sääntelyllä voidaan saavuttaa kansalaisten luottamus markkinoihin ja niiden toimivuuteen.[95] Luottamuksella on merkittävä rooli sosiaalisessa ja taloudellisessa kanssakäymisessä. Se on yksi tärkeimmistä tekijöistä, jolla

[84] Yleistä IT–standardisointityöstä, SFS:n www–sivut: www.sfs.fi (viitattu 16.11.2015).
[85] IETF:n www–sivut: http://www.ietf.org (viitattu 10.11.2015).
[86] W3C:n www–sivut: http://www.w3.org (viitattu 10.11.2015).
[87] BSI:n www–sivut: http://www.bsigroup.com (viitattu 10.11.2015).
[88] EESSI:n www–sivut: http://ec.europa.eu/social/main.jsp?catId=869&langId=fi (viitattu 10.11.2015).
[89] ETSI:n www–sivut: http://www.etsi.org (viitattu 10.11.2015).
[90] CEN/ISSS:stä löytyy lisätietoa EU:n IDABC:n www–sivuilta (http://ec.europa.eu/idabc/en/document/6990.html, viitattu 10.11.2015).
[91] ITU–T lyhyesti, ITU:n www–sivut: www.itu.int, About ITU–T (10.11.2015).
[92] ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä. SFS:n www–sivut: www.sfs.fi, ISO/IEC 27000 Tietoturvallisuuden hallinta (viitattu 10.11.2015).
[93] ISO/IEC 27001 (Saatavilla: http://www.sfs.fi/ajankohtaista/tuoteuutiset/uusi_versio_tietoturvastandardista_iso_iec_27001.1777.news, 10.11.2015)
[94] ISO:n www–sivuilta löytyy lisätietoa standardoinneista: http://www.iso.org/ (viitattu 10.11.2015).
[95] Saarenpää–Pöysti (toim.) 1997, s. xxxix.

voidaan vähentää epävarmuutta erilaisissa suhteissa. Sähköisen maailman potentiaalia ei ole mahdollisuutta toteuttaa ilman luottamusta.[96]

5.1 Strategioita, aloitteita ja tiedonantoja

5.1.1 eEurope –aloite

Euroopan unionin komissio käynnisti vuonna 1999 eEurope–aloitteen, jonka tarkoituksena oli varmistaa Euroopan unionin täysimittainen tietoyhteiskunnan muutosten hyödyntäminen. Myös tietoturva–asiat huomioitiin eEuropen tavoitteissa. Sähköisiä yhteyksiä haluttiin parantaa tuolloin erityisesti älykorttien avulla. Älykortit nähtiin tietoturvan parantajina ja sähköisten verkkojen luottamuksellisuuden takaajina.[97] Erityisinä painopisteinä tietoturvallisuuden osalta olivat luotettavat verkko– ja tietojärjestelmärakenteet, infrastruktuurin haavoittuvuus ja keskinäiset riippuvuussuhteet. Tarkoituksena oli myös tukea standardointia. Lisäksi tutkimustoiminnassa haluttiin erityisesti otettavan huomioon myös ”inhimillinen tekijä” tietoturvassa, kuten esimerkiksi tietoturvallisuusajattelun perusperiaatteet ja järjestelmien käyttäjäystävällisyys. Tällöin ehdotettiin muun muassa tietoverkkoturvallisuuden työryhmän perustamista[98], tietoturvakulttuurin luomista ja viranomaisten välisen tiedonsiirron turvaamista.[99] Tavoitteena oli, että vuoteen 2005 mennessä Euroopassa olisi oltava turvallinen tietoverkkoinfrastruktuuri.[100]

5.1.2 Muita Euroopan unionin tiedonantoja

Vuonna 2001 komissio antoi tiedonannon Verkko– ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi. Tuolloinkin komissio korosti verkko– ja tietoturvan kasvavaa merkitystä.[101] Tämän jälkeen annettiin Turvallisen tietoyhteiskunnan strategia, jonka tavoitteena oli myös kehittää verkko– ja tietoturvakulttuuria. [102] Näiden lisäksi komissio on

[96] OECD Digital Economy Outlook 2015, s. 209.
[97] Prodi käynnistää eEurope–aloitteen nopeuttaakseen Euroopan kehittymistä tietoyhteiskunnaksi European Commission – IP/99/953, Bryssel, 8. joulukuuta 1999 (viitattu 11.11.2015)..
[98] Lisäksi luotiin niin sanottuja CERT–ryhmiä (Computer Emergency Response Teams), joiden tehtävänä oli ehkäistä ja ratkaista tietoteknosia ongelmatilanteita yritysten, viranomaisten ja kansalaisten eduksi kaikissa jäsenvaltioissa (ks. Komission tiedonanto neuvostolle ja Euroopan parlamentille, eEurope2002 Vaikutukset ja painopisteet, Tiedonanto Eurooppa–neuvoston Tukholman kokoukselle 23.–24. maaliskuuta 2001 (KOM(2001) 140 lopullinen), s. 17).
[99] Komission tiedonanto neuvostolle, Euroopan parlamentille, Talous– ja sosiaalikomitealle sekä Alueiden komitealle, eEurope 2005: Tietoyhteiskunta kaikille (KOM(2002) 263 lopullinen), s. 16.
[100] Komission tiedonanto neuvostolle, Euroopan parlamentille, Talous– ja sosiaalikomitealle sekä Alueiden komitealle, eEurope 2005: Tietoyhteiskunta kaikille (KOM(2002) 263 lopullinen) , s. 3.
[101] KOM(2001) 298 lopullinen.
[102] KOM(2006) 251 lopullinen.

antanut maaliskuussa 2009 elintärkeiden infrastruktuurien suojaamista koskevan tiedonannon. Siinä käsitellään Euroopan suojaamista tietoverkkohäiriöiltä parantamalla turvallisuutta.[103]

5.1.3 Euroopan digitaalistrategia

Euroopan digitaalistrategia hyväksyttiin toukokuussa 2010.[104] Tällöin todettiin, että luottamus ja tietoturva ovat ehdottomia perusedellytyksiä tieto– ja viestintäteknologian laajalle käyttöönotolle. Digitaalistrategian päämääränä on myös Eurooppa 2020 –strategian tavoitteiden saavuttaminen. Tarkoituksena tässäkin strategiassa on, että yhteistyöllä varmistettaisiin tieto– ja viestintäteknologian infrastruktuurien suoja ja sietokyky. Yksi digitaalistrategian päämääristä on korkean tason verkko– ja tietoturvapolitiikan lujittaminen ja siihen tähtäävät toimenpiteet. Myöhemmissä tiedonannoissaan komissio on myös todennut, että puhtaasti kansalliset lähestymistavat turvallisuuden asettamiin haasteisiin eivät ole riittäviä. Siksi Euroopan unionin olisi jatkettava pyrkimyksiään luoda johdonmukainen ja yhteistyöhön perustuva lähestymistapa tietoturvaan EU:ssa.[105]

5.1.4 Euroopan kyberturvallisuusstrategia

Euroopan komissio on julkistanut unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan kanssa kyberturvallisuusstrategian vuoden 2013 alussa. Kyberturvallisuusstrategialla on viisi painopistealuetta, jotka ovat 1. kyberuhkien sietokyvyn edistäminen (kyberresilienssi), 2. verkkorikollisuuden (kyberrikollisuuden) vähentäminen, 3. verkkopuolustuspolitiikan ja yhteisen turvallisuus– ja puolustuspolitiikkaan liittyvien valmiuksien kehittäminen (Common Security and Defence Policy, CSDP / yhteinen turvallisuus– ja puolustuspolitiikka, YTPP), 4. kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittäminen sekä 5. johdonmukaisen kansainvälisen verkkotoimintapolitiikan luominen Euroopan unionille sekä EU:n keskeisten arvojen edistäminen.[106]

Samaan aikaan kyberturvallisuusstrategian kanssa komissio antoi asiaan liittyvän verkko– ja tietoturvaa koskevan direktiiviehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko– ja tietoturvan varmistamiseksi koko unionissa (NIS–direktiivi).[107] Direktiiviehdotuksen käsittely on vielä kesken.[108]

[103] KOM(2009) 149 lopullinen.
[104] KOM(2010) 245 lopullinen.
[105] COM(2013) 48 final, s. 5.
[106] JOIN(2013) 1 final.
[107] COM(2013) 48 final.
[108] Lisää direktiiviehdotuksesta voi lukea Euroopan parlamentin lainsäädännön seurantatyökalusta, josta on saatavilla ajantasaista tietoa direktiivin tilanteesta. (Saatavilla:

Ehdotetun direktiivin tavoitteena on varmistaa verkko– ja tietoturvan korkea taso unionin alueella. Tarkoituksena on velvoittaa jäsenvaltiot nostamaan varautumistasoaan ja parantamaan yhteistyötään. Elintärkeiden infrastruktuurien operaattorit ja keskeiset tietoyhteiskunnan palvelujen tarjoajat sekä julkishallinnot halutaan myös velvoittaa ryhtymään tarvittaviin toimiin turvariskien hallitsemiseksi ja raportoimaan vakavista turvapoikkeamista kansalliselle toimivaltaisille viranomaisille. Direktiivissä ehdotetaan myös toimenpiteitä, joiden mukaan jäsenvaltioiden olisi hyväksyttävä verkko– ja tietoturvastrategia sekä nimettävä verkko– ja tietoturvaviranomainen.[109]

5.2 Toimijat EU:ssa

5.2.1 Euroopan verkko– ja tietoturvavirasto (ENISA)

Suuri osa Euroopan unionin hallintovirastoista keskittyy informaation keräämiseen, analysointiin ja levittämiseen. Unionin informaatiovirastojen keskeisimpänä tehtävänä on tehdä ja hankkia teknisiä ja taloudellisia selvityksiä toimialaansa liittyvistä kysymyksistä. Nämä virastot jakavat lisäksi tätä tietoa ja toimivat jäsenvaltioiden välisten verkostojen tukena.[110]

Informaatiovirastojen ryhmään on luettavissa myös muun muassa Euroopan verkko– ja tietoturvavirasto (ENISA, European Union Agency for Network and Information Security,), joka on perustettu 2004 ja sijaitsee Heraklionissa Kreikassa. ENISA:lla on lisäksi sivutoimisto Ateenassa.[111] ENISA:n toimikautta on jatkettu edellisen kerran kesällä 2013 seitsemän vuoden kaudeksi ((EU) N:o 526/2013, 36 artikla). ENISA on asiantuntijaelin, joka seuraa tietoturvallisuuden tilaa ja pyrkii myös samalla vaikuttamaan siihen. Virasto on määräaikainen, koska on katsottu, että tietoturvallisuus on sellainen asia, joka on vaikeasti alistettavissa unionin sääntelyn alaiseksi.[112]

Mielenkiintoista on, että Euroopan verkko– ja tietoturvavirastolla ei ole varsinaista valvonnallista tai ohjaavaa toimivaltaa, eikä myöskään toimivaltaa tehdä yksityistä velvoittavia päätöksiä. ENISA:n toiminta keskittyy keräämään ja analysoimaan tietoa sekä helpottamaan jäsenvaltioiden välistä tietojenvaihtoa. Tällaiseen toimintaan voi sisältyä silti merkittävää

http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0027(COD) (16.11.2015).
[109] COM(2013) 48 final, s. 1.
[110] Mäenpää 2010, s. 187.
[111] Mäenpää 2010, s. 187.
[112] Saarenpää 2012b, s. 534.

informaatioon perustuvaa ohjausta ja yhtenäistämistä koskevia suosituksia, joilla voi ainakin epäsuorasti olla vaikutusta myös yksityisten oikeusasemaan.[113]

5.2.2 Euroopan verkkorikostorjuntakeskus

Tammikuussa 2013 perustettiin osaksi Euroopan poliisivirastoa (EUROPOL, European Police Office) Euroopan verkkorikostorjuntakeskus (EC3, European Cybercrime Centre), joka toimii linkkinä verkkorikollisuuden torjunnassa Euroopan unionissa.[114] Verkkorikostorjuntakeskuksen tehtävänä on kerätä tietoa verkkorikollisuudesta Euroopassa, keskittää verkkorikollisuutta koskeva asiantuntemus, tukea jäsenvaltioita verkkorikostutkimuksessa ja edustaa verkkorikostutkijoita tuomioistuimissa.[115]

5.2.3 CERT–EU

Euroopan unionin toimielimet ja muut elimet sekä virastot ovat perustaneet myös oman tietotekniikan kriisiryhmän, CERT–EU:n (Computer Emergency Response Team) osana Euroopan digitaalistrategiaa.[116] CERT–EU:n tehtävänä on ennaltaehkäistä ja havainnoida tietoturvaloukkauksia sekä tiedottaa tietoturvauhkista.[117]

5.3 Unionin sääntely

5.3.1 Euroopan ihmisoikeussopimus (SopS 18–19/1990) ja Euroopan unionin perusoikeuskirja (2000/C 364/01)

Euroopan talous– ja sosiaalikomitea (ETSK) on korostanut, että tietoturva on välttämättä nivottava henkilötietojen suojan vahvistamiseen ja vapauksien suojeluun, sillä ne ovat Euroopan ihmisoikeussopimuksessa taattuja oikeuksia.[118] Samaiset oikeudet taataan myös osittain Euroopan unionin perusoikeuskirjassa (2000/C 364/01), joka saatettiin voimaan Lissabonin sopimuksella.

Yleisenä pelkona on, etteivät käyttäjät turvallisuusongelmien takia halua ottaa käyttöön tietotekniikkaa. Käytettävyys, luotettavuus ja turvallisuus ovat ehdottomia edellytyksiä, jotta perusoikeudet voidaan verkossa taata.[119]

---

[113] Mäenpää 2010, s. 187.
[114] KOM(2012) 140.
[115] KOM(2012) 140, s. 4–6.
[116] Digitaalistrategia: Euroopan komissio tarkastelee jäsenvaltioiden suojautumista tietoverkko-hyökkäyksiltä European Commission – IP/11/395 01/04/2011.
[117] CERT–EU, tietoa meistä. CERT–EU:n www–sivut: http://cert.europa.eu (viitattu 12.11.2013).
[118] ETSK, Täysistunnossa 15.–16. Helmikuuta 2007 annetut lausunnot, Bryssel 23. helmikuuta 2007, s. 6.
[119] KOM(2006) 251, s. 5.

5.3.2 Direktiivit, asetukset ja muu sääntely

Euroopan unionissa yksityisyyttä ja tietosuojaa on säännelty usein direktiivein ja asetuksin. Muun muassa henkilötietodirektiivissä säännellään tietoturvasta 17 artiklassa (95/46 EY[120]). Henkilötietodirektiivin 17 artikla asettaa rekisterinpitäjälle velvollisuuden huolehtia tietojärjestelmien turvallisuudesta. Euroopan parlamentin ja neuvoston asetuksessa yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (45/2001 EY[121]) säädetään tietojen käsittelyn turvallisuudesta 22 artiklassa. Sähköisen viestinnän tietosuojadirektiivissä (2002/58 EY[122]) turvallisuudesta säädetään 4 artiklassa.

5.3.3 Tietoverkkorikosdirektiivi – tietoturvan rikosoikeudellinen suoja

Kansainvälisiin tietoverkkorikoksiin on kiinnitetty jo jonkin aikaa huomiota. Tietoturvallisuutta voidaan pyrkiä parantamaan osittain myös rikoksia koskevalla sääntelyllä. Tietotekniikka– ja tietoverkkorikoksia koskevilla kriminalisoinneilla suojataan tietoturvallisuuden eri osa–alueita eli tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä.[123]

Ainakin Euroopan parlamentin ja neuvoston direktiivistä 2013/40/EU (tietoverkkorikosdirektiivi) on merkitystä tietoturvallisuuden kannalta.[124] Erilaiset verkkohyökkäykset voivat aiheuttaa merkittäviä taloudellisia vahinkoja siten, että niillä keskeytetään tietojärjestelmien toiminta ja viestintä. Tietoturvallisuutta parantamalla ja tietoturvallisuustietoisuutta lisäämällä voidaan parantaa erilaisten tietojärjestelmien kykyä selvitä hyökkäyksistä. Suomessa tietoverkkorikosdirektiivi on implementoitu syksyllä 2015.[125]

Tietoverkkorikollisuudesta tehty Euroopan neuvoston yleissopimus on merkittävä asiakirja (Convention on Cybercrime, SopS 60/2007)[126], joka tunnetaan myös nimellä

---

[120] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, henkilötietodirektiivi (EYVL L 281, 23.11.1995).

[121] Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, (EYVL nro L 008 12.1.2001).

[122] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, sähköisen viestinnän tietosuojadirektiivi(EYVL L 201, 31.7.2002).

[123] Pihlajamäki 2004, s. 121.

[124] Kyseisellä direktiivillä korvattiin myös Neuvoston puitepäätös 2005/222/YOS, tehty 24 päivänä helmikuuta 2005, tietojärjestelmiin kohdistuvista hyökkäyksistä (EUVL nro L 069, 16.3.2005). Direktiivissä on myös säännöksiä samoista asioista kuin Budapestin sopimuksessa. Yleissopimus sisältää kuitenkin kattavammat ja laajemmat määräykset tietoverkkorikoksista kuin puitepäätös ja direktiivi. Se sisältää määräyksiä muun muassa oikeudellisesta yhteistyöstä. Eräs tietoverkkodirektiivin tavoitteista onkin saattaa kaikkien jäsenvaltioiden lainsäädäntö vastaamaan tiettyjä yleissopimuksen vaatimuksia.

[125] Ks. tarkemmin HE 232/2014 vp.

[126] Ks. myös HE 153/2006 vp.

Budapestin sopimus. Tietoverkkorikollisuudesta laadittuun yleissopimukseen on liitetty myös lisäpöytäkirja, joka koskee tietojärjestelmien välityksellä tehtyjen luonteeltaan rasististen ja muukalaisvihamielisten tekojen kriminalisointia (Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, SopS 83/2011).

6. Tietoturvasääntely Suomessa

6.1 Perustuslaki

Tietoturvallisuus sisältyy taustatekijänä useisiin perusoikeuksiin. Verkkoyhteiskunnassa tietoturvallisuusriippuvaisia perusoikeuksia ovat oikeus henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen, yksityiselämän, kunnian ja henkilötietojen suoja sekä luottamuksellisen viestin ja salaisuuden loukkaamattomuus, viestinnän vapaus ja viranomaisten asiakirjojen ja tallenteiden julkisuus, omaisuuden suoja ja asian joutuisan käsittelyn ja hyvän hallinnon takeet.[127] Tietoturvallisuusriippuvaisista perusoikeuksista mainitaan Suomen perustuslaissa (PeL, 731/1999) ainakin oikeus elämään sekä henkilökohtaiseen vapauteen (PeL 7 §) ja koskemattomuuteen, yksityiselämän suoja (PeL 10 §), sananvapaus ja julkisuus (PeL 12 §), omaisuuden suoja (15 §) ja oikeusturva (PeL 21 § sisältää asian joutuisan käsittelyn ja hyvän hallinnon takeet).

Aikaisemman hallitusmuodon (HM, kumottu 94/1919) 6 §:ssä säädettiin, että jokainen Suomen kansalainen ”olkoon lain mukaan turvattu hengen, kunnian, henkilökohtaisen vapauden ja omaisuuden puolesta”. Perusoikeusuudistuksen yhteydessä omaisuuden suoja erotettiin omaksi säännökseksi (PeL 15 §). Kunnian suoja puolestaan sisällytettiin osaksi nykyistä PeL 10 §:ää, jossa säädetään yksityisyyden suojasta. Säännöksen muuttamisen taustalla ovat ihmisoikeussopimukset (KP–sopimus ja Euroopan ihmisoikeussopimus[128]). Perusoikeusuudistuksessa muokattu HM 6 § siirrettiin perustuslakiuudistuksessa PeL 7 §:ään, jonka mukaan ”jokaisella on oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen”.[129]

Tietoturvan voidaan nähdä liittyvän erityisen läheisesti perustuslain 7 §:ssä mainittuun yksilön oikeuteen turvallisuuteen. Oikeutta turvallisuuteen on kansallisessa ja eurooppalaisessa katsannossa tulkinnaltaan pidetty henkilökohtaisen vapauden ja koskemattomuuden suojaan kytkeytyvänä oikeutena. Oikeus henkilökohtaiseen turvallisuuteen

[127] Saarenpää–Pöysti (toim.) 1997, s. ixii.
[128] Oikeus henkilökohtaiseen turvallisuuteen on tuodaan julki Euroopan ihmisoikeussopimuksen 5 artiklassa ja KP–sopimuksen 9 artiklassa.
[129] Pellonpää 2011, s. 283–286.

suojaa yksilöä mielivaltaiselta puuttumiselta henkilökohtaiseen vapauteen ja koskemattomuuteen. [130]

PeL 7.1 §:ään on sisällytetty oikeus henkilökohtaiseen turvallisuuteen.[131] Julkisen vallan positiivisena toimintavelvoitteena nähdään yhteiskunnan jäsenten suojaaminen rikoksilta ja muilta heihin kohdistuvilta oikeudenvastaisilta teoilta.[132] Henkilökohtainen turvallisuus liittyy perinteisesti erityisesti fyysiseen turvallisuuteen. Tietoturvallisuus puolestaan harvoin liittyy suoraan fyysiseen turvallisuuteemme. Turvallisuusperusoikeuden liittäminen fyysiseen turvallisuuteen ei ole nykyisessä verkkoyhteiskunnassa riittävä. Elämme nykyään erilaisessa yhteiskunnassa, jossa tietoturvallisuudesta on tullut tärkeä osa yksilön toimintaa. Tietoturvallisuus olisi nähtävä yhtenä PeL 7.1 §:n suojaamista oikeuksista.[133] Sama näkemys tästä asiasta on ollut myös perustuslakivaliokunnalla. Perustuslakivaliokunnan näkemys on, että tietoturvallisuuden vaarantumista voidaan nykyaikana pitää riskinä yksilön ja yhteiskunnan laajasti ymmärretyn turvallisuuden kannalta.[134] Toisaalta tietoturva voidaan nähdä kollektiivisena hyvänä, esimerkiksi tietoturva viestintäjärjestelmien takaajana, mutta toisaalta tietoturva voidaan nähdä yksilön perusoikeutena, joka tarkoittaa, että jokaisella yksilöllä on oikeus tietoturvaan.[135]

Oikeutta turvallisuuteen ei nähdä kuitenkaan itsenäisenä perusoikeutena. Hallituksen esityksessä perusoikeusuudistuksesta turvallisuuden nimenomainen mainitseminen korostaa julkisen vallan positiivisia toimintavelvoitteita yhteiskunnan jäsenten suojaamiseksi rikoksilta ja muilta heihin kohdistuvilta oikeudenvastaisilta teoilta, olivatpa niiden tekijät julkisen vallan käyttäjiä tai yksityisiä tahoja. Säännös edellyttää toimia myös rikosten uhrien oikeuksien turvaamiseksi ja aseman parantamiseksi.[136]

6.2 Tietoturvallisuus metaperusoikeutena ja oikeusperiaatteena

Sääntelyn teorian ja erityisesti lainsäädäntöopin tutkimuskohteisiin kuuluvat säädettävän lain sisältöön ja vaikutuksiin kohdistuva de lege ferenda –tutkimus sekä normin sisältöä ja normin asettamisen menettelyä ohjaavat metanormit. Metanormit tarkoittavat toisen asteen normeja ja valtiosääntöisiä normeja, jotka toimivat menettelyohjeina oikeudellisten ongelmien ratkaisemisessa. Metanormi voi olla esimerkiksi oikeusnormi, joka osoittaa kahden keskenään

[130] HE 309/1993 vp, s. 47/II.
[131] Pellonpää 2011, s. 283–286.
[132] HE 309/1993 vp, s. 47.
[133] Råman 2006, s. 819.
[134] PeVL 9/2004 vp, s. 4.
[135] Råman 2006, s. 820.
[136] HE 309/1993 vp, s. 47.

ristiriidassa olevan normin keskinäisen konfliktinratkaisuperusteen. Myös oikeudellisia tulkintaperiaatteita osoittavat normit voivat olla metanormeja. Tällaisten normien avulla juristi tunnistaa oikeudellisen ongelman. Metanormi on normi, jonka lainsäätäjän on lisäksi otettava huomioon lainsäädäntötyössä.[137]

Oikeus tietoturvaan voidaan nähdä yhtenä informaatio–oikeuden yleisistä opeista (metaperusoikeutena). Muita informaatio–oikeuden yleisiä oppeja ovat oikeus tietoon, oikeus viestintään, informaation vapaus, informaation kulun vapaus ja tiedollinen itsemääräämisoikeus. Oikeus tietoturvaan on ihmisoikeusperusteinen oikeus. Tästä oikeudesta ei kuitenkaan sellaisenaan ole nimenomaista perusoikeustasoista säännöstä.[138] Oikeus tietoturvaan on verkkoyhteiskunnan informaatioinfrastruktuurin toimivuuden perusedellytys sekä perusoikeuksiemme ja –vapauksiemme käytön välttämätön edellytys. Jokaisella on oikeus tietoturvaan kuten muuhunkin turvallisuuteen. Demokraattinen yhteiskunta ja oikeusvaltio voidaan rakentaa vain, jos asianmukaisen tietoturvan avulla voidaan taata informaatioinfrastruktuurin toimivuus.[139]

Tietoturvallisuus on yksilön näkökulmasta eräänlainen metaperusoikeus. Yksilöllä on oikeus tietoturvalliseen informaatioinfrastruktuuriin. Kollektiiviset hyvät, kuten yleinen järjestys ja turvallisuus tai tarkemmin tietoturvallisuus informaatioinfrastruktuurin toimivuuden edellytyksenä on pidettävä perusoikeusjärjestelmän ulkopuolella. Tietoturvallisuus on metaperusoikeus (ja oikeusperiaate).[140]

Tietoturvallisuuden ymmärtäminen oikeusperiaatteena auttaa hahmottamaan oikeusjärjestyksen, normien ja oikeuskäytännön suhdetta tietojenkäsittelyn ja informaation luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseen. Tietoturvallisuus oikeusperiaatteena on nimenomaan systeemiperiaate. Systeemiperiaatteet ovat perustavaa laatua olevia periaatteita, jotka toimivat monimutkaisen oikeusjärjestyksen koherenssin (johdonmukaisuuden) luojina.[141]

6.3 Kansallisen sääntelyn kehitys

Nykyisestä oikeudellisesta tietoturvallisuudesta puhuttaessa yhtenä alkuvaiheena voidaan nähdä henkilörekisterilain (HRL, kumottu 1987/471) säätäminen 1987. Suomi sai

[137] Pöysti 1997, s. 7.
[138] Saarenpää 2012b, s. 515.
[139] Råman 2006, s. 818–819.
[140] Råman 2006, s. 821.
[141] Saarenpää–Pöysti (toim.) 1997, s. ixxi–ixxii.

tällöin uuden oikeudellisen instituution, henkilötietojen suojan. Alettiin puhua tietosuojasta.[142] Tietoturvallisuus ei ole kuitenkaan pitkään aikaan ollut ainoastaan henkilötietojen suojan (tietosuoja) tai salassapidon turvaamista. Tietoturvallisuuden luottamuksella on ollut merkitystä jo kauan esimerkiksi tietoverkoissa tekijänoikeuksien ja muiden henkisen omaisuuden oikeuksien (immateriaalioikeuksien) oikeudettoman käytön estäjänä.[143]

Tietoturvasääntelyn kehityksen alussa muutosvastarinta oli näkyvää. Tämän osoittivat erityisesti media ja tietotekniikan ammattilaiset. Oli totuttu hyödyntämään vapaasti informaatiota raaka–aineena käyttäen ja yhtäkkiä siitä tulikin säänneltyä, rajoitettua ja ohjelmointia vaikeuttavaa. Informaatiovapauden aikakausi oli tullut tiensä päähän. Tietosuojan alkuvaiheet olivat hankalia osaksi myös osaamattomuuden ja huomaamattomuuden takia. Samalla tietoturvallisuus jäi vähäiselle huomiolle ja asiana sitä ei tuotu tarpeeksi näkyvästi esille. Tietoturvallisuuspalveluita alettiin vasta tuoda markkinoille.[144]

Kumottu henkilörekisterilaki sisälsi tietoturvaan liittyvän säännöksen, jonka mukaan rekisterinpitäjän oli huolehdittava siitä, että henkilörekisteri ja sen tiedot olivat asianmukaisesti suojattuja luvatonta käsittelyä, käyttöä, tuhoamista ja muuttamista sekä anastusta vastaan. Sama velvollisuus oli sillä, joka itsenäisenä elinkeinon– tai toiminnanharjoittajana toimi rekisterinpitäjän lukuun tai jolle rekisterinpitäjä oli luovuttanut henkilötietoja massaluovutuksena tai arkaluonteisena otantana. Henkilörekisterilakia ei tunnettu käytännössä tarpeeksi hyvin ja sen soveltamisessa oli ongelmia. Henkilörekisterilain tietoturvasäännöksen sivuuttamisesta annettiin Suomelle myös langettava ratkaisu I. vs. Finland 17.07.2008. Tapaukseen liittyi se, että tuomioistuimet eivät osanneet soveltaa henkilörekisterilakia käytännössä, eivätkä siis tunteneet lakia.[145]

Myöhemmin henkilötietodirektiivin (95/46 EY) implementointi sai tietoturvallisuuden uudella tavalla näkyville. Direktiiviin liittyy tietoturvallisuusartikla (17 artikla, käsittelyn turvallisuus). Se siirrettiinkin Suomen lakiin sellaisenaan yhdeksi pykäläksi henkilötietolakiin (523/1999, 7:32). Henkilötietolakia valmisteltaessa heräsi laatimiseen osallistuneiden henkilöiden kesken keskustelu yleisemmästä tietoturvallisuuden säätämisen tarpeesta. Lapin yliopiston oikeusinformatiikan instituutti laatikin valtiovarainministeriön toimeksiannosta

[142] Saarenpää 2012b, s. 531–532.
[143] Pöysti 1997b, s. 65.
[144] Saarenpää 2012b, s. 531–532.
[145] Saarenpää 2012b, s. 532.

laajan raportin aiheesta nimellä Tietoturvallisuus ja laki.[146] Siinä esitettiin yleisen tietoturvalain säätämistä. Sen säätämiseen ei kuitenkaan alettu.[147]

Tietoturvallisuusraportin jälkeen julkisuuslakiin (621/1999) säädettiin hyvän tiedonhallintatavan säännös. Julkisuuslain 18 §:ään sisältyy velvoite ottaa tietoturvallisuus huomioon jo julkisen tietohallinnon tietojärjestelmiä suunniteltaessa. Tämän jälkeen ollaan säädetty useita yksittäisiä tietoturvasäännöksiä.[148]

Suomessa ei olla toistaiseksi säädetty yleistä tietoturvallisuuslakia. Julkisella sektorilla tietoturvaa järjestävät ensisijaisesti julkisuuslaki (621/1999), asetus tietoturvallisuudesta valtionhallinnossa (681/2010) sekä henkilötietojen osalta henkilötietolaki (523/1999). Erityislainsäädännössä on lisäksi runsaasti salassapito– ja vaitiolosäännöksiä sekä tietojen suojaamisvelvoitteita. Nekin voidaan nähdä osana tietoturvalainsäädäntöä.[149]

Julkisuuslain 18 §:ssä määritellään hyvä tiedonhallintatapa. Se sisältää osana tietojärjestelmävaatimuksia myös tietoturvaa koskevia sääntöjä. Asetus tietoturvallisuudesta valtionhallinnossa täsmentää julkisuuslakia. Asetuksessa tietoturvallisuus nähdään osana hyvää tiedonhallintatapaa. Lainsäädännössä ensisijaisina sääntelyn kohteina ovat kuitenkin asiakirjojen sääntely ja asiakirjojen tietosisältöjen luokittelu. Tietoturvallisuuden perustason saavuttaminen edellyttää asetuksen mukaan myös tietoturvariskien kartoittamista. Asetus sisältää asiakirjojen kaikkiin käsittelyvaiheisiin liittyvää sääntelyä. Sääntelykohteena on myös asiakirjojen siirtäminen verkossa. Suojaamaton sähköpostiliikenne on ollut yksi informaatiohallinnon tavallisimpia ongelmia. Myös henkilötietolaki sisältää yleissäännöksen tietoturvallisuudesta henkilötietoja käsiteltäessä. Henkilötietolaki on yleislaki, jota tietoturva–asetus täydentää.[150]

Lisäksi lainsäädännössä on suuri joukko erillisiä tietoturvasäännöksiä. Muun muassa arkistolaki (ArkistoL, 831/1994) sisältää säännöksiä julkisen hallinnon viranomaisten arkistoinnista ja sen järjestämisestä, asiakirjojen laatimisesta, säilyttämisestä, käytöstä ja hävittämisestä. Sähköisestä asioinnista viranomaistoiminnassa (SähkAsL, 13/2003) annetun lain 22 §:n mukaan arkistolaitos antaa tarkempia määräyksiä ja ohjeita sähköisen asioinnin kirjaamisesta tai muusta rekisteröinnistä sekä arkistoinnista. Valtiovarainministeriö antaa ohjeita ja suosituksia sähköisen asioinnin yhteentoimivuuden ja tietoturvallisuuden

[146] Katso tarkemmin esim. Saarenpää–Pöysti (toim.) 1997.
[147] Saarenpää 2012b, s. 532.
[148] Saarenpää 2012b, s. 533–534.
[149] Saarenpää 2012b, s. 464.
[150] Saarenpää 2012b, s. 464–465.

varmistamisesta sekä sähköisten asiointipalvelujen järjestämisestä. Suomessa valtiovarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä.[151]

Edellinen tietoturvalainsäädännössä tapahtunut merkittävä parannus oli vuonna 2015 voimaan tullut tietoyhteiskuntakaari (516/2004), johon koottiin keskeiset sähköistä viestintää ja tietoyhteiskunnan palvelujen tarjontaa koskevat säännöt. Hanke perustui hallitusohjelmaan.[152] Tietoyhteiskuntakaarella kumottiin useita lakeja ja kyseinen laki sisältää 352 pykälää sähköistä viestintää koskevaa sääntelyä.[153] Tietoyhteiskuntakaaren tarkoituksena oli poistaa sääntelyn päällekkäisyyttä ja selkeyttää sääntelyä. Lisäksi haluttiin uudistaa toimilupajärjestelmä, turvata sähköisen viestinnän ja palveluiden jatkuvuus, tarkastaa kuluttajansuojaa ja yksityisyyden suojaa koskevat säännökset sekä selventää toiminnanharjoittajan velvoitteita.[154]

Laissa kansainvälisistä tietoturvallisuusvelvoitteista (KvtietoturvaL, 588/2004) säädetään puolestaan viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Lisäksi on olemassa valtavasti hajanaista sääntelyä tietoturvasta. Sääntelyä löytyy muun muassa laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (TietoturvallisuusarviointiL, 1406/2011), rikoslaissa (RL, 39/1889), henkilökorttilaissa (HKorttiL, 829/1999), valmiuslaissa (ValmiusL, 1552/2011), laissa turvallisuusselvityksistä (TurSeL, 726/2014), laissa yksityisyyden suojasta työelämässä (YksTyöelämäL, 759/2004) ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (TunnistamisL, 617/2009).

Laeissa on määriteltynä etuja ja haasteita tietoturvan ja tietosuojan kehittämiselle. Pääsääntö on, että tietojen pitää kulkea suojatusti siten, etteivät ne päädy sivulliselle. Lisäksi tietojen käyttöä pitää pystyä valvomaan. Käytännössä järjestelmiä joudutaan muuttamaan tai jopa kokonaan vaihtamaan tietoturvan varmistamiseksi. Hyvä tietoturvan ja tietosuojan lopputulos saavutetaan tietoturvan ja tietosuojan riskien hallinnalla sekä asiakokonaisuuksien ymmärtämisellä. [155] Suomen lainsäädännön mukaan tietoturva ja tietosuoja ovat, tai ainakin

[151] Saarenpää 2012b, s. 245.
[152] Pääministeri Jyrki Kataisen hallituksen ohjelma 22.6.2011, s. 51.
[153] Ks. tarkemmin tietoyhteiskuntakaaren 351 §. Lailla kumottiin ainakin viestintämarkkinalaki, sähköisen viestinnän tietosuojalaki, laki radiotaajuuksista ja telelaitteista, laki televisio– ja radiotoiminnasta, verkkotunnuslaki, laki eräiden suojauksen purkujärjestelmien kieltämisestä, laki eräiden radiotaajuuksien huutokaupoista ja laki tietoyhteiskunnan palvelujen tarjoamisesta sekä näiden lakien nojalla annetut lait,
[154] Tietoyhteiskuntakaari, Liikenne– ja viestintäministeriön www–sivut: www.lvm.fi, Tietoyhteiskuntakaari (viitattu 11.11.2015).
[155] Andreasson & Koivisto 2013, s. 16–17.

niiden pitäisi olla, osa organisaation päivittäistä toimintaa ja koskevat kaikkia organisaation toimintoja ja koko henkilöstöä.[156]

7. Tietoturvan kehittäminen ja ohjaus Suomessa

Nykyään Euroopan unionin sääntelyllä on vahva vaikutus Suomeen. Unionin sääntely ohjaa voimakkaasti kansallista lainsäädäntöä. Useiden kansallisten strategioiden, säädösten tai sääntelyn taustalla on sitoumus kansainväliseen sopimukseen tai unionin sääntely tai periaatepäätös.

Kansainvälistyminen on vaikuttanut parin viime vuosikymmenen aikana voimakkaasti Suomen oikeusjärjestykseen ja sen lähdepohjaan.[157] Normien määrä on kasvanut ja oikeusjärjestelmästä on tullut pirstaleinen. Samalla sovellettavan normistokokonaisuuden hallitseminen on vaikeutunut. Esimerkiksi Euroopan unionin myötä kansallisen oikeuden yhteydessä sovellettavaksi on tullut laaja ylikansallinen oikeusjärjestys, jossa on lisäksi lukuisia erityyppisiä ja eriasteisia normeja.[158] Samalla valta antaa uutta lainsäädäntöä on useilla aloilla siirretty kokonaan tai osittain jäsenvaltioilta unionille (niin sanottua delegoitua toimivaltaa). Toisaalta jäsenvaltiot luovuttavat valtaa EU–järjestelmälle ja sen ylikansallisille instituutioille vain siinä suhteessa kuin se edistää jäsenmaiden kansallisia intressejä. Lisäksi toimivallan käytössä tulee huomioida suhteellisuusperiaate (subsidiariteettiperiaate) ja toissijaisuusperiaate.[159] Toissijaisuusperiaate antaa vastauksen siihen, tuleeko jäsenvaltion vai EU:n käyttää toimivaltaa kyseisellä alalla. Suhteellisuusperiaatteen avulla arvioidaan sitä, millaisia menettelytapoja tulee omaksua tietyn tavoitteen saavuttamiseksi eli kuinka toimivaltaa tulee käyttää.[160] Nykyisin EU:n toimielimet ovat monissa suhteissa kansallisen lainsäätäjän yläpuolella. Muutoinkin nykyään yhä enemmän sääntelyä laaditaan niin sanotussa ylikansallisessa tilassa, tavallaan yksittäisen valtion yläpuolella.[161]

Suomessa ollaan tehty tietoturvaan liittyviä periaatepäätöksiä ja strategioita paljon. Seuraavaksi esitellään niistä muutama, kuten kansallinen tietoturvastrategia, toinen kansallinen tietoturvastrategia, yhteiskunnan turvallisuusstrategia ja kyberturvallisuusstrategia. Tämän jälkeen esitellään joukko tavalla tai toisella tietoturvallisuuden parissa työskenteleviä viranomaisia, joita niitäkin on lukuisa määrä.

[156] Andreasson & Koivisto 2013, s. 30.
[157] Kanninen 2009, s. 175 & Tala 2000, s. 390–392.
[158] Kanninen 2009, s. 175–176.
[159] Tiilikainen, 2005, s. 19 & Raitio 2010, s. 213.
[160] Raitio 2010, s. 215.
[161] Tala 2005, s. 55 & 77.

7.2 Periaatepäätökset ja strategiat

7.2.1 Kansallinen tietoturvastrategia (VNp 4.9.2003)

Ensimmäisen kansallisen tietoturvastrategian mukaan tietoyhteiskunnan mahdollisuuksien ja uhkien torjunta edellyttivät kaikkien toimijoiden luottamusta kehityksen suuntaan. Strategian mukaisesti kansalaisten ja yritysten luottamusta tietoyhteiskuntaan voitiin (ja voidaan) lisätä erityisesti tietoturvallisuutta ja yksityisyyden suojaa parantamalla. Strategialla pyrittiin torjumaan tietoturvallisuuden uhkia, mutta toisaalta myös hyödyntämään korkeatasoisen tietoturvallisuuden tarjoamia mahdollisuuksia.[162]

Tietoturvastrategian avulla Suomesta pyrittiin rakentamaan tietoturvallinen tietoyhteiskunta. Strategian tavoitteena oli edistää kansallista ja kansainvälistä tietoturvallisuusyhteistyötä, edistää kansallista kilpailukykyä ja suomalaisten tieto– ja viestintäalan yritysten toimintamahdollisuuksia, parantaa tietoturvallisuusriskien hallintaa, turvata perusoikeuksien toteutuminen ja kansallinen tietopääoma sekä lisäksi lisätä tietoturvallisuustietoisuutta ja –osaamista.[163]

7.2.2 Toinen kansallinen tietoturvastrategia (VNp 4.12.2008) – ”Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla”

Toisen kansallisen tietoturvastrategian visiona oli, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto– ja viestintäverkoissa että niihin liittyvissä palveluissa ja Suomi olisi tietoturvan edelläkävijämaa maailmassa vuonna 2015. [164]Keskeisenä painopisteenä strategialla on kansainvälisen verkostoyhteistyön ja kilpailukyvyn kehittäminen. Strategialla on kolme painopistealuetta, jotka ovat 1. perustaidot arjen tietoyhteiskunnassa, 2. tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä 3. kilpailukyky ja kansainvälinen verkostoyhteistyö.[165]

7.2.3 Yhteiskunnan turvallisuusstrategia (VNp 16.12.2010)

Strategia yhteiskunnan turvallisuudesta on jatkoa vuonna 2003 laaditulle ja vuonna 2006 päivitetyllä valtioneuvoston periaatepäätökselle yhteiskunnan elintärkeiden toimintojen

[162] Tietoturvalliseen yhteiskuntaan, Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 14.12.2004, s. 16.
[163] Tietoturvalliseen yhteiskuntaan, Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 14.12.2004, s. 17.
[164] Elämme jo pian vuodenvaihdetta 2016. Voi olla, että olemme piakkoin saamassa uuden tietoturvastrategian.
[165] Periaatepäätös kansallisesta tietoturvastrategiasta 4.12.2008.

turvaamisen strategiasta. Strategian tavoitteena oli turvata yhteiskunnan toimintakyky, säilyttää Suomen itsenäisyys ja edistää kansalaisten hyvinvointia ja turvallisuutta.[166]

Yhteiskunnan turvallisuusstrategian mukaan erityisesti elintärkeät toiminnot on turvattava kaikissa tilanteissa. Elintärkeät toiminnot[167] on tarkoitus turvata hallinnonalojen välisellä yhteistyöllä, johon liittyy tutkimusta, toiminnanohjausta ja lainsäädännön valmistelua. Strategiassa määritellään yhteiskunnan elintärkeät toiminnot ja niiden tavoitetilat, elintärkeitä toimintoja vaarantavat uhkamallit ja niihin liittyvät häiriötilanteet, toimintojen turvaamisen edellyttämät ministeriöiden strategiset tehtävät, kriisijohtamisen perusteet häiriötilanteiden hallitsemiseksi, strategian toimeenpanon seurannan ja kehittämisen sekä varautumisen ja kriisijohtamisen harjoittelun periaatteet. [168]

Uhkamallit ovat kuvauksia turvallisuusympäristön mahdollisista häiriöistä. Strategiassa kuvatut uhkamallit liittyvät muun muassa voimahuollon vakaviin häiriöihin, tietoliikenteen ja tietojärjestelmien vakaviin häiriöihin (kyberuhkiin), kuljetuslogistiikan vakaviin häiriöihin, yhdyskuntatekniikan vakaviin häiriöihin, elintarvikehuollon vakaviin häiriöihin, rahoitus– ja maksujärjestelmän vakaviin häiriöihin, julkisen talouden rahoituksen saatavuuden häiriintymiseen, väestön terveyden ja hyvinvoinnin vakaviin häiriöihin, suuronnettomuuksiin, luonnon ääri–ilmiöihin ja ympäristöuhkiin, terrorismiin ja muihin yhteiskuntajärjestystä vaarantavaan rikollisuuteen, rajaturvallisuuden vakaviin häiriöihin, poliittiseen, taloudelliseen ja sotilaalliseen painostukseen sekä sotilaallisen voiman käyttöön.[169]

7.2.4 Kyberturvallisuusstrategia (VNp 24.1.2013)

Valtioneuvosto antoi 24.1.2013 periaatepäätöksensä Suomen kyberturvallisuusstrategiasta. Strategian mukaan kyberturvallisuus on tavoitetila, jossa kyberympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus on Suomelle erityisen tärkeä, koska Suomi on tietoyhteiskuntana (verkkoyhteiskunta) riippuvainen tietoverkkojen ja järjestelmien toiminnasta ja näin ollen samalla myös haavoittuvainen näihin kohdistuville häiriöille. Toisaalta sama voidaan sanoa useasta muustakin länsimaasta. Kyberturvallisuuteen liittyy uhkia, mutta myös mahdollisuuksia ja voimavaroja. Turvallinen kybertoimintaympäristö helpottaa yksilöiden ja organisaatioiden

[166] Yhteiskunnan turvallisuusstrategia (VNp 16.12.2010).
[167] Suomalaisen yhteiskunnan elintärkeitä toimintoja ovat valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys (Yhteiskunnan turvallisuusstrategia, VNp 16.12.2010).
[168] Yhteiskunnan turvallisuusstrategia (VNp 16.12.2010).
[169] Yhteiskunnan turvallisuusstrategia (VNp 16.12.2010).

toimintaa ja suunnittelua. Hyvä toimintaympäristö voi parantaa myös Suomen kansainvälistä kiinnostavuutta investointikohteena. Toimiva ja hyvä kyberturvallisuus nähdään siis taloudellisen kasvun yhtenä mahdollistajana.[170]

Kyberturvallisuusstrategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Kyberturvallisuuden visioon kuuluu kolme kohtaa. Ensimmäisen kohdan mukaan Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan. Toinen kohta on, että kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti. Kolmantena kohtana esitetään, että vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.[171]

7.3 Viranomaiset

7.3.1 Ulkoministeriö, puolustusministeriö, suojelupoliisi, Viestintävirasto ja Viestintäviraston Kyberturvallisuuskeskus

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) 4 §:n mukaan ulkoministeriö (UM) toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena (National Security Authority, NSA). Tietoliikenneturvallisuuteen liittyvistä tehtävistä vastaavaa viranomaista kutsutaan kansainvälisen terminologian mukaan tietoliikenneturvallisuusviranomaiseksi (National Communications Security Authority, NCSA).[172] Suomessa Viestintävirasto toimii kansallisena tietojärjestelmien ja tietoliikenteen tietoturvallisuudesta (NCSA) vastaavana viranomaisena.[173]

Puolustusministeriö, pääesikunta, suojelupoliisi ja Viestintävirasto toimivat kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA). Ulkoministeriössä tehtävää hoitaa valtiosihteerin alaisuudessa toimiva kansallisen turvallisuusviranomaisen yksikkö. Suojelupoliisi (Supo) ja pääesikunta huolehtivat muun muassa henkilöiden taustojen selvittämisestä turvallisuusselvityksistä annetun lain (726/2014) nojalla.[174]

[170] Suomen kyberturvallisuusstrategia (VNp 24.1.2013), s. 1.
[171] Suomen kyberturvallisuusstrategia (VNp 24.1.2013), s. 2–3.
[172] HE 53/2010 vp, s. 3.
[173] Kansallinen turvallisuusviranomainen. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje 30.11.2010, s. 3.
[174] HE 53/2010 vp, s. 3 & ks. myös HE 57/2013 vp.

Kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), turvallisuusselvityksistä (726/2014) sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen (1406/2011) lakien mukaan Viestintäviraston tehtäviin kuuluvat erilaiset tietojärjestelmien turvallisuusarvioinnit ja –hyväksynnät.[175] Suomessa Viestintävirasto toimii Pohjois–Atlantin puolustusliiton (NATO, North Atlantic Treaty Organization) kanssa toteutettavan rauhankumppanuus–ohjelman edellyttämänä tietoliikenteen tietoturvallisuudesta vastaavana yhteistyötahona.[176]

Lisäksi tietoturvaloukkausten havainnointiin ja selvittämiseen liittyvät tehtävät (niin sanottu CERT –toiminta[177]) kuuluvat Viestintävirastolle. CERT –organisaatioita on perustettu ympäri maailmaa. Kyseiset organisaatiot toimivat yhteistyössä keskenään jakaen tietoa tietoturvaloukkauksista ja tiedottavat loukkauksista järjestelmien käyttäjille. CERT –toiminnan tarkoituksena on tietojärjestelmiin kohdistuvien tietoturvaloukkauksien ja uhkien toteutumisen ennaltaehkäisy ja torjunta mahdollisimman tehokkaasti. [178]

Viestintävirastoon perustettiin vuoden 2014 alusta Kyberturvallisuuskeskus, mikä perustuu valtioneuvoston hyväksymään kyberturvallisuusstrategiaan. Kyberturvallisuuskeskuksen tarkoituksena on vahvistaa Viestintäviraston nykyisten tietoturvatehtävien hoitamista. Kyberturvallisuuskeskuksen osaksi liitettiin viraston CERT–, NCSA– ja varautumistehtävät.[179]

7.3.2 Valtiovarainministeriö, VAHTI–ohjeet ja tietoturvallisuuden osa–alueet

Suomessa valtiovarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Valtiovarainministeriön alaisuudessa toimiva valtion tieto– ja kyberturvallisuuden johtoryhmä (VAHTI) on laatinut tietoturvallisuutta koskevia ohjeita, suosituksia, ja tavoitteita sekä muita tietoturvallisuuden linjauksia.[180] VAHTI:lla ei kuitenkaan ole erityistä lainsäädännöllistä asemaa.[181]

Tietoturvallisuudessa tarvitaan yhteensopivia ja yhdenmukaisia toimintaohjeita. Tietoturvaohjeet ja muutkin ohjeet voidaan jakaa yleisiin ohjeisiin, organisaatiokohtaisiin ohjeisiin ja jotain suppeaa osa–aluetta koskeviin erityisohjeisiin. VAHTI–ohjeet ovat hyvä

[175] Ks. lisää Viestintäviraston NCSA–toiminnoista. Viestintävirasto ohje 7.5.2015.
[176] HE 53/2010 vp, s. 6.
[177] CERT–toiminnalla tarkoitetaan tietoturvaloukkauksien ennaltaehkäisyä, havainnointia ja ratkaisua sekä tietoturvauhkista tiedottamista.
[178] HE 122/2008 vp, s. 1–2.
[179] Kyberturvallisuuskeskus vahvistaa Viestintäviraston nykyisiä tietoturvatehtäviä, julkaistu 24.10.2013.
[180] Ks. lisätietoa esim. Vahti Ohjaus, Valtiovarainministeriön www–sivut. (Saatavilla: http://vm.fi/ohjaus, viitattu 11.11.2015).
[181] Saarenpää 2012b, s. 245.

esimerkki joukosta yleisiä tietoturvaohjeita, joita organisaatiot voivat käyttää tietoturvatyönsä perustana.[182]

VAHTI:n ohjeet kattavat kaikki tietoturvallisuuden osa–alueet, jotka VAHTI:n mukaan ovat muun muassa henkilöstöturvallisuus, fyysinen turvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoliikenneturvallisuus, käyttöturvallisuus, haittaohjelmistoilta suojautuminen sekä tietoaineiston turvallisuus, varmuus– ja suojakopiointi. Käytännössä organisaatiot muodostavat kuitenkin omat tietoturvaosa–alueensa toiminnoissaan. Tietoturvallisuusohjeistuksen tavoitteena on sisällyttää tietoturvallisuus osaksi organisaation toimintaprosesseja, jolloin tietoturva toteutuu käytännön toiminnassa.[183]

7.3.3 Eduskunta

Perustuslain (PeL, 731/1999) mukaan eduskunta hyväksyy valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä (PeL 94.1). Perustuslakivaliokunnan tutkintakäytännön mukaisesti määräys katsotaan lainsäädännön alaan kuuluvaksi seuraavissa tapauksissa 1. jos se koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista, 2. jos määräys koskee yksilön oikeuksien ja velvollisuuksien perusteita, 3. jos määräyksen tarkoittamassa asiassa on perustuslain mukaan säädettävä lailla tai 4. Jos määräyksessä tarkoitetusta asiasta on jo voimassa lain säännöksiä taikka 5. siitä Suomessa vallitsevan käsityksen mukaan on säädettävä lailla. Lisäksi perustuslakivaliokunnan mukaan kansainvälisen velvoitteen määräys kuuluu lainsäädännön alaan siitä riippumatta, onko määräys ristiriidassa vai sopusoinnussa Suomessa lailla annetun säädöksen kanssa.[184] Eduskunta siis hyväksyy myös kansainväliset valtiosopimukset ja velvoitteet, jotka liittyvät tietoturvaan ja joiden nähdään sisältävän lainsäädännön alaan kuuluvia määräyksiä. Lisäksi eduskunta luonnollisesti talousarviossaan ainakin osittain päättää tietoturvan kehittämiseen laitettavista taloudellisista resursseista.[185]

7.3.4 Valtioneuvoston kanslia

Yksi 12 ministeriöstä on valtioneuvoston kanslia (VNK), jonka vastuulla ovat yhteiskuntapoliittiset suunnittelutehtävät ja asiat, jotka eivät kuulu muiden ministeriöiden toimialoihin. Kanslian toiminta muodostuu muun muassa pääministerin ja hallituksen

[182] Andreasson & Koivisto 2013, s. 44.
[183] Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007, s. 37 ja s. 88.
[184] PeVL 11/2000 vp, PeVL 12/2000 vp ja HE 139/2012 vp, s. 18.
[185] Ks. tarkemmin perustuslain 83 §.

toimintaa ja päätöksentekoa tukevista tehtävistä sekä yleisön ja viranomaisten palveluista. Lisäksi valtioneuvoston kanslia valmistelee Suomen unionipolitiikan yleisiä linjauksia yhdessä ministeriöiden kanssa.[186] Valtioneuvoston kanslia vastaa myös muun muassa kyberturvallisuusstrategian kansallisen valmistelun yhteensovittamisesta.[187]

7.3.5 Liikenne– ja viestintäministeriö

Suomen tietoverkkojen kansallisia kehittämislinjoja suunniteltiin lisää vuonna 1994. Tuona vuonna liikenneministeriö laati mietinnön Tietoverkkojen kansalliset kehittämislinjat (1995–1998), jonka pohjalta käynnistettiin vuonna 1995 tietoverkkojen kehittämisohjelma (TIVEKE).[188]

Nykyään Liikenne– ja viestintäministeriön (LVM) hallinnonalaan kuuluvat viestintävirasto, liikennevirasto, liikenteen turvallisuusvirasto, ilmatieteen laitos, Finnpilot Pilotage Oy, Finavia Oy ja yleisradio. Ministeriön yksi päätehtävä on hallinnonalansa strateginen tulosohjaus. Ministeriö valvoo virastojensa ja laitostensa toimintaa ja seuraa niiden kehitystä. Viestintävirasto huolehtii muun muassa siitä, että Suomi on tietoturvallinen yhteiskunta, jossa viestintäverkot ja viestintämarkkinat toimivat häiriöttä ja tehokkaasti ja jossa kuluttajan asema on turvattu. Liikenteen turvallisuusvirasto on puolestaan liikennejärjestelmän sääntely– ja valvontatehtävistä vastaava hallinto– ja turvallisuusviranomainen, jonka tehtävänä on edistää liikenteen turvallisuutta ja kestävää kehitystä liikennejärjestelmissä.[189]

Tällä hetkellä ehkä kaksi merkittävintä hanketta liikenne– ja viestintäministeriössä ovat Digitaalisen liiketoiminnan kasvuympäristön rakentaminen ja norminpurku säädösten sujuvoittamiseksi.[190] Molemmilla voi olla nähtävillä jollain tasolla vaikutuksia kansalliseen tietoturvaan ja sääntelyyn. Digitalisaatiota voidaan parantaa kasvattamalla luottamusta sähköiseen maailmaan esimerkiksi tietoturvaa parantamalla. Norminpurku puolestaan voi vaikuttaa tietoturvan sääntelyperustaan.

---

[186] Valtioneuvoston kanslian toiminta. Valtioneuvoston kanslian www–sivut (Saatavilla: http://vnk.fi/, viitattu 11.11.2015).
[187] Suomen kyberturvallisuusstrategia – mitä tehdään ja miksi? Turvallisuuskomitean esitys 26.11.2013 & lisätietoa turvallisuuskomiteasta sen www–sivuilta (Saatavilla: http://www.turvallisuuskomitea.fi/, viitattu 11.11.2015).
[188] Huuhtanen 2001, s. 22 & Lilius 1997, s. 13.
[189] Liikenne– ja viestintäministeriön hallinnonala, LVM:n www–sivut: hallinnonala (Saatavilla: http://www.lvm.fi/hallinnonala, viitattu 11.11.2015).
[190] Ks. tarkemmin Pääministeri Juha Sipilän hallituksen strateginen ohjelma 29.5.2015, hallituksen julkaisusarja 10/2015 & LVM:n www–sivuilta hallituksen kärkihanke: Norminpurku ja hallituksen kärkihanke Digitaalisen liiketoiminnan kasvuympäristön rakentaminen.

7.3.6 Arkistolaitos

Arkistolaitos toimii opetus– ja kulttuuriministeriön hallinnonalassa. Laitos ohjaa viranomaisten asiakirjahallinnon ja arkistotoimen hoitoa, huolehtii arkistotoimen kehittämisestä ja määrää, mitkä valtion– ja kunnallishallinnon asiakirjat tulee säilyttää pysyvästi. Ohjeissaan arkistolaitos ottaa kantaa myös tietoturvallisuuteen liittyviin asioihin. Arkistolaitoksen tehtäviä säätelee arkistolaki (831/1994) ja asetus arkistolaitoksesta (ArkistoA, 832/1994).[191]

7.3.7 Keskusrikospoliisi

Valtioneuvosto ohjaa poliisitoimintaa. Sisäministeriö puolestaan vastaa poliisin toimialan ohjauksesta ja valvonnasta. Poliisin organisaatio on kaksiportainen. Organisaatiota johtaa sisäasianministeriön alainen poliisihallitus. Poliisihallituksen alaisuudessa toimivat poliisilaitokset, poliisin valtakunnalliset yksiköt. Yksi poliisin valtakunnallisista yksiköistä on keskusrikospoliisi (KRP).[192]

Keskusrikospoliisin päätehtävänä on 1. torjua kansainvälistä, järjestäytynyttä, ammattimaista, taloudellista ja muuta vakavaa rikollisuutta, 2. suorittaa tutkintaa, 3. tuottaa asiantuntijapalveluita ja 4. kehittää rikostorjuntaa ja rikostutkintamenetelmiä.

KRP on vahvasti mukana muun muassa tietotekniikka– ja kyberrikollisuuden torjunnassa. Keskusrikospoliisin päätehtäviä tietotekniikkarikollisuuden torjunnassa ovat vakavimpien rikosten tutkinta, internet– ja verkkotiedustelu sekä esitutkintaan liittyvät asiantuntijapalvelut poliisille ja muille viranomaisille. Näiden lisäksi KRP seuraa tietotekniikan ja tietoverkkojen kehitystä sekä tunnistaa niissä esiintyviä uusia rikosilmiöitä. Internet– ja verkkotiedustelusta vastaa KRP:n tiedusteluosaston Internet–tiedustelujaos.[193] Tietotekniikkaan liittyviä rikosilmiöitä ovat muun muassa identiteettivarkaudet ja kohdistetut (haittaohjelma)hyökkäykset sekä sähköpostihuijaukset ja maksukorttirikollisuus.[194]

Keväällä 2015 KRP:n yhteyteen perustettiin kyberrikostorjuntakeskus. Kyberrikostorjuntakeskuksen keskeisimmät tehtävät ovat muiden poliisiyksiköiden tukeminen kyberrikostorjuntaan liittyvissä asioissa, verkkorikostorjunta, tietoteknisen tutkinnan asiantuntijapalvelut, internettiedustelu, tietoverkkorikostorjunnan päivystys, tilannekuvan

[191] Lisätietoa arkistolaitoksesta www–sivuilta: www.arkisto.fi (viitattu 11.11.2015).
[192] Tietoa poliisista, organisaatio, poliisin www–sivut: Organisaatio (Saatavilla: http://www.poliisi.fi/tietoa_poliisista/organisaatio, viitattu 11.11.2015).
[193] Tietotekniikkarikollisuus, poliisin www–sivut: Tietotekniikkarikollisuus (Saatavilla: https://www.poliisi.fi/rikokset/tietotekniikkarikollisuus, viitattu 11.11.2015).
[194] Rikosilmiöitä, poliisin www–sivut: Tietorikoksia (Saatavilla: https://www.poliisi.fi/rikokset/rikosilmioita/tietorikoksia, viitattu 11.11.2015).

ylläpitäminen, uhka–arvioiden tuottaminen sekä toimialaan liittyvä kansallinen ja kansainvälinen yhteistyö.[195]

7.7.8 Tietosuojavaltuutetun toimisto

Tietosuojavaltuutettu on keskeisin henkilötietojen valvontaa suorittava viranomainen. Virka perustettiin henkilörekisterilain (kumottu 471/1987) voimaantulon yhteydessä. Tietosuojavaltuutetun toimivaltuuksia tarkistettiin tietyiltä osin henkilötietolain (523/1999) korvatessa henkilörekisterilain. Tietosuojavaltuutetun ensisijainen tehtävä on vaikuttaa rekisterinpidon lainmukaisuuteen ennakolta, kehittää hyvää tietojenkäsittelytapaa ja ehkäistä tietosuojaloukkausten tapahtumista. Ennaltaehkäisevä työ on tietosuojavaltuutetun toimiston työssä tärkeää. Tietosuojavaltuutettu muun muassa luennoi koulutustilaisuuksissa ja panostaa puhelinneuvontaan. Suuri merkitys on myös sidosryhmäyhteistyöllä. Tietosuojavaltuutetun toimiston edustajat osallistuvat eri hallinnonalojen neuvottelukuntiin ja työryhmiin, joiden työssä yksityisyyden suojan merkitys on suuri.[196]

Tietosuojavaltuutettu ohjaa ja valvoo henkilötietolain täytäntöönpanoa. Henkilötietoja käsitellessä lainsäädännön velvoite on selvä. Henkilötietoja käsitellessä huolellisuus– ja suojaamisvelvoitteet sekä tietoturva on otettava riittävällä tavalla huomioon. Suojaamisvelvoitteeseen kuuluu lisäksi fyysisestä tietoturvasta huolehtiminen, esimerkiksi ovet on lukittava ja henkilötietoja sisältävä manuaalinen aineisto suojattava siten, etteivät sivulliset pääse näkemään tietoja.[197]

7.4 Työ– ja elinkeinoministeriö sekä Huoltovarmuuskeskus

Huoltovarmuuskeskus (HVK) on työ– ja elinkeinoministeriön (TEM) hallinnonalan laitos. Keskuksen tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta. Huoltovarmuus tarkoittaa kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.[198]

---

[195] Poliisin valmiuksia parannetaan nykybudjetin raameissa, mutta se ei riitä, 19.03.2015 (Saatavilla: https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/poliisin_valmiuksia_parannetaan_nykybudjetin_raameissa_mutta_se_ei_riita_28088, viitattu 11.11.2015).
[196] Vanto 2011, s. 168 ja HE 96/1998 vp, s. 65–66.
[197] Ks. lisätietoja esim. Saako henkilötietoja lähettää sähköpostilla salaamattomana? Tietosuojavaltuutetun www–sivut, 2008 (Saatavilla: http://www.tietosuoja.fi/fi/index/ratkaisut/saakohenkilotietojalahettaasahkopostilla.html, viitattu 14.11.2015).
[198] Lisätietoa huoltovarmuuskeskuksen www–sivuilta: www.huoltovarmuus.fi (viitattu 11.11.2015).

7.5 Yksityiset toimijat ja organisaatiot

Suomessa on kansallisten viranomaisten lisäksi lukuisia yksityisiä toimijoita ja organisaatioita, jotka on perustettu kehittämään ja ylläpitämään tietoturvaa.

Suomessa perustettiin vuonna 1981 tietotekniikan kehittämiskeskus (TIEKE). Vuonna 1984 TIEKE:ssä alettiin tutkia uusina projekteina muun muassa tietoturvaa ja atk–riskiselvitystä.[199]

Tietoturva ry (Finnish Information Security Association, FISA) on puolestaan perustettu 1997. Yhdistyksellä on 850 henkilöjäsentä ja 50 yritys– ja yhteisöjäsentä, mikä tekee yhdistyksestä Suomen suurimman tietoturva–alan organisaation. Yhdistyksen tavoitteena on toimia edistäjänä tietoturva–alalla ja jäsentensä yhdyssiteenä, sekä edistää hyvien tietoturvatapojen noudattamista kaikilla tietoturvan osa–alueilla. Toimintamuotoina yhdistyksellä ovat erilaisten tapahtumien, keskustelutilaisuuksien, seminaarien ja yritysvierailuiden järjestäminen. Tietoturva ry on tietotekniikan liitto ry:n alajärjestö.[200]

Suomalaisen tietoturva–alan yksi suurimpia vahvuuksia ovat hyvä maine ja aktiivinen tietoturvaharrastajien yhteisö. Vuonna 2012 perustetussa tietoturvaklusteri FISC:issä (Finnish Information Security Cluster[201]) on mukana 35 yritystä. Eurooppalaisittain Suomessa on tärkeä tietoturva–alan keskittymä. Tietoturva–alan toimijoiden välinen yhteistyö on tärkeää alan kehityksen kannalta.[202]

8. Tietoturvasääntelyn tulevaisuus

8.1 Lainsäädäntö

8.1.1 Tarvitaanko yleistä tietoturvalakia?

Verkkoyhteiskunnassa tietoturvallisuus on tietoteknisesti että oikeudellisesti tärkeä asia. Elämme nykyään tietoverkoista riippuvaisessa maailmassa. Myös perusoikeuksiemme käsittely on tietojärjestelmissä ja tietoverkoissa tapahtuvaa. Yhteiskunta on muuttunut, mutta muutoksista huolimatta meille ei ole edelleenkään yleistä tietoturvallisuuslakia. Tietoturvan merkitys ollaan kuitenkin nykyään paremmin ymmärretty esimerkiksi valtionhallinnossa. VAHTI ohjeineen ei kuitenkaan vastaa laissa säätämistä. Viestintäviraston Kyberturvallisuuskeskuksen CERT–toiminto on puolestaan rajallisine resursseineen vaatimaton yritys parantaa julkisen sektorin taholta verkkoyhteiskunnan tietoturvan

[199] Huuhtanen 2001, s. 30.
[200] Tietoturva ry:n www–sivut (Saatavilla: www.tietoturva.fi, viitattu 14.11.2015).
[201] Lisätietoa FISC:n www–sivut (Saatavilla: http://fisc.fi/, viitattu14.11.2015).
[202] Suomesta tietoturvan turvasatama? TTL ry, julkaistu 30.09.2013.

toteutumista.[203] Toisaalta vuoden 2014 alussa perustetun Kyberturvallisuuskeskuksen tarkoituksena on ollut vahvistaa Viestintäviraston nykyisten tietoturvatehtävien hoitamista.[204]

Tietoturvallisuuden sääntely on kokonaisuutena erittäin vaativa asia. Tietoturvallisuus alueena ulottuu ohjelmisto–, laite– ja verkkoturvallisuudesta pääte– ja päätekäyttäjäturvallisuuteen sekä lisäksi turvallisuuteen tietojenkäsittelyn ulkoistamistilanteissa aina pilvipalveluihin asti. Vain osa tästä kokonaisuudesta on säänneltyä tai ohjattua. Alue, johon tietoturvallisuus liittyy, on valtava ja sen sääntеleminen kokonaisuudessaan on suuri haaste. Osaksi sääntelyn ja ohjauksen puute johtuu siitä, että tietoturvallisuutta yleisenä oikeusperiaatteena ei olla asianmukaisesti tunnistettu.[205] Juuri yleisten oppien varaan myös lainsäädäntökin rakennetaan tai tulisi rakentaa. Yleisten oppien keskeisen osan muodostavat oikeudelliset käsitteet, teoriat ja oikeusperiaatteet. Tietoturvallisuus alueena on myös haastava siinä mielessä, että se osuu perinteisessä oikeussystematiikassa useille eri oikeudenaloille.[206]

Tilanteen parantamiseksi tarvitaan yhteinen käsitys ihmisen oikeuksien merkityksestä tietotekniikkaa hyödynnettäessä. Tarvittaisiin eri asiantuntijoiden yhteistoimintaa ja –ymmärrystä tietoturva–asioista. Oikeudellisesti katsottuna tarvittaisiin myös perustuslain muuttamista siten, että jo siinä osoitettaisiin selkeästi tietoturvallisuuden merkitys perusoikeutena. Tarvitsemme yleistä tietoturvalakia.[207] Nykyinen sääntely on hajanaista, josta seuraa vaikeus varmistua riittävän yhtenäisestä tietoturvallisuusnormien soveltamisesta ja tulkinnasta. Lisäksi normeja on nykyään valtava määrä ja tietoturvallisuusnormeja on sijoitettu hajalleen lainsäädäntöön. Oikeusvarmuus voi kärsiä tästä. Tietoturvan yleislakiin voitaisiin koota tietoturvaa ohjaavat yleisperiaatteet. Yleislain normeja voitaisiin tarvittaessa täsmentää erityislainsäädännössä ja alemmanasteisissa normeissa.[208]

8.1.2 Tietoturvallisuusnormien jaottelua

Tietoturvallisuuteen liittyvät normit voidaan tunnistaa sen mukaan, mikä on normin tavoite tai tehtävä suhteessa informaation tai tietojenkäsittelyn luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseen. Turvallisuusnormien jaottelu voidaan esittää seuraavan yhdeksän pääryhmän avulla:

[203] Saarenpää 2012b, s. 533.
[204] Kyberturvallisuuskeskus vahvistaa Viestintäviraston nykyisiä tietoturvatehtäviä, julkaistu 24.10.2013.
[205] Saarenpää 2012b, s. 519.
[206] Pöysti 1997, s. 3.
[207] Saarenpää 2012b, s. 534.
[208] Saarenpää–Pöysti (toim.) 1997, s. ixxiv.

1. Tietoturvallisuuden ylläpitoon välittömästi velvoittavat käyttäytymisnormit ja näitä tehostavat sanktionormit.
2. Tietoturvallisuuden huolehtimisesta välillisesti edellyttävät normit ja näitä tehostavat sanktionormit.
3. Tietoturvallisuuden institutionaaliset suojasäännökset (eli tietoturvallisuutta edistäviä ja ylläpitäviä organisaatioita perustavat) ja näiden toimintaa ohjaavat normit ja instituutiot.
4. Informaatioon ja tietojärjestelmiin kohdistuvia vahingollisia tekoja ehkäisevät ja sanktioivat normit (muun muassa tietorikoksia koskevat normit).
5. Tiedon ja informaatioaineiston todennettavuutta ja historiallista säilymistä turvaavat ja edistävät normit (muun muassa muotosäännökset).
6. Todistelua ja hyväksyttävien todisteiden muotoa koskevat todistusoikeudelliset normit ja riskinjakoa reaalimaailman tapahtumien selvittämiseen epävarmuustilanteissa osoittavat todistustaakka– ja presumptionormit.
7. Rikollisuuden ehkäisemistä ja torjuntaa koskevat normit.
8. Informaatiosodankäyntiin varautumista ja yhteiskunnan ja valtion ulkoisiin turvallisuusuhkiin valmistautumista koskevat ja yhteiskunnan kriittisten tietoliikennetoimintojen jatkuvuutta turvaavat normit.
9. Tietoturvallisuuspalveluja ja –tuotteita sääntelevät normit (muun muassa sähköistä allekirjoitusta ja kolmannen osapuolen palveluja koskevat normit).[209]

8.1.3 Sääntelyn vaihtoehdot

Aina on olemassa vaihtoehtoja uudelle sääntelylle. Lainvalmistelussa koskevissa ohjeissa ja kehittämisohjelmissa on 1970–luvulta lähtien korostettu erilaisten toimintavaihtoehtojen selvittämistä osana säädösvalmistelua. Kansallisissa ja kansainvälisissä lainvalmistelun kehittämisoppaissa vaaditaan usein vaihtoehtojen parempaa hyödyntämistä. Ainakin OECD on arvostellut vaihtoehtojen hyödyntämättömyyttä. OECD on myös todennut, että eri vaihtoehtojen tarjoamat mahdollisuudet jäävät edelleen usein hyödyntämättä[210] Lisäksi muun muassa Vuoden 2007 lainsäädäntösuunnitelmaan sisältyi yhtenä säädösvalmistelun periaatteena erilaisten vaihtoehtoisten ohjauskeinojen aktiivinen käyttö.[211] Monipuolinen

[209] Saarenpää–Pöysti (toim.) 1997, s. ixxi.
[210] Tala 2007, s. 1–2.
[211] Tuloksellisuustarkastuskertomus hallituksen lainsäädäntösuunnitelma, valtiontalouden tarkastusviraston tarkastuskertomukset 18/2012, s. 47.

vaihtoehtojen tarkastelu voi parantaa sääntelyn tuloksellisuutta tavoitteiden kannalta, lisätä sääntelyn kustannustehokkuutta ja tuottaa sellaisia paremmin toimivia sääntelyjä, joita erilaiset kohdetahot hyväksyvät ja noudattavat aiempaa paremmin.[212]

Lainvalmistelutoiminnan kannalta käyttökelpoinen vaihtoehto on esimerkiksi itsesääntely. Itsesääntelyssä organisaatio laatii itse omaa toimintaansa koskevat säännöt, luo niihin valvontajärjestelmän mahdollisine sanktioineen ja mekanismin, jolla erimielisyydet voidaan tarvittaessa ratkaista. Itsesääntelyllä on vahvat perinteet ja Euroopan talous– ja sosiaalikomitean mukaan ainakin 60 % eurooppalaisista eri alojen ammatillisista yhteisöistä on luonut jonkinlaisen itsesääntelyjärjestelmän.[213]

Erilaiset standardit voidaan laskea kuuluvaksi itsesääntelyyn. Tietoturvallisuuden oikeudellisen sääntelyn tulisikin perustua hallinto–oikeudelliseen ja yksityisoikeudelliseen sääntelyyn.[214] Tietoturvallisuuden sääntelyssä itsesääntelyn vaihtoehtoa tulisi punnita perusteellisesti.

Yhteissääntelyssä julkinen vallankäyttäjä ja yksityinen osapuoli osallistuvat yhdessä sääntelytehtävän hoitamiseen. Kummallakin osapuolella on oma roolinsa, oma tehtävänsä ja oma vastuunsa. Hyvä esimerkki yhteissääntelystä on asianajotoiminnan valvontajärjestelmä, jonka keskeisiä osia ovat asianajajalaki, itsesääntelyn avulla luodut hyvää asianajotapaa koskevat ohjeet sekä alan ja valtiovallan nimeämistä edustajista koostuva valvontaelin.[215]

Lisäksi vaikka oikeudellisella sääntelyllä pyritään usein hallitsemaan erilaisia riskejä, oikeudellinen sääntely itsessäänkin saattaa aiheuttaa kustannuksia ja riskejä. Sääntelyriski tarkoittaa uhkaa siitä, että sääntely ja oikeusnormit aiheuttavat tarkoittamattomia kustannuksia ja muita epäedullisia vaikutuksia yksilöille, ryhmille ja taloudellisille toimijoille.[216] Suhteellisuusperiaatteen mukaan tietoturvallisuustoimenpiteiden ja –sääntelyn laajuus ja kustannukset sekä suojattavan intressin, esimerkiksi yksityisyyden suojaamisen, tulee olla tulee olla järkevässä tasapainossa keskenään.[217]

Yksi ryhmittely vaihtoehtoiselle sääntelylle voi olla esimerkiksi seuraava: 1. ei mitään uutta julkisen vallan toimenpidettä, 2. Nykyisen sääntelyn sisällön tai toimeenpanon tarkastaminen, 3. tiedotus ja kasvatus, 4. itsesääntely, 5. yhteissääntely ja 6. taloudelliset toimintavälineet.[218]

---

[212] Tala 2007, s. 5.
[213] Tala 2007, s. 9–10.
[214] Saarenpää–Pöysti (toim.) 1997, s. xxxv.
[215] Tala 2007, s. 11–13.
[216] Pöysti 1997b, s. 45.
[217] Pöysti 1997b, s. 53.
[218] Tala 2012, s. 8.

8.1.4 Mitä seuraavaksi sääntelyssä?

Komission kyberturvallisuusstrategiaan liittyvä ehdotettu verkko– ja tietoturvaa koskeva direktiiviehdotus[219] lisännee tietoturvaan liittyvää sääntelyä Suomessa, sillä direktiivin tavoitteet tulee implementoida osaksi kansallista sääntelyä. Direktiivi jättää kansallisten viranomaisten valittavaksi muodon ja keinot, joilla direktiivi saatetaan osaksi jäsenvaltion kansallista lainsäädäntöä.

Euroopan parlamentin ja neuvoston asetusehdotus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta[220] (yleinen tietosuoja–asetus) ja sen kanssa samaan aikaan annettu direktiiviehdotus henkilötietojen käsittelystä rikos– ja poliisiasioissa[221] voivat tuoda osaltaan uutta sääntelyä Suomeen. Toisaalta tietosuoja–asetus voi myös osaltaan vähentää kansallista sääntelyä, kun useasta henkilötietojen sääntelyyn liittyvästä asiasta säännelläänkin unionitasolla. Tämä tosin voi tehdä sääntelystä pirstaloitunutta. Tulevaisuudessa asetuksen voimaantulon jälkeen voidaan luottaa siihen, että henkilötietojen käsittelystä säännellään samalla tavalla kaikissa unionin jäsenmaissa.

Asiassa on huomioitava myös pääministeri Juha Sipilän hallitusohjelman kärkihankkeet. Yksi näistä on norminpurku säädösten sujuvoittamiseksi. Norminpurkuhankkeen tavoitteena on helpottaa sekä yritysten toimintaa että kansalaisten arkea sääntelyä keventämällä ja uudistamalla. Tarkoituksena on myös tukea Suomen kasvua, vahvistaa kilpailukykyä ja edistää digitalisaatiota. [222] Mahdollinen uusi tietoturvaa koskeva sääntely tulisi olla erityisen hyvin perusteltua, jotta se olisi yhdensuuntainen kyseisen kärkihankkeen kanssa. Käyttökelpoinen vaihtoehto uudelle lainsäädännölle on toimiva itsesääntely, standardit ja toimintaa ohjaavat strategiat.

---

[219] COM(2013) 48 final, ns. NIS–direktiivi.

[220] Ehdotus Euroopan parlamentin ja neuvoston asetukseksi: yksilöiden suojelusta henkilötietojenkäsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja–asetus) / COM(2012) 11 Final, annettu 25.1.2012.

[221] Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimusta, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (direktiiviehdotus henkilötietojen käsittelystä rikos– ja poliisiasioissa) COM(2012) 10 Final, annettu 25.1.2012.

[222] Ks. tarkemmin Pääministeri Juha Sipilän hallituksen strateginen ohjelma 29.5.2015, Hallituksen julkaisusarja 10/2015 sekä LVM:n www–sivuilta hallituksen kärkihanke: Norminpurku.

8.2 Teknologia, johtaminen ja tavat toimia

8.2.1 Teknologia ja sen kehitys

Tietoturvallisuus on monitahoinen, usean eri alan asiantuntijoita ja erityisosaamista vaativa alue. Tietoturvallisuutta voidaan parantaa usein eri tavoin. Tavat voidaan karkeasti jakaa hallinnollisiin, teknisiin tai lainsäädännöllisiin. Usein tarvitaan kaikkia näitä tapoja, jotta tietoturvan tosiasiallisesti voidaan sanoa olevan hyvällä mallilla.

Uusia teknologisia ratkaisuja kehitetään jatkuvasti ja tietoturvaongelmien tekninen havainnointikyky paranee koko ajan. Tekninen tietoturva liittyy muun muassa palomuurien, virustorjunnan, roskapostin suodatuksen, tietojen varmuuskopioinnin, työasemien, palvelinympäristön sekä konesalien ajanmukaiseen hoitamiseen sekä laitteiden toimintahäiriöihin varautumiseen.[223]

8.2.2 Riskit ja tietoturva

Liiketoimintaan ja tietojenkäsittelyyn sekä kaikkeen inhimilliseen toimintaa kuuluu aina riskejä.[224] Turvallisuus voidaan kuvata olotilaksi, jossa mahdollisuus riskien ja uhkien toteutumisesta on mahdollisimman pieni.[225] Tietoturvallisuuden perustason saavuttaminen edellyttää tietoturvariskien kartoittamista ja tietoturvatoimenpiteet on hyvä perustaa kattavaan riskien arviointiin.[226] Tietoturvariskejä tulee arvioida vallitsevan lainsäädännön, toimintaympäristön vaatimusten ja kustannusten näkökulmasta. Lisäksi tietoriskejä tulee arvioida organisaation perustehtävien ja niiden saavuttamiseksi asetettujen strategioiden ja tavoitteiden mukaan.[227]

Riskien arvioinnin merkitys tulee esille myös asetuksessa tietoturvallisuudesta valtionhallinnossa. Lisäksi OECD:n tietoturvaperiaatteista kuudes on riskien arviointi. Periaatteen mukaan toimijoiden tulee suorittaa riskien arviointia. Jatkuvaan riskienhallintaan kuuluu riskien ja uhkien arviointi sekä riskinhallintakeinoista päättäminen.[228] Riskianalyysin lähtökohtana on aina organisaation kokonaisturvallisuus. Tarkoituksena ei siis ole tehdä riskianalyysia pelkästään tietystä tietojärjestelmästä vaan riskien kartoittaminen alkaa kokonaisuuden kartoittamisella ja arvioinnilla.[229]

---

[223] Andreasson & Koivisto 2013, s. 237.
[224] Hakala et al. 2006, s. 90.
[225] Pöysti 1997b, s. 21.
[226] Porvari 2012, s. 103 ja Andreasson & Koivisto 2013, s. 39.
[227] Andreasson & Koivisto 2013, s. 39.
[228] Porvari 2012, s. 103.
[229] Hakala et al. 2006, s. 79.

Tietoriskit (myös tietoturvariskit) voidaan nähdä sekä liikeriskeinä että vahinkoriskeinä. Perinteisten liiketoimintaa ja organisaatioiden tiloja uhkaavien riskien (tulipalo, myrskyvahinko, varkaus jne.) joukkoon on tullut uusia vaikeammin arvioitavia tietoriskejä. Uusia järjestelmiä otetaan käyttöön huolimatta siitä, että niihin liittyviä riskejä ei tunneta. Tekniikka kehittyy valtavaa vauhtia. Osa riskeistä paljastuu vasta vahingon tapahduttua. Tietoriskin luonteeseen liittyy se, ettei niillä ole kansallisia rajoja. Tietoriskejä voidaan ryhmitellä eri tavoin. Yksi tapa on ryhmitellä riskit neljään alueeseen, jotka ovat käyttöriskit, kehittämisriskit, infrastruktuuririskit ja strategiset riskit. Tavallisimpia käyttöriskejä ovat tietoturvallisuus– ja luotettavuusongelmat. Tyypillisiä kehittämisriskejä ovat puolestaan hankkeiden myöhästyminen tai kustannusten ylittyminen. Infrastruktuuririskejä ovat laitteistojen tai ohjelmistojen yhteensopimattomuus ja tiedon huono laatu. Ohjelmistojen yhteensopivuutta voidaan parantaa esimerkiksi standardein. Strategiset riskit johtuvat puolestaan menetetyistä strategisista mahdollisuuksista huonon ajoituksen tai strategian takia.[230]

On olemassa paljon erilaisia tapoja hallita ja kontrolloida turvallisuus–, tietosuoja– ja luottamusriskejä. Yksi esimerkki riskien hallinnan ohjenuorasta on ISO 27000 standardin parhaat toimintatavat.[231] Tietoturvastandardit mahdollistavat riskien ottamisenkin, kunhan ne otetaan tietoisesti ja päätös perustuu ennalta määriteltyjen kriteerien perusteella tehtyyn harkintaan.[232]

Alueita, joilla käytännön tietoturvatoimintaa voidaan eri tavoin hallita ovat muun muassa fyysinen kulun– ja käytönvalvonta, sovellusten kehittäminen ja ylläpitäminen, haavoittuvuuksien hallinta, havainnointi, tunnistaminen ja todentaminen, käytön– ja kulunvalvonta, salaaminen, jatkuvuus ja tietoturvaloukkauksien havainnointi, tietoturvatestaus, yleisesti tunnustettujen komponenttien käyttö sekä tiedon koko elinkaaren selventäminen.[233]

Organisaatiot voivat pyrkiä hallitsemaan riskejä myös siirtämällä niitä organisaation ulkopuolelle. Yritykset voivat esimerkiksi käyttää ulkoisia palveluita muun muassa laskutuksessa tai rahoituksessa. Tietoturvallisuusriskejä voidaan siirtää organisaation ulkopuolella ulkoistamalla tietojenkäsittelytoimia niitä tuottaville yrityksille. Toisaalta on huomioitava, että ulkoistettu riskikin voi olla hoitamattomana yhtä vakava kuin sisäinen riski.

[230] Porvari 2012, s. 4.
[231] Robinson et al. 2010, s . 17.
[232] Hakala et al. 2006, s. 90.
[233] Robinson et al. 2010, s . 17.

Ulkoistustilanteessa on varmistuttava palveluntarjoajan turvallisuuden riittävästä tasosta ja seurattava palveluntarjoajan toimintaa.[234]

8.2.3 Tietoturvallisuuden johtaminen

Tietoturvallisuuden johtaminen on vielä suhteellisen uusi asia. Pelkkä tietoturvallisuuden tekninen kohentaminen ei auta parantamaan tietoturvan tasoa organisaatioissa ja yrityksissä. Tarvitaan myös tietoturvallisuuden johtamista. Tietoturvallisuuden johtaminen on järjestelmällistä työtä turvallisuusajattelun lisäämiseksi. Tarkoituksena on sitoa turvallisuusajattelu organisaation jokapäiväisiin rutiineihin kaikissa toiminnoissa.[235] Voidaan puhua toimintaan sisäänrakennetusta tietoturvasta.

Kokonaisvastuu tietoturvallisuuden kehittämisestä ja ylläpidosta on organisaation ylimmällä johdolla. Johdon tulee sitoutua tietoturvallisuuden tavoitteisiin, huolehtia yleisen tietoturvallisuustietoisuuden levittämisestä, tukea turvallisuutta edistävää koulutustoimintaa, taata tietoturvallisuuteen tarvittavat resurssit sekä huolehtia siitä, että tietoturvallisuudessa noudatettavat käytännöt tulevat osaksi organisaation liiketoimintaa. Luonnollisesti johto on myös vastuussa tietoturvallisuuteen liittyvän lainsäädännön ja sopimusten mukaisten velvoitteiden selvittämisestä.[236]

Yksi tietoturvan toteuttamisen haasteista on resurssien vähyys. Tietoturvatyöhön ei ole esimerkiksi riittävästi henkilöstöä eikä rahaa. Pienissä organisaatioissa tilanne saattaa olla haastavaa, jos tietoturvatyötä tehdään muun työn ohessa. Johdon tulisi tällöin lisätä tietoturvan toteuttamiseen liittyviä resursseja. Isoissa organisaatioissa vastaavaa ongelmaa ei usein ole, vaan niistä löytyy yleensä tietoturvavastaava tai –päällikkö. Suurien organisaatioiden haasteena saattaa toisaalta olla se, että tietoturvasta vastaavan henkilön on saatava koko henkilöstö toimimaan tietoturvan kannalta oikein.[237]

Erityisesti osaamisen kehittäminen on tärkeää. Tietoturvallisuuden ylläpito ja toteuttaminen edellyttävät yleistä tietoturvallisuustietoisuutta ja tietojenkäsittelyn erityisosaamista. Erityisesti asiantuntijatehtävissä toimivien henkilöiden koulutuksesta on huolehdittava. Lisäksi koko henkilöstön tietoturvatietoisuuden toteuttaminen on hoidettava asianmukaisesti.[238]

---

[234] Hakala et al. 2006, s. 90.
[235] Hakala et al. 2006, s. 105.
[236] Hakala et al. 2006, s. 114–115.
[237] Andreasson & Koivisto 2013, s. 45.
[238] Hakala et al. 2006, s. 115.

9. Nykypäivän ja tulevaisuuden haasteita

Tietoturvallisuus alueena on valtavan laaja ja tietoturvaan liittyy monenlaisia riskejä. Seuraavaksi tarkastellaan aiheeseen liittyviä haasteita.

Tietoturvariskejä voivat aiheuttaa esimerkiksi haittaohjelmat, varmuuskopiointi (tai sen puuttuminen), sähköposti, salasanat (tai salasana), tietojen salaus (puuttuminen tai vanha teknologia) sekä roskaposti. Suojaamaton sähköpostiliikenne on ollut myös yksi informaatiohallinnon tavallisimpia ongelmia.[239] Viestintäviraston kyberturvallisuuskeskus on puolestaan omassa vuosikatsauksessaan esittänyt Suomen näkökulmasta erilaisia tietoturvallisuuteen liittyviä riskejä, joita ovat olleet muun muassa tietojenkalastelun yleistyminen, vakoiluhaittaohjelmahavaintojen lisääntyminen ja palvelunestohyökkäyksien voiman kasvu. Toisaalta samalla kansallinen kyky havaita tietoturvaongelmia on parantanut.[240] Euroopan verkkorikostorjuntakeskus on arvioinut tulevaisuuden haasteita hieman eri näkökulmasta. Rikollinen toiminta on muuttunut nopeasti ja siinä käytetään hyväksi tekniikan kehitystä ja lainsäädännön aukkoja. Tulevaisuuden uhkakuvia ovat muun muassa se, että verkkorikollisten ja rikosten määrä kasvaa, rikokset tehdään yhä taidokkaammin ja rikokset kohdistuvat pilvipalveluihin.[241] Uhkakuvia on valtava määrä, mutta perusteellisesti tehdyllä tietoturvatyöllä niihin on mahdollista varautua.

Tietoturvan erityiskysymyksiä liittyy pilvipalveluihin, tietoliikennehyökkäyksiin sekä esimerkiksi kohdistettuihin haittaohjelmahyökkäyksiin, etätyöhön, ulkoistamiseen ja identiteettivarkauksiin. Nämä tapaukset esitellään lyhyesti seuraavaksi.

9.1 Pilvipalvelut

Pilvipalvelu tarkoittaa yleisesti internetissä hankittua tietokapasiteettia. Palveluun saattaa sisältyä erilaisia sovelluksia tai muita palvelusuoritteita. Pilvipalvelu ei kuitenkaan ole pelkkä tekninen ratkaisu vaan enemmänkin ajattelutapa. Pilvipalveluja käyttämällä voidaan luopua fyysisistä konesaleista, vaikka toisaalta jossakinhan pilvipalvelimetkin sijaitsevat.[242] Pilvipalvelua kutsutaan joskus myös etäresurssipalveluksi.[243]

---

[239] Ks. esim. Tietosuojavaltuutetun kannanotto 1.7.2010 dnro 1475/41/2009.
[240] Katsaus kyberturvallisuuteen vuonna 2014.
[241] Euroopan verkkorikostorjuntakeskus toiminut vuoden, Bryssel 10. helmikuuta 2014.
[242] Heino 2010, s. 32.
[243] Ks. lisää pilvipalveluiden turvallisuudesta esim. Pilvipalveluiden turvallisuus – Mitä organisaatioiden tulisi huomioida pilvipalveluja, Viestintäviraston julkaisu. Kyseisessä julkaisussa on myös lyhyt kuvaus pilvipalveluihin liittyvistä sopimusasioista ja lainsäädännöstä. (Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf, viitattu 16.11.2015).

Pilvipalvelu on Yhdysvaltojen julkishallinnon standardointilaitoksen (National Institute of Standards, NIST) mukaan toimintamalli, joka mahdollistaa pääsyn vapaasti muokattaviin ja skaalautuviin tietotekniikkaresursseihin, jotka voidaan ottaa käyttöön tai poistaa käytöstä helposti ja nopeasti. NIST:n mukaan pilvipalveluiden ominaispiirteitä ovat nopea joustavuus (rapid elasticity), resurssien yhteiskäyttö (recource pooling), itsepalvelullisuus (on–demand self service), päätelaiteriippumattomuus (broad network access) ja tarkka resurssien käytön valvonta (measured service).[244]

Pilvipalveluissa tieto tai palvelu saattaa sijaita eri valtiossa kuin missä loppukäyttäjä oleilee. Sama infrastruktuuri voi olla myös jaettuja eri käyttäjien kanssa, mikä johtaa tiedon erotteluun liittyviin ongelmiin. Erilaiset vahingot pilvipalvelussa saattavat aiheuttaa katkoksia palvelun toimintaan niin, ettei välttämättä tiedetä, missä ongelma sijaitsee ja kuinka ongelma voidaan kohdentaa sekä tietysti selvittää. Tiedon tuhoaminen pilvipalvelussa voi olla myös hankalaa. Käyttäjä ei voi olla varma, onko tieto todellakin poistettu järjestelmästä vai onko tieto vain tehty käyttäjälle luoksepääsemättömäksi (inaccessible). Pilvipalveluun liittyvän järjestelmän tarkastaminen tai tutkiminen voi myös olla haastavampaa kuin perinteisen järjestelmän. Virtuaaliteknologian käyttäminen voi aiheuttaa sen, että on hankalaa selvittää, mihin kaikkialle tieto on tallennettu.[245]

Euroopan komissio on julkaissut syyskuussa 2012 strategian pilvipalveluiden käytöstä Euroopan unionissa. Komission tiedonannon mukaan keskeisiä ongelmia pilvipalvelujen käytössä ovat digitaalisten sisämarkkinoiden hajanaisuus, sopimusongelmat sekä standardiviidakko. Myös tietosuoja–asiat nähdään pilvipalveluissa haasteena.[246]

Virtualisaatio on yksi keskeisimmistä asioista toteutettaessa pilvipalveluita (palveluita tai tallennustilaa). Virtualisaation sekä samalla myös pilvipalveluiden ongelmat liittyvät turvallisuuteen, suurten konesalien hallintaan sekä yhteentoimivuuteen.[247] Turvallisuuden kannalta ensisijaisesti tutkittavia ja selvitettäviä asioita ovat käyttäjien luottamuksen aikaansaaminen[248], tietojen ja toimintojen havainnointi siten, ettei käyttäjien tietosuojaa tai turvallisuutta menetetä, sekä konesalien elinkaaren hallinta. Keskeisimmät, oikeudellisestikin merkittävät, teknologia–alueet pilvipalveluiden osalta voidaan jakaa seuraaviin: resurssien kohdentaminen, sopimus– ja palveluneuvottelut, työnkulun organisointi, hajautettu varastointi

[244] NIST Cloud Computing Program, NIST:n www–sivut: Cloud Computing (Saatavilla: http://www.nist.gov/itl/cloud/, viitattu 16.11.2015).
[245] Robinson et al. 2010, s . 17–18.
[246] COM(2012) 529 final, s. 6.
[247] Robinson et al. 2010, s . 41.
[248] Luottamus voidaan perinteisesti saavuttaa erityisesti hyvällä tietoturvalla.

sekä käyttäjien identiteettien hallinta.[249] Haastetta on siinä, kuinka pilvipalveluiden luottamus säilytetään hajautetussa pilvipalvelujärjestelmässä. Lisäksi erityisesti yhteentoimivuus saattaa aiheuttaa ongelmia pilvipalveluissa, kun sama käyttäjä haluaa käyttää pilvipalveluita eri alustoilla ja laitteilla. Pilvipalveluissa tulee taata yhteentoimivuus, tietojen ja palveluiden saatavuus sekä tietojen siirrettävyys.[250]

Pilvipalvelut ovat kansainvälinen asia. Käyttäjä ja konesali, jonne tarvittava tieto on tallennettu, eivät välttämättä sijaitse saman valtion alueella. Siksi pilvipalveluiden toimivuuden osalta voidaan nähdä tarvittavan kansainvälistä harmonisointia (yhteinen säädöskehys), vastuullisuutta (esim. palvelutasosopimukset, SLA, Service Level Agreement), läpinäkyvyyttä (esim. parhaat toimintatavat) ja ainakin Eurooppa–tasoista teknologian hallintaa (esim. tietoturvaloukkauksien havainnointi ja tiedottaminen).[251]

Lainsäädännön kehittämisen kannalta on huomioitava, että Euroopan unionin sääntely ei saisi rajoittaa liikaa eurooppalaisten palveluntarjoajien asemaa. Unionin sääntelyllä EU voi asettaa eurooppalaiset pilvipalveluntarjoajat huonompaan asemaan kuin unionin ulkopuoliset palveluntarjoajat ovat. Toisaalta säännöt eivät saisi olla liian joustaviakaan, jottei palveluiden käyttäjille aiheutuisi haittaa. Lainsäädännössä tulisi tunnistaa palveluntarjoajien sekä loppukäyttäjien oikeudet ja velvoitteet. Erityisesti turvallisuus ja henkilötietojen suoja on taattava.[252] Tarvitaan yhteinen kansainvälinen säädöskehys, jota tarkentaa unionin sääntely ja kansallinen lainsäädäntö. Lisäksi tarvitaan myös soft law –tyyppistä sääntelyä. Tähän sisältyy muun muassa ohjesäännöt, hyvät käytännöt, parhaat toimintatavat ja itsesääntely. Näiden ohella myös sopimusoikeudellista kehystä tulee tarkentaa. Standardoidut ehdot ja mallisopimukset ovat tästä hyvä esimerkki.[253]

9.2 Tietoliikennehyökkäykset, kohdistetut hyökkäykset

Verkon turvallisuus liittyy erityisesti internetiin ja sen kautta tuleviin hyökkäyksiin ja roskapostiin. Tietohallinnossa puolestaan sisäisen verkon tietoturvallisuus (eheys, käytettävyys ja luottamuksellisuus) on tärkeää. Suurin osa tietoturvarikkomuksista tapahtuu kuitenkin yhä organisaation sisällä.[254]

[249] Robinson et al. 2010, s .43.
[250] Robinson et al. 2010, s. 52.
[251] Robinson et al. 2010, s. xxi.
[252] Robinson et al. 2010, s. 53.
[253] Robinson et al. 2010, s. 62–63.
[254] Hakala et al. 2006, s. 187.

Kohdistetulla hyökkäyksellä (Advanced Persistent Threat, APT) tarkoitetaan sellaista tietoturvaloukkausta, joka kohdistuu tiettyyn organisaatioon tai rajattuun joukkoon henkilöitä. Hyökkäyksissä käytetään räätälöityjä haittaohjelmia, joita ei välttämättä havaita virustorjuntaohjelmistoilla. Niiden levittäminen tapahtuu vain rajatulle joukolle ihmisiä tai organisaatioita. Tällöin hyökkäys ei paljastu myöskään kovin helposti. Hyökkäyksen tekijä voi suunnitella tekoa pitkään ja tekijä valitsee kohteensa huolellisesti sekä hankkii kohteesta ennakolta tietoja. Kohdistetun hyökkäyksen tavallisia tekotapoja ovat sähköpostiviestien liitetiedostot, kiinnostavat verkkosivustot tai USB–muistitikut. Haittaohjelma voidaan myös piilottaa liitetiedostoon tai sähköpostissa voi olla linkki haitallista sisältöä tarjoavalle verkkosivulle, jolloin sitä ei voida kovin helposti havaita. Tartunnan jälkeen ohjelmat pyrkivät usein levittäytymään lähiverkon kautta myös muihin organisaation tietokoneisiin. Ne voivat myös ottaa yhteyksiä organisaation verkosta ulospäin ja välittää tietokoneista löydettyjä tietoja hyökkääjälle tai ladata itseensä lisäominaisuuksia sisältäviä päivityksiä. Haittaohjelmalla voi olla myös suojautumismekanismeja. Se voi esimerkiksi tuhota jälkiä, jotka voivat johtaa tekijän jäljille. Usein kohdistetun haittaohjelmien taustalta löytyy järjestäytyneitä ryhmiä, myös valtiollisia toimijoita. Jos haittaohjelmat saavat toimia verkossa pitkään, jopa useita vuosia, ne voivat levitä laajalle ja varastaa organisaatiosta paljon tietoja.[255]

Haittaohjelmatartuntoja voidaan löytää tarkkailemalla verkkoliikennettä ja niitä voidaan torjua esimerkiksi sähköpostiviestien sisällön perusteella seulomalla liikennettä.[256] Myös käyttäjien kouluttaminen ja ohjeistaminen on tärkeää. Mikäli sähköpostiin saapuu epäilyttävä viesti, liitetiedostoa ei ole pakko avata. Suomessa tietoyhteiskuntakaaressa säännellään organisaatioiden oikeudesta (ja velvollisuudesta) käsitellä verkon välitystietoja tietoturvaperusteella. Tietoyhteiskuntakaaren mukaan teleyrityksillä on myös velvollisuus huolehtia verkko– ja viestintäpalveluidensa tietoturvasta ja toimivuudesta. Kansallisesti merkittävä toimija asian osalta on myös Viestintäviraston Kyberturvallisuuskeskus, jossa sen CERT –toiminto kerää tietoa, tiedottaa ja selvittää erilaisia tietoverkoissa tapahtuvia tietoturvauhkia ja –loukkauksia.

[255] Kohdistetut haittaohjelmahyökkäykset, Viestintäviraston www–sivut (Saatavilla: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2013/11/ttn201311011336.html, viitattu 14.11.2015).

[256] Lue lisää keinoista suojautua hyökkäykseltä: Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti, Viestintäviraston julkaisu (Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf, viitattu 14.11.2015).

9.3 Etätyö

Erityisesti etätyöhön tai kotityöhön saattaa liittyä tietoturvariskejä. Etäkäyttö on työpisteen ulkopuolelta etäyhteyden avulla tapahtuvaa tietoteknisten palvelujen käyttöä. Etätyössä on enemmän tietoturvallisuusuhkia kuin toimistossa tehtävässä työssä ja näiden riskien hallinta on vaikeampaa. VAHTI on antanut etätyöstä omat tietoturvallisuusohjeensa. Etätyön suunnittelussa tulee huomioida se, ettei kaikkea työtä voi tehdä etätyönä. Esimerkiksi kokonaan kiellettyä on käsitellä salaisia tai erittäin salaisia tietoja etätyönä. [257] Yleisesti erittäin salaisiksi turvaluokiteltuja asiakirjoja ei saa myöskään lähettää sähköpostilla.[258]

Töiden jaottelu voidaan tehdä esimerkiksi työssä käytettävän tietoaineiston luottamuksellisuuden perusteella. Etätyötä on pystyttävä tekemään myös tarkkojen annettujen ohjeistusten mukaisesti. Henkilöiden valmiudet etätyöhön on arvioitava lisäksi tapauskohtaisesti. Esimerkiksi työntekijän valmiudet tietotekniikan hallintaan tulee arvioida. Organisaatioiden tulee myös järjestää käyttäjille riittävä etätyön käyttäjätuki. Etätyönkin osalta on tehtävä riskianalyysia eli työhön kohdistuvia riskejä, niiden todennäköisyyksiä ja hallintakeinoja tulee analysoida ennen kuin etätyöhön voidaan ryhtyä.[259]

9.4 Ulkoistaminen

Kaikessa ulkoistamisessa tulee miettiä myös sen vaikutuksia tietoturvaan. Tieto– ja tietoturvariskit eivät ulkoistamistilanteissa ole enää täysin omassa hallinnassa. Palvelujen ulkoistamisessa tietoriskit ovat yksi keskeisin riskienhallinnan osa–alue. Ulkoistamistilanteessa ulkopuoliselle toimijalle saatetaan antaa käyttöön salassa pidettäviä tietoja, joiden tietoturvaa ohjaa joskus myös erityislainsäädäntö.[260] Lisäksi tietoturva–asiat olisi hyvä ottaa huomioon ulkoistamissopimuksissa.

Ulkoistamisen tavoitteena on usein toiminnan tehokkuuden, laadun ja joustavuuden parantaminen sekä kokonaiskustannusten alentaminen. Ulkoistamiseen voidaan turvautua myös tilanteessa, jossa omasta organisaatiosta ei löydy resursseja tai osaamista tietojärjestelmien, palvelinten ja tietoliikenneverkon ylläpitotehtäviä varten. [261]

[257] Valtionhallinnon etätyön tietoturvallisuusohje, Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003.
[258] Andreasson & Koivisto 2013, s. 136.
[259] Valtionhallinnon etätyön tietoturvallisuusohje, Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003.
[260] Andreasson & Koivisto 2013, s. 77.
[261] Andreasson & Koivisto 2013, s. 78.

VAHTI on julkaissut myös Valtion ICT–hankintojen tietoturvaohjeen 2011. Ohjeen mukaisesti ICT–palveluita hankittaessa organisaatioiden tulee kiinnittää huomiota tietoturvallisuuteen, varautumiseen, palvelun laatuun ja kustannustehokkuuteen.[262]

9.5 Identiteettivarkaudet

Sisäasianministeriön identiteettiohjelman työryhmän loppuraportissa käsitellään kattavasti henkilöllisyyden luomiseen liittyviä menetelmätapoja. Raportissa käsitellään muun muassa identiteettivarkauksia, henkilöllisyyden suojaamista sähköisessä ympäristössä, valtion tehtävää henkilöllisyyksien luojana sekä vastuuviranomaisena, tunnistamista ja siinä käytettäviä tunnistamisasiakirjoja sekä biometriikan käyttömahdollisuuksia tunnistamisasiakirjojen osalta.[263]

Toisena henkilönä esiintyminen rajoittaa merkittävästi henkilön tiedollista itsemääräämisoikeutta. Identiteettivarkauden uhrilla Suomessa on aikaisemmin ollut heikko rikosoikeudellinen suoja.[264] Suomessa tietoverkkorikosdirektiivin implementoinnin yhteydessä syksyllä 2015 kriminalisoitiin identiteettivarkaus. [265] Rikoslain 38 luvun 9 b §:n mukaan joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon. Identiteettivarkaus on asianomistajarikos. Nykyisestä rikosoikeudellisesta sääntelystä huolimatta toimijoiden tulisi kuitenkin erityisesti panostaa sähköisten järjestelmien ja – asiointipalveluiden tietoturvaan ja tietosuojaan.[266] Hallituksen esitöissäkin jo epäiltiin, että identiteettivarkaudet eivät todennäköisesti ole kovin harvinaisia.[267] Kyseisistä rikoksista ei ainakaan tarvitse tehdä helppoja. Moni tapaus voitaneen estää hyvällä tietoturvalla.

10. Tietoturvakoulutus

Tietoturvallisuus on monitahoinen, usean eri alan asiantuntijoita ja erityisosaamista vaativa alue. Koulutuksen osalta haasteena on tietoturvan ymmärtäminen laajassa mielessä. Vieläkin usein käy niin, että tietoturva nähdään pelkkänä teknisenä asiana.

---

[262] Andreasson & Koivisto 2013, s. 77 & Valtion ICT–hankintojen tietoturvaohje, VAHTI 3/2011.
[263] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma) Työryhmän loppuraportti. Sisäasiainministeriön julkaisuja 32/2010, s. 6.
[264] Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma) Työryhmän loppuraportti. Sisäasiainministeriön julkaisuja 32/2010, s. 8.
[265] Ks. tarkemmin HE 232/2014 vp.
[266] Andreasson & Koivisto 2013, s. 16–17.
[267] HE 232/2014 vp, s. 5.

Osaamisen kehittämisen tärkeyttä ei voi korostaa liikaa. Tietoturvallisuuden ylläpito ja toteuttaminen edellyttävät yleistä tietoturvallisuustietoisuutta ja tietojenkäsittelyn erityisosaamista. Erityisesti asiantuntijatehtävissä toimivien henkilöiden koulutuksesta ja myös koko henkilöstön tietoturvatietoisuudesta on huolehdittava.[268] Toimivassa tietoturvallisessa organisaatiossa tietoturvakoulutus on sisällytettynä organisaation koko henkilökunnan peruskoulutukseen.

Tietoturvan toteuttamisessa suurin haaste on teknisen tietoturvan, hallinnollisen tietoturvan, tietosuojakäytäntöjen sekä henkilöstön osaamisen noston samanaikaisessa hallinnassa. Riskien hallitsemiseksi johdon on sitouduttava tietoturvan kehittämiseen ja toteuttamiseen sekä budjetoitava ja resursoitava tietoturva asianmukaisella tavalla. [269]

Tietoturvariskien torjuminen vaatii usein huomion kiinnittämistä ennen kaikkea itse tietojen ja tietojärjestelmien käyttäjiin. Kunnollisen tietoturvakulttuurin luominen voi viedä useita vuosia. Henkilöstön kouluttamiseen on syytä panostaa entistä enemmän koko ajan muuttuvassa maailmassa. Työntekijöille kannattaa tarjota esimerkiksi tietoturvan ja –suojan verkkokursseja. Työntekijöille on syytä muistuttaa tietoturva–asioista mieluummin pieninä palasina kuin satasivuisina määräyksinä. Erilaiset tietoturvaseminaaritkin voivat olla hyvä tapa levittää tietoturvatietoisuutta. Lisäksi voidaan myös laatia perustason tietoturvaopas, josta tietoturvan perusteet saa tietoonsa helposti omaksuttavassa muodossa.[270]

Tietoturvakoulutuksia järjestäviä organisaatioita on runsaasti. Lähes kaikki tietoturvaorganisaatiot antavat ajantasaista tietoturvaan liittyvää koulutusta ja jakavat ilmaiseksikin tietoturvatietoutta.

Ylipistot ja korkeakoulutkin ovat vähitellen heränneet tietoturvan merkitykseen ja tarjoavat tietoturvaan liittyviä kursseja opiskelijoilleen. Positiivista kehitystä tietoturva–alan koulutustarjonnassa on selkeästi nähtävillä. Tämän lisäksi tietoturvaan liittyvään akateemiseen jatkotutkimukseen ollaan panostamassa resursseja ja varoja. Suurimmassa osassa Suomen yliopistoja ja korkeakouluja on tarjolla kursseja tietoturvasta. Useissa yksittäisissä kursseissa on myös tunnistettu kurssin osa–alueeksi tietoturva. Osassa opinahjoista on tarjolla myös kokonaisia räätälöityjä tietoturvallisuuden koulutusohjelmia.

[268] Hakala et al. 2006, s. 115.
[269] Andreasson & Koivisto 2013, s. 237.
[270] Andreasson & Koivisto 2013, s. 237–238.

11. Lopuksi

Tietoturva on tunnistettu yhdeksi tärkeäksi tekijäksi verkkoyhteiskunnassa. Tietoturva ei ole pelkkä tekninen tai fyysinen asia. Jo pitkään sekä kansainvälisesti että kansallisesti ollaan tehty erilaisia tietoturvasopimuksia, –sitoumuksia ja strategioita pitkän aikavälin tavoitteiden saavuttamiseksi. Lainsäädännössäkin on tapahtunut pieniä parannuksia. Tietoyhteiskuntakaari saatiin vihdoin vuoden 2015 alussa voimaan. Tuleva tietosuoja–asetus ollaan todennäköisesti saamassa maaliin vuoden 2016 aikana, ehkä jo alkuvuodesta. Tärkeä kysymys vielä on, tarvitaanko yleistä tietoturvasääntelyä. Asia olisi syytä pohtia perusteellisesti.

Tietoturva lisää luottamusta verkkoyhteiskunnassa. Käytännön tietoturvatyö on usein riskien tunnistamista ja niihin varautumista. Teknologinen kehitys tuo mukanaan uusia riskejä. Näihin riskeihin voidaan varautua perusteellisella ja hyvällä tietoturvatyöllä.

Koulutus on ehkäpä parhaimpia keinoja lisätä tietoturvatietoisuutta. Yliopistot ja korkeakoulut sekä yksityiset toimijat tarjoavatkin jo runsaasti erilaista tietoturvaan liittyvää koulutusta. Vielä ei kuitenkaan voida sanoa, että tietoturva olisi jokaiseen organisaatioon sisäänrakennettu toimintatapa ja kulttuuri. Toimivan tietoturvakulttuurin luominen voi kestää vuosia, mutta matka on aloitettu jo monissa organisaatioissa ja kouluista kasvaa uusi tietoturvan paremmin tunnistava sukupolvi.

DIGITALISAATION EDISTÄMINEN TIETOTURVALAINSÄÄDÄNNÖN AVULLA

Asko Lehtonen

Oikeustieteen professori (emeritus), Rikosoikeuden dosentti, Oikeustieteen tohtori, varatuomari, asko.lehtonen@professori.fi

Digitalisoituminen on megatrendi, jonka nähdään parantavan palveluiden laatua ja tuottavuutta. Populaarissa keskustelussa digitalisaatio on yläkäsite, jonka alle ryhmitellään monia käsitteitä, kuten teollinen internet, pilvipalvelut, massadata sekä erilaiset älykkäät verkot. Akateemisessa keskustelussa digitalisaation on ns. yleiskäyttöinen teknologia (general purpose technology), joka rinnastuu muutosvoimassaan höyry– tai sähkövoimaan. [1]

Yksi selkeä digitalisoitumisen este suomalaisille pk–yrityksille on huoli tietoturvasta. Toisaalta hyvin hoidettu tietoturva nähdään myös mahdollisuutena yrityksille profiloitua ja saada kilpailuetua kilpailijoihinsa nähden. [2]

Koetut riskit ovat todellisia. Huoltovarmuuskriittisille yrityksille ja toimijoille suunnattu tietoturvaloukkausten havainnointi– ja varoitusjärjestelmään eli ns. HAVARO–järjestelmä havaitsi vuoden 2015 tammi–elokuussa yhteensä yli 1800 niin sanottua punaista havaintoa.[3] Vuonna 2014 Suomessa tehtiin yli 200 000 haittaohjelmahavaintoa viestintäverkoissa.[4] Aalto–yliopiston tutkimuksessa vuonna 2013 jopa 60 prosentilla tutkimuksen piiriin kuuluneista teollisuuden automaatiojärjestelmistä sisälsi julkisesti tiedossa olevan haavoittuvuuden.[5] Internetin leviäminen, pilvipalveluiden lisääntyminen ja langattomien laitteiden eksponentiaalinen kasvu ovat luoneet alustan uudenlaisen kyberrikollisuuden kasvulle, jonka

[1] Ks. esim. Helpman, Elhanan. 1998. *General Purpose Technologies and Economic Growth*. The MIT Press tai Liikenne– *ja viesintäministeriön julkaisu* ”Digitalisaatio keskisuurissa yrityksissä”. 14/2014 s. 4. Saatavilla URL: http://www.lvm.fi/c/document_library/get_file?folderId=3082174&name=DLFE–24299.pdf&title=Julkaisuja%2014–2014.

[2] Keskuskauppakamari teki laajan digitalisaatiokiertueen pk–yrityksille ympäri Suomen vuonna 2013 ja kiertueesta tehdyssä yhteenvedossa todetaan yhtenä kolmesta uhasta: ”Tietoturvan kehitys ajautuu kriisiin ja saa käyttäjät (yritykset ja kuluttajat) siirtymään pois palveluista (Internetin balkanisoituminen ja rajat ylittävän toiminnan vaikeutuminen).” Ks. Liikenne– *ja viesintäministeriön julkaisu* ”Digitalisaatio keskisuurissa yrityksissä”. 14/2014 s. 23. Myös Accenturen haastattelututkimuksen mukaan tietoturva nähdään esteenä digitalisaation laajemmalle soveltamiselle. Ks. *Accenture*. ”Growing the Digital Business: Accenture Mobility Research 2015. Saatavilla URL: http://www.slideshare.net/fullscreen/AccentureDigital/mobility–research–2015–digital–overview–final/3.

[3] Ks. Viestintäviraston Toimalakatsaus 3/2015. S. 25. Julkaistu 16.09.2015. Saatavilla URL: https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2015/toimialakatsaus32015.html.

[4] Ks. Viestintäviraston Toimalakatsaus 2/2015. S. 25. Julkaistu 31.08.2015. Saatavilla URL: https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2015/toimialakatsaus22015.html.

[5] Ks. *Aalto–yliopisto.* ”Tuhannet automaatiolaitteet Suomessa haavoittuvia kyberhyökkäyksille”. 20.03.2013. Saatavilla URL: www.aalto.fi/fi/current/news/view/2013–03–20/.

motiivit ovat usein taloudellisia. McAfeen mukaan verkkorikollisuuden tuotto on 750 miljardia euroa vuodessa.[6] Euroopan komission mukaan noin 148 000 on kyberrikollisuuden kohteena joka päivä.

Vakavina tietoturvauhkina voidaan pitää muun muassa seuraavia:

a) Palvelunestohyökkäykset.
b) Tietomurrot, joissa hankitaan yritysten ja henkilöiden "arkoja" tietoja, mm. ohjelmien haavoittuvuuksia hyväksikäyttämällä.
c) Kohdistetut haittaohjelmat, kuten Ulkoasiainministeriön vakoilutapaus.
d) Kiristyshaittaohjelmat (Ransomware), jossa ohjelmalla aiheutetaan tietokoneelle palvelunestotila, minkä purkamiseksi kiristetään käyttäjältä rahaa.
e) Salasanojen yms. "kalastaminen" (phishing).

Suomessa tietoturva on säännelty alakohtaisissa erillissäännöksissä sekä tietosuojalainsäädännön yleistason sääntelyllä. Suomessa ei ole yleistä tietoturvalakia. Tietoturva on tässäkin yhteydessä syytä erottaa tietosuojasta.[7]

Tietosuojan (data protection) tarkoitus on turvata asianomaiset perusoikeudet (kuten henkilötietojen suoja, yksityisyys ja viestinnän luottamuksellisuus) tilanteessa, jossa henkiötietoja käsitellään, ja toisaalta mahdollistaa tiedon sujuva käyttö. Tietosuojalainsäädäntö koskee henkilötietoja eli tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevia tietoja.[8]

Suomessa EU:n tietosuojadirektiivi (EC 95/46) on toimeenpantu kotimaiseen lainsäädäntöön henkilötietolaissa (22.4.1999/523), joka on yleislaki. Sähköisen viestinnän palveluille on erillissäännöksiä EU:n sähköisen viestinnän tietosuojadirektiivissä (2002/58/EY), joka on toimeenpantu kotimaiseen lainsäädäntöön tietoyhteiskuntakaaressa (7.11.2014/917). EU:ssa on valmisteilla uusi tietosuoja–asetus, joka on edennyt ohi trilogivaiheen.

Keskeisiä digitalisaatioon liittyviä kysymyksiä tietosuojan kannalta ovat esim. seuraavat:

---

[6] Ks. Euroopan Kommissio. "EU Cybersecurity plan to protect open internet and online freedom and opportunity". 7.2.2013. Saatavilla URL: http://europa.eu/rapid/press–release_IP–13–94_en.htm.

[7] Tässä yhteydessä ei määritellä tarkemmin käsitettä "tieto" tai sen suhdetta lähellä oleviin käsitteisiin. Todettakoon kuitenkin, että käsitteitä data, informaatio ja tieto käytetään arkikielessä usein synonyymeinä, mutta niillä on epistemologinen merkitysero ja hierarkia, joita ei tilanpuutteen vuoksi tarkemmin avata. Lyhyesti sanottuna data tarkoittaa käsittelemättömiä havaintoja faktoja, kuten yksittäisiä lämpötila–arvoja. Informaatio on dataa kontekstissa; esim. viikon keskilämpötilat ovat sääennustamisen kontekstissa merkityksellistä vertailutietoa. Tieto taas on käytettävissä olevaa informaatiota; esim. vertailtuaan keskilämpötiloja historialliseen aineistoon, viranomainen voi antaa kuivuusvaroituksen tms.

[8] Henkilötietolain (1999/523) 3 §:n mukaan henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

- Millä edellytyksillä henkilötietoja voidaan prosessoida?
- Missä tilanteissa tarvitaan suostumus?
- Voidaanko tietoa siirtää Euroopan unionin alueen ulkopuolelle?
- Mihin toimenpiteisiin pitää ryhtyä, jos suostumus peruutetaan?

Tietoturva (information security) koskee puolestaan IT–järjestelmien ja viestintäverkkojen luottamuksellisuutta, eheyttä (integriteettiä) ja käytettävyyttä. Lainsäädännössämme on ensimmäisen kerran määritelty tietoturvan käsite yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetussa laissa (22.4.1999/565). Tämä lain 3 §:ään oli otettu erilaisia käsitemääritelmiä. Tässä yhteydessä oli säädetty, että puheena olevassa laissa tarkoitettiin teletoiminnan tietoturvalla teleyrityksen hallinnollisin ja teknisin toimenpitein varmistamaa televiestinnässä välitetyn tiedon 1) luottamuksellisuutta, 2) eheyttä ja 3) käytettävyyttä. Saman lain 6 §:ssä säädettiin teleyrityksen velvollisuuksista, joiden mukaan teleyrityksen tulee mm. huolehtia harjoittamansa teletoiminnan tietoturvasta.

Henkilötietolain (22.4.1999/523) 7 luvun otsikossa käytetään myös käsitettä ‘tietoturvallisuus’. Laissa ei ole tarkemmin luonnehdittu tietoturvan käsitettä. Lain esitöissä mainitaan tietoturvallisuuden elementtinä ‘tiedon eheys’, jolla tarkoitettiin tiedon muodon säilyttämistä tahattomalta tai lainvastaiselta muuttamiselta eli tiedon säilymistä talletettua tietoa vastaavassa muodossa.

Nykyisin tietoturva on määritelty tietoyhteiskuntakaaren 3 §:n 28) kohdassa. Tämän säännöksen mukaan *tietoturvalla* tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Tietoturvallisuudesta valtionhallinnossa annetun asetuksen (1.7.2010/681) 3 §:n määrittelyn mukaan *tietoturvallisuudella* tarkoitetaan puolestaan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä. Määrittelyjen erot eivät ole merkittäviä. Jälkimmäisessä määrittelyssä on suppeampi eli valtionhallinnon näkökulma. Tietoyhteiskuntakaaren luonnehdinta on yleisluonteisempi ja sen perusteena on ollut sähköisen viestinnän tietosuojalain 2 §:n määritelmäsäännös.

Suomessa ei ole yleistä tietoturvalakia, vaan tietoturva on osa alakohtaisia erillissäännöksiä. Näistä tärkeimpiä ovat mm. seuraavat.

Viestintäverkoissa tarjottavien sähköisen viestinnän tietoturvasta säädetään tietoyhteiskuntakaaressa (7.11.2014/917).[9] Viranomaisia koskevia tietoturvaan liittyviä säännöksiä löytyy mm. laista viranomaisten toiminnan julkisuudesta (21.5.1999/621), laista sähköisestä asioinnista viranomaistoiminnassa (24.1.2003/13) sekä laista kansainvälisistä tietoturvallisuusvelvoitteista (24.6.2004/588).[10] Laki yksityisyyden suojasta työelämässä (13.8.2004/759) puolestaan asettaa välillisiä vaatimuksia tietoturvasta työelämässä.[11] Myös mm. finanssisektorille kohdistuu lukuisia erillissäännöksiä, jotka koskettavat myös tietoturvaa ja joista mainittakoon luottotietolaki (11.5.2007/527), sekä laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (7.8.2009/617). Lisäksi kansainvälisesti toimivien finanssilaitosten täytyy ottaa toiminnassaan huomioon mm. Yhdysvaltain Sarbanes–Oxley lain vaatimukset.[12] Myös esim. terveydenhuollon toimijoihin kohdistuu lukuisia erillissäännöksiä, mm. henkilötietolaissa (22.4.1999/523)[13] ja laissa potilaan asemasta ja oikeuksista (17.8.1992/785).

EU:ssa on valmisteilla verkko– ja tietoturvadirektiivi, jossa mm. tietoturvaloukkausten pakollinen ilmoitusvelvollisuus laajennettaisiin koskemaan kriittistä infrastruktuuria ja tiettyjä internet–toimijoita kuten pilvipalveluita. Tällä hetkellä pakollinen ilmoitusvelvollisuus koskee vain sähköisen viestinnän palveluita.[14]

Keskeisiä digitalisaatioon liittyviä tietoturvakysymyksiä ovat esimerkiksi:

- Onko järjestelmien tietoturvan varmistaminen huomioitu jo suunnitteluvaiheessa?
- Miten on varauduttu toimimaan poikkeustilanteissa?
- Pitääkö tietoturvaloukkauksista, kuten hakkeroinnista, ilmoittaa viranomaisille?
- Mitä vaatimuksia asetetaan standardien, sertifikaattien ja salauksen suhteen?
- Minkälaisia sanktioita merkittävistä tietoturvaloukkauksista voi seurata?

Tietoturva ja tietosuoja liittyvät toisiinsa. Ilman toimivaa tietoturvaa on mahdotonta varmistaa henkilötietojen asianmukaista suojaa. Vastaava periaate pätee myös tietoturvan ja

[9] Ks. mm. tietoyhteiskuntakaaren 17 luku sähköisen viestin ja välitystietojen käsittelystä ja 33 luku, jossa säädetään esim. toimenpiteistä tietoturvan toteuttamiseksi. Lisäksi huomattavan markkinavoiman omaavalla teleyritykselle voidaan asettaa velvoitteita ottaen huomioon myös tietosuojaan ja tietoturvaan liittyvät vaatimukset (ks. 53 § ja 80 §). Tietoyhteiskuntakaaren sähköisen viestinnän luottamuksellisuutta koskevan säännökset ovat korvanneet sähköisen viestinnän tietosuojalain (516/2004).

[10] Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 §:n 2 momentin mukaan lakia sovelletaan myös elinkeinonharjoittajaan, joka on sopimusosapuolena turvallisuusluokitellussa sopimuksessa, osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.

[11] Tietoturvaa välillisesti koskevista säännöksistä esimerkkeinä mainittakoon 5 §:n säännökset terveydentilaa koskevien tietojen käsittelystä ja 13 §:n säännökset henkilö– ja soveltuvuusarviointitesteistä.

[12] Sama vaatimus koskee myös Yhdysvaltain pörssissä listattuja suomalaisyrityksiä. Ks. esim. Kinnunen, Niina (2015). *Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen*. Vaasa: Vaasan yliopisto.

[13] Ks. esim. henkilötietolain 11 §:n kohta 4), 27 §:n kohta 2) ja 28 §:n 3 mom.

[14] Ks. tietoyhteiskuntakaaren (7.11.2014/917) 243, 274 ja 275 §.

monien muiden oikeushyvien välisessä suhteessa: esim. omaisuuden suoja (esim. liikesalaisuudet) ja yksityisyyden suoja edellyttävät alati tietoteknistyvässä yhteiskunnassa myös toimivaa tietoturvaa.

Monissa puheenvuoroissa on nähty ongelmallisena, jos merkitykseltään koko ajan kasvava tietoturvallisuus jätetään yksittäisten erillissäännösten ja henkilötietolain yleistasoisen sääntelyn varaan. Myöstään rikosoikeudellisten sanktioiden varaan ei hyvää tietoturvaa voida järjestää. Erillisäännökset koskevat vain tietyn toimialan tiettyjä toimijoita. Yleinen tietoturvalainsäädäntö koskisi kaikkia yhteiskunnan toimijoita alasta riippumatta.[15]

Yleiseen tietoturvalain soveltamisalaan on ehdotettu kuuluvan ainakin nimenomainen liittymä ihmis– ja perusoikeuksiin sekä sen tulisi kattaa kaikki digitaalisessa toimintaympäristössä tapahtuvat toimet tietojärjestelmien suunnittelusta niiden käyttöön. Yleislain tulisi olla teknologianeutraali sekä sen tulisi sisältää säännökset sanktioista ja viranomaisten pakkokeinoista tietyissä tilanteissa.

Tietoturvaan liittyvällä lainsäädännöllä voidaan edistää digitalisaatiota monella eri tavalla. Luottamus on keskeinen elementti, jolla voidaan parantaa niin digitalisaation tarjontaa kuin kysyntääkin.

Tarjontapuolella on kysymys ennen kaikkea yritysten ja muiden toimintaansa digitalisoivien toimijoiden luottamuksesta. Digitalisaatio edellyttää usein tietojen jakamista arvoketjussa muiden toimijoiden kanssa avoimien rajapintojen yli, pilvipalveluiden käyttöä sekä kolmansien osapuolien tietovarantojen hyödyntämistä omassa toiminnassa.

Digitalisaatio voi periaatteessa tarkoittaa vain yrityksen omien manuaalisten prosessien korvaamista digitaalisilla, mutta tämä on ns. matalan tason digitalisaatiota. Suurimmat hyödyt digitalisaatiosta liittyvät korkeamman tason digitalisaatioon, joka taas edellyttää tiedon kulkemista yritysten välillä sekä prosessien ja toimitusketjujen muokkaamista digitalisaation mahdollisuuksia hyödyntäväksi.[16]

---

[15] Mm. professori Ahti Saarenpää sekä eduskunnan oikeusasiamies ovat puoltaneet yleisen tietoturvalain säätämistä. Ks. esim. Saarenpää, Ahti. (2015). Oikeusinformatiikka. Teoksessa: *Oikeus tänään. osa 1*. s. 175–177. Toim. Marja–Leena Niemi. 3. painos. Lapin yliopiston oikeustieteellisiä julkaisuja. C63. Rovaniemi: Lapin yliopisto tai Saarenpää, Ahti et al. *Sähköinen viestintä, tietoturvallisuus ja perusoikeudet*. s. 2. 2004. Rovaniemi: Lapin yliopisto.

[16] Digitalisaation viisi tasoa: 1. yksittäiset manuaaliset prosessit on korvattu digitaalisilla, mutta järjestelmät eivät keskustele keskenään; 2. tieto kulkee sähköisesti organisaation sisällä; 3. tieto kulkee sähköisesti organisaatioiden välillä; 4. organisaation prosessit on muokattu hyödyntämään digitalisaatiota; 5. koko liiketoimintaekosysteemi tai toimitusketju on muokattu IT:tä ja digitalisaation mahdollisuuksia hyödyntäväksi. Ks. Venkatraman. IT enabled business transformation: From automation to business scope redefinition. MIT Sloan Management Review.

Myös kysyntäpuolella digitalisaation välttämätön edellytys on luottamus, sillä yksittäiset kansalaiset tai yritykset eivät kokeile uusia järjestelmiä tai hyödynnä digitalisaation mahdollisuuksia, elleivät he usko, että heidän tietonsa on turvassa tai että he voivat luottaa esim. pilvessä olevan järjestelmän saatavuuteen kaikkina hetkinä.

Luottamuksen keskeistä merkitystä voidaan havainnollistaa analogialla ja lyhyellä tarinalla keskitetystä sähköntuotannosta. Thomas Edison tunnetaan erityisesti hehkulampun keksijänä, mutta vähintään yhtä tärkeä hänen keksinnöistään oli sähkögeneraattori. Alussa yritykset hankkivat omat generaattorinsa valaisemaan tehdastaan tai kotiaan.

Omista generaattoreista alettiin luopua 1800–luvun lopulla kytkeytymällä keskitettyihin sähkölaitoksiin. Näin toimii myös moderni sähköntuotanto. Aluksi keskitettyjen sähkön tuottajien turvallisuuteen tai luotettavuuteen ei uskottu. Luottamus rakentui vuosikymmenien kuluessa – ja omalla tavallaan se ansaitaan yhä uudelleen jokaisen myrskyn ja sähkökatkon jälkeen. Moderni yhteiskunta on täysin riippuvainen keskitetystä sähköntuotannosta.

Digitalisoituva maailma käy läpi samaa evoluutiota. Tähän asti jokainen on ostanut tietokoneen ja asentanut siihen valitsemansa ohjelmistot, ja vastaavasti yritykset ovat ostaneet ja operoineet omia palvelinkeskuksiaan. Internetin varaan rakentuvassa pilvipalveluiden ja suurten tietovarantojen maailmassa ei tarvita muuta kuin pääsy Internetin keskitettyihin tietovarantoihin millä tahansa päätelaitteella, kuten kannettavalla tietokoneella tai puhelimella.

Aloitteleville yrityksille muutos mahdollistaa merkittävästi alemmat alkuinvestoinnit ja juoksevat kustannukset. Yksittäisille kansalaisille se mahdollistaa laajan palveluvalikoiman ja resurssit alhaisemmalla hinnalla.

Useimmat meistä hyödyntävät päivittäin esim. pilvipalveluita: maksamme laskuja nettipankissa, etsimme tietoa hakukoneilla ja lähetämme sähköpostia älypuhelimella. Modernin yhteiskuntamme alkaa olla yhtä riippuvainen keskitetystä tietojenkäsittelystä kuin keskitetystä sähkön tuotannosta. Ilman luottamusta nettipankin tietovarantojen turvallisuuteen, hakukoneen salausprotokollaan tai kirjeenvaihtomme yksityisyyden suojaan, merkittävä osa kuluttajista jättäisi palvelut käyttämättä.

Tämän tyyppiset riskit ovat vasta kasvussa. Älyliikenne tulee perustumaan tulevaisuudessa osittain automatisoituun liikenteeseen, joka puolestaan ei ole mahdollista taikka turvallista ilman, että kulkuneuvo pystyy olemaan luotettavasti koko ajan yhteydessä ympäristöönsä ja muihin autoihin ja ilman kyydissä olevien ihmisten uskomusta siihen, että terroristi ei pääse murtautumaan autoon tai ympäröiviin ohjausjärjestelmiin.

Toinen esimerkki on terveydenhuollon puolelle ennustettu hoivarobottien määrän merkittävä kasvu. Näiden robottien odotetaan voivan mm. suoriutua tietyistä mekaanisista

tehtävistä, kuten vanhuksen nostamisesta, ja niitä ohjataan monesti etäisyyden päästä esim. keskitetystä ohjauskeskuksesta. Keskeiset riskit tässä visiossa liittyvät juuri tietoturvaan ja mm. kysymykseen siitä, miten hoivarobotin tulisi toimia siinä tapauksessa, että yhteys katkeaa.

Keskeinen kysymys tulee olemaan myös seuraava: Pitäisikö tietoturvaloukkauksista ilmoittaminen olla pakollista? Yritysten ja yksityisten kansalaisten kohdalla tietoturvaloukkauksista ei välttämättä haluta kertoa ainakaan julkisuudessa, ellei ole pakko. Kyseessä on peliteoreettinen paradoksi: jos yksi yritys kertoo, että sen tietojärjestelmiin on murtauduttu tilanteessa, jossa muut eivät kerro, seurauksena voi olla asiakaskato vähemmän avoimiin yrityksiin. Jos taas kaikki yritykset olisivat avoimia, jolloin myös tieto haavoittuvuuksien paikkaamisesta leviäisi nopeammin, kaikkien tietoturva paranisi.

Yksi tapa lisätä tietoturvaa on salaustekniikoiden käytön leviäminen laajemmin kuluttajakäyttöön. Toisaalta luottamus myös salaustekniikkaan on vähentynyt erityisesti tietovuotaja Edward Snowdenin paljastusten johdosta. Snowdenin paljastuksista opimme, että NSA on tahallaan heikentänyt Internetin tietoturvaprotokollia ja tekniikoita, kuten https–salausta, SSL–salausta tai laajalti käytettyä tunnelointi–ratkaisua (Virtual Private Network eli VPN).[17] Tämän seurauksena Internetin keskeiset protokollat pitää mahdollisesti päivittää tai suunnitella kokonaan uudella tavalla varmistaen riippumattomuus valtioiden vakoilukoneistoista. Monet tietoturva–asiantuntijat puhuvat avoimen lähdekoodin ratkaisujen puolesta.

Myös rikosoikeudellisella sääntelyllä on yleispreventiivinen merkitys tietoturvarikosten ehkäisemisessä. Verkkoyhteiskunnan näkökulmasta olemme nyttemmin saaneet kansainvälisen tason johtoa Euroopan neuvoston yleissopimuksesta tietoverkkorikollisuudesta (ETS No. 185) ja tietoverkkorikosdirektiivistä (2013/40/EU).

Henkilötietolain mukaan henkilötietoja on suojattava a) asiattomalta pääsyltä tietoihin ja b) tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä, tapahtuipa se vahingossa tai laittomasti, taikka c) muulta laittomalta käsittelyltä. Suojaamisvelvoitteen laiminlyöntiä ei ole kriminalisoitu rikoslain 38 luvun 9 §:ssä tarkoitettuna henkilörekisteririkoksena. Sen sijaan henkilötietojen suojaamisvelvoitteen rikkomisesta

[17] Ks. esim. *The New York Times*. ”N.S.A. Able to Foil Basic Safeguards of Privacy on Web”. 5. syyskuuta 2013. URL: http://www.nytimes.com/2013/09/06/us/nsa–foils–much–internet–encryption.html; *The New York Times.* ”Unlocking Private Communcations”. 5. syyskuuta 2013. URL: http://www.nytimes.com/interactive/2013/09/05/us/unlocking–private–communications.html?ref=us; sekä **Error! Main Document Only.**Greenwald, Glenn (2014). No Place to Hide. Edward Snowden and the USA. Surveillance State. New York: Metropolitan Books.

voidaan henkilötietolain 48 §:n nojalla tuomita sakkoon, jos menettelyllä on vaarannettu rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan.

Tiedon luottamuksellisuutta (kuten tiedon säilymistä vain siihen oikeutettujen käytettävissä) loukkaavista rikoksista on säädetty rikoslaissa. Esimerkkinä mainittakoot rikossäännökset, jotka koskevat yritysvakoilua (RL 30:4), salassapitorikosta (RL 38:1), viestintäsalaisuuden loukkausta (RL 38:3), tietomurtoa (RL 38:8) ja henkilörekisteririkosta (RL 38:9).

Tiedon ja tietojärjestelmän luottamuksellisuutta tai eheyttä loukkaavia rikoksia, joiden törkeistä tekomuodoista tuomitaan normaalirangaistuksena vankeutta, ovat muun muassa seuraavat:

1) Vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a), jossa rikoksessa tekijän tarkoituksena on aiheuttaa haittaa tai vahinkoa tietojenkäsittelylle taikka tieto– tai viestintäjärjestelmän toiminnalle tai turvallisuudelle tunnusmerkistössä kuvatuilla tekotavoilla,
2) tietovarkaus anastusrikoksena (RL 28:1 tai 4) tai yritysvakoiluna (RL 30:4),
3) kavallus ns. elektronisena kavalluksena eli tilisaldoista ilmenevien varojen anastamista siirtämällä varoja toisen tililtä omalle tilille, mikä suoritetaan esim. muuttamalla pankin tieto– järjestelmän tilitietoja oikeudettomasti, (RL 28:4),
4) luvaton käyttö tietokoneen ja ohjelman tai tietojärjestelmän luvattomana käyttönä, kuten Bot–verko perustaminen haittaohjelmien avulla luvattomasti toisten tietokoneisiin ja niiden käyttö palvelunestohyökkäyksiin (RL 28:7),
5) väärennys; esim. automaattiseen tietojenkäsittelyyn soveltuvan tallenteen sisältämän informaation tai datan väärentäminen tai väärän tallenteen valmistaminen taikka niiden käyttäminen harhauttavana todisteena (RL 33:1),
6) tuhotyö (RL 34:1), mikä voidaan suorittaa mm. siten, että a) omaisuutta vahingoittamalla tai tuhoamalla taikka b) tuotanto–, jakelu– tai tietojärjestelmän toimintaan oikeudettomasti puuttumalla aiheutetaan vakavan vaaran energiahuollolle, yleiselle terveydenhuollolle, maan– puolustukselle, oikeudenhoidolle tai muulle näihin rinnastettavalle yhteiskunnan tärkeälle toiminnolle,
7) datavahingontekona (RL 35:3a–c), mikä voidaan suorittaa hävittämällä, turmelemalla, kätkemällä, vahingoittamalla, muuttamalla, saattamalla käyttökelvottomaksi tai salaamalla oikeudettomasti tietovälineelle tallennettu tieto tai muu tallennus taikka tietojärjestelmässä oleva data,

8) petos ns. tietojenkäsittelypetoksena (RL 36:1), minkä tekotapoja ovat hyötymis– tai vahin– goittamistarkoituksessa suoritettu a) väärien tietojen syöttäminen tietojenkäsittelylaitteeseen tai b) muu puuttuminen koneelliseen tietojenkäsittelyyn, minkä seurauksena tietojenkäsittelyn lopputulosta vääristetään ja aiheutetaan toiselle taloudellista vahinkoa,
9) maksuvälinepetos (RL 37:8),
10) rekisterimerkintärikos (RL 16:7), minkä tekotapoja ovat a) väärän tiedon antaminen rekisteriä pitävälle viranomaiselle oikeudellisesti merkityksellisen virheen aiheuttamiseksi viranomaisen pitämään mm. atk–pohjaiseen yleiseen rekisteriin tai b) sanotulla tavalla aiheutetun virheen hyväksi käyttäminen hyödyn hankkimiseksi itselle tai toiselle taikka toisen vahingoittamiseksi,
11) tietoliikenteen häirintä (38:5),
12) tietojärjestelmän häirintä (RL 38:7a) ja
13) identiteettivarkaus (RL 38:9a), josta on tosin säädetty rangaistukseksi vain sakkoa

OIKEUDELLINEN LAATU EDUNVALVONTAPALVELUISSA

Guardianship Services, Self–determination and Legal Quality

Johanna Tornberg

OTT Lapin yliopisto, jotorn@gmail.com

Abstract: *The research examined procedural legislation, material legislation and legislation concerning information and information processing as a whole in the area of guardianship. Two situations in particular were chosen for analysis: One is where a person files a petition on his/her own initiative requesting appointment of a guardian, the other where donee applies to a registry office to confirm a continuing powers of attorney. Information processes in these situations were seen as starting from the first contact with the guardianship authority and ending when the information related to the case is expunged from the authority's archives and registers. The decision making that a case entails was viewed as part of the information process as a whole.*

The two focal processes were studied from a perspective of individual rights. In looking at the information systems and especially the Register of Guardianship Affairs, one observes a tension between the need to protect and the obligation to safeguard the rights and interest of the ward. According to Guardianship Services Act section 64 the register is maintained in order to supervise the activities of guardians and to safeguard the rights of third parties. The register should not be seen merely as a technical tool but also as an information system that influences ward's life and rights. Information processing is also a legal process, one whose overall success depends crucially on the quality of information and of its processing.

The skeleton for the legal quality is procedural legislation, which includes regulation concerning information processing. The relevant material legislation puts flesh on these bones. However, the legislation in place is not enough in a state governed by the rule of law. The interpretation of that legislation also affects legal quality. In the area of guardianship, those interpreting the law should consider every single case in terms of the interests and rights of the ward. It can be said that legal quality is best safeguarded when interpretation proceeds in accordance with human and fundamental rights.

1. Johdanto

Elämälle on ominaista jatkuva muutos. Kaikella on elinkaarensa, loppunsa ja alkunsa. Tämä kuvaa myös tiedon tietä, kun se kulkee läpi julkisen hallinnon. Tieto ja informaatio ovat osa suurempaa kokonaisuutta, vaikuttaen toimintatapojen valintaan ja asioiden etenemiseen. Ne kuuluvat tehokkuuteen, työprosesseihin ja tietojärjestelmiin. Jotta voisi nähdä yksityiskohtien merkityksen, on ensin hahmotettava kokonaisuus. Ja se vaatii työtä. Henkilötietojen kohdalla kuvaan tulee lisäksi mukaan ihminen. Edunvalvontapalveluissa

ihminen on tässä suhteessa alastomimmillaan. Kun maistraatissa selvitetään edunvalvonnan tarvetta, ihmisestä piirretään hyvin kokonaisvaltainen kuva: ihmissuhteet, taloudellinen tilanne, terveydentila. Kaikilla näillä on merkitystä ja kaikista alueista tietoa kerätään. Niihin perustuu edunvalvojan määräämistä koskeva päätös, jolloin erityistä merkitystä on annettava sille, esiintyykö henkilö informaation kautta oikeassa valossa.[1] Koko prosessin yhdistävänä tekijänä on informaatio: oikeudellinen informaatio ja oikeuden ulkopuolisia seikkoja koskeva informaatio. Näiden avulla tapahtuvat oikeudellisen ongelman tunnistaminen ja sen ratkaiseminen.[2]

Artikkeli perustuu vuonna 2012 julkaistuun väitöskirjaani, jossa tutkin edunvalvonnan oikeudellista laatua.[3] Tutkimuksen aiheena oli edunvalvojan määrääminen oikeudellisena informaatioprosessina ja tuon informaatioprosessin oikeudellinen laatu. Edunvalvojan määräämisasioista tarkastelun alla oli tilanne, jossa henkilö itse hakee edunvalvojaa eli tilanteet, joissa maistraatti on toimivaltainen määräämään edunvalvojan. Vertailukohtana käytettiin edunvalvontavaltuutuksen vahvistamista. Informaatioprosessi ymmärrettiin tutkimuksessa tiedon elinkaaren mittaiseksi eli sen ei katsottu päättyvän oikeudelliseen ratkaisuun itse asiassa.[4] Edunvalvojan määrääminen kartoitettiin vaihe vaiheelta. Vaiheita tarkasteltiin päämiehen oikeuksien näkökulmasta, sillä edunvalvontaoikeuden keskeisin periaate on ihmisen kunnioittaminen. Väitöskirja on toinen edunvalvontaoikeudesta tehty väitöskirja Suomessa ja ainoa, jossa asiaa tarkastellaan päämiehen edun ja oikeuksien kautta.[5] Tässä artikkelissa keskitytään informaatioprosessien merkitykseen ja tutkimuksen keskeisiin tuloksiin – päivittäen niitä tarpeellisilta osin tähän päivään.

2. Informaatioprosessien merkityksen kasvaminen

Tietotekniikka tuli alun perin apuvälineeksi ja toimistoautomaation mahdollistajaksi. 1960–luvulta lähtien yhteiskunta alkoi kehittyä jälkiteollisesta yhteiskunnasta informaatioyhteiskunnaksi.[6] Informaatioyhteiskuntaa kohti mentäessä informaatiosta kasvoi merkittävä taloudellinen resurssi. Se piti saada entistä tehokkaammin käyttöön myös

[1] Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 316
[2] Pöysti: Tehokkuus, informaatio ja eurooppalainen oikeusalue (1999) s. 135
[3] Tornberg: Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu (2012)
[4] Näin esimerkiksi teoksessa Lenk – Traunmüller: Broadening the Concept of Electronic Government (2007) p. 14. Heidän mukaansa päätös on informaatioprosessin ja informaation käsittelyn lopullinen tulos.
[5] Ensimmäinen suomalainen edunvalvontaoikeuden väitöskirja oli *Matti Kuulialan* vuonna 2011 julkaistu väitöskirja Edunvalvontaan esitetyn kuuleminen alioikeudessa. Väitöskirja edustaa perinteistä lainopillista tutkimusta.
[6] Saarenpää: Oikeusinformatiikka (1999) s. 20–21 ja Webster: Theories of the Information Society (2014) s. 2

organisaation sisällä. [7] Tätä vauhditti teknologian kehitys, jonka kautta harvojen käytössä olleet tietokonejärjestelmät alkoivat jokapäiväistyä parin seuraavan vuosikymmenen aikana. Nykyisin työ tehdään digitaalisessa toimintaympäristössä, jossa se on yhä enemmän pääte– ja verkkosidonnaista ja niistä riippuvaista.[8]

Yhteiskunnan suhde informaatioon on muuttunut siten, että informaatiosta on edellä mainitun kehityksen tuloksena tullut nykyaikaisen talouden ja työelämän perusta.[9] Se on rakentunut hyödykkeiksi, tuotteiksi ja palveluiksi muodostaen informaatiomarkkinat.[10] Informaation merkityksen ja määrän kasvaessa nousi esille tarve miettiä informaation varastointia ja käsittelytapoja uudelleen. Julkishallinnossa tämä on merkinnyt tarvetta arvioida vanhat luokitukset ja käsitteet uudelleen.[11] Se on lisäksi merkinnyt uudenlaista roolia tiedon– ja palveluntuottajana, johon liittyy hallinnossa asioivan ihmisen roolissa tapahtunut muutos julkishallintoa palvelevasta hallintoalamaisesta aktiiviseksi toimijaksi, jolla on omat oikeutensa. Tämä kehitys linkittyy ihmis– ja perusoikeuksien vahvistumiseen. Hallinnon toiminnan tulee olla oikeusjärjestyksen mukaista ja sen tulee toimia vuorovaikutuksessa kansalaisten kanssa.[12] Yksi esimerkki muutoksesta on neuvonta. Hallinnon asiakkaan ollessa hallintoalamaisen asemassa neuvo ei ollut neuvo vaan määräys.[13] Nykyisin neuvonta on yksi viranomaisen velvollisuuksista. Suomessa neuvonnasta on oma säännöksensä hallintolaissa. Neuvontavelvollisuus sisältää käsiteltävää asiaa koskevan neuvonnan lisäksi yleisen velvollisuuden vastata asiointia koskeviin kysymyksiin ja tiedusteluihin. Se tarkoittaa velvollisuutta vastata menettelyllistä, tosiasiallista ja oikeudellista neuvontaa koskeviin kysymyksiin.[14]

Yhteiskunnan kehitys suhteessa informaatioon jatkui seuraavassa vaiheessaan verkkoyhteiskunnan syntymisellä. Verkkoyhteiskunnan ominaispiirteitä ovat tietoliikenteen ja tietoverkkojen entistä monimuotoisempi käyttäminen sekä eri toimintojen yhä suurempi

[7] Webster: Theories of Information Society (2014) s. 10. *Webster* kritisoi tätä näkökulmaa, sillä se aiheutti esimerkiksi tutkimuksessa puutteita sen havainnoinnissa, millä kaikilla tavoilla ja miksi informaatiosta tuli ja on tullut yhä keskeisempää nykypäivänä. Jopa niin keskeistä, että se vie meitä kohti uudentyyppistä yhteiskuntaa.
[8] Gelati: Agent–based Systems in Public Administrations (2004) s. 97–98 ja Saarenpää: Oikeusinformatiikka (2012) s. 437–438. Ensimmäisiä tietojärjestelmiä informaation nopeampaan käytettävyyteen olivat file–based systems, which were developed in response to the needs of industry for more efficient data access. Ks. Connolly – Begg: Database systems (2005) s. 8
[9] Webster: Theories of Information Society (2014) s. 15–18, *Webster* muistuttaa siitä, ettei pelkkä kvantitatiivinen tutkimus esimerkiksi informaatiotyöläisten määrästä kerro koko totuutta tapahtuneesta muutoksesta vaan tulisi katsoa myös sitä, millaisia informaatiotyöläisiä yhteiskunnassa on, millainen on heidän paikkansa hierarkioissa ja kuinka paljon heillä on valtaa.
[10] Pöysti: Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet (2002) s. 3
[11] Bing: Information Law? (2004) s. 26 alaviite 37
[12] Mäenpää: Hallintolaki ja hyvän hallinnon takeet (2008) s. 59
[13] Kuusikko: Neuvonta hallinnossa (2000) s. 22–23
[14] Oka 22.9.2005 430/1/04 ja eoa 28.5.2008 dnro 1311/2/08

riippuvuus näistä ja niiden toimivuudesta. Verkkoyhteiskunnassa informaation hyökyminen eri lähteistä on nopeutunut entistä kehittyneempien teknologisten ratkaisujen parantaessa tiedon kulkua ja saantia.[15] Pääte– ja verkkosidonnaisuus koskettaa myös yksittäisen ihmisen elämää. Tämän on todennut korkein hallinto–oikeus ratkaisuissaan KHO:2006:18 ja KHO 12.4.2006 T 876/2006. Tapauksissa oli kysymys hankittavista, tietokoneen käytön mahdollistavista apuohjelmista. Korkein hallinto–oikeus velvoitti kummassakin tapauksessa kaupungin hankkimaan nämä apuohjelmat hakijoille, sillä se katsoi, että palvelujen siirtyessä yhä laajemmin ensisijaisesti verkon välityksellä käytettäviksi, ei kysymys ollut harrastustoiminnan tukemisesta vaan sosiaalisen toimintakyvyn tukemisesta sekä itsenäisen elämäntilanteen hallinnan ja päivittäisistä toiminnoista selviämisen edistämisestä. Kysymys on ihmisen mahdollisuudesta osallistua yhteiskuntaan yhtä lailla kuin tietoverkkojen tarjoamasta mahdollisuudesta koulutukseen ja itsensä kehittämiseen.[16] Ratkaisujen jälkeen 13.12.2006 hyväksytty YK:n yleissopimus koskien vammaisten henkilöiden oikeuksia tukee tulkintaa. Yleissopimuksen 9 artiklan mukaan:

> ”To enable persons with disabilities to live independently and participate fully in all aspects of life, States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications, *including information and communications technologies and systems*, and to other facilities and services open or provided to the public, both in urban and in rural areas.”[17]

Mielenkiintoista onkin, ettei eduskunnan oikeusasiamies reilu vuosi korkeimman hallinto–oikeuden ratkaisujen julkaisemisen jälkeen antamassaan ratkaisussa dnro 4042/4/06 millään tavalla pohtinut sitä, mikä vaikutus päämiehen elämään oli edunvalvojan päätöksellä kieltää tietokoneen ja laajakaistan hankkiminen.

EU on ottanut julkaisuissaan kantaa sen puolesta, että tietojärjestelmien tulee olla esteettömästi kaikkien käytettävissä, koska kysymys on yksilön oikeuksista verkkoyhteiskunnassa. Jokaisella tulee olla mahdollisuus omien asioidensa hoitamiseen sekä

[15] Saarenpää: Verkkoyhteiskunnan oikeutta – johdatusta aiheeseen (2000) s. 4 ja Saarenpää: Yksityisyyden suoja tietämättömyyden uteliaisuusympäristössä (2004) s. 13
[16] Ks. Kleve – de Mulder: Privacy Concerns in the Information Society (2008) p. 81–82, jossa kirjoittajat puhuvat tietämysyhteiskunnasta (Knowlegde Society), jossa internetillä on tärkeä rooli myös koulutuksessa ja yksilön kehittämisessä.
[17] Kursivointi tässä. Suomessa sopimus tuli voimaan vasta 10.6.2016.

osallistumiseen.[18] Verkkoyhteiskunnan kehittymisen myötä yhä enemmän palveluita on siirretty verkkoon ja julkisessa hallinnossa on siirrytty sisäisestä tietojenkäsittelystä ja tiedonhallinnan järjestämisestä kohti sähköistä hallintoa.[19] Sähköinen hallinto voidaan määritellä tieto– ja viestintäteknologian välityksellä tarjottavaksi julkiseksi palveluksi, johon kuuluvat viranomaisen omat sisäiset tietojärjestelmät ja tietojenkäsittely.[20] Laajemmasta näkökulmasta sähköisessä hallinnossa on kysymys informaatioteknologian käyttämisestä julkisen hallinnon toimintojen tukemiseen.[21] Sähköinen hallinto on kuitenkin korostanut sitä, että jokaiselle tulee turvata mahdollisuus sähköisesti tarjottavien palveluiden käyttämiseen. Asiakaspalvelupisteiden harventaminen on tarkoittanut henkilökohtaisesti saatavilla olevien palveluiden siirtymistä yhä kauemmas, jolloin sähköisesti tapahtuva yhteydenotto voi puhelimen lisäksi olla ainoa vaihtoehto. Asianhallinta– ja tietojärjestelmien tuottavuutta parantavia vaikutuksia ovat kuitenkin Suomessa heikentäneet käyttöönotossa tapahtuneet viivästykset ja suunnittelun sisältämät puutteet.[22]

Suomen nykyinen taloudellinen tilanne on luonut paineen julkisen hallinnon rakennemuutokselle, jossa melko iso osa paineista asettuu tieto– ja viestintäteknologian ja digitalisaation varaan. Yhdeksi tuottavuuden kasvattamisen välineeksi on kaavailtu kansallista palveluväylä– eli KaPa–hanketta. Kansallisella palveluväylällä tarkoitetaan tiedonvälityspalvelua, joka perustuu Virossa käytössä olevaan tekniseen X Road–ratkaisuun. Kansallinen palveluväylä on osa kansallista palveluarkkitehtuuria. Valtiontalouden tarkastusvirasto on korostanut, että aiemmista virheistä tulisi ottaa oppia ja kiinnittää huomiota hankkeen ohjaukseen ja johtamiseen. IT–hankkeet eivät muutoinkaan saisi jäädä omaksi saarekkeekseen vaan ne pitäisi tuoda osaksi toiminnan kehittämistä kokonaisuudessaan.[23] Sähköisen hallinnon kehittäminen ei saisi kutistua vain julkisen hallinnon taloudellisen

[18] Ks. European Disability Strategy 2010–2020: A Renewed Commitment to a Barrier–Free Europe COM(2010) 636, eAccessibility COM(2005) 425, Ageing well in the Information Society: An i2010 Initiative Action Plan on Information and Communication Technologies and Ageing COM(2007) 332 and A Digital Agenda for Europe COM(2010) 245

[19] Saarenpää: Oikeusinformatiikka (2012) p. 435–437

[20] eEurope 2005: An information society for all COM(2002) 263 p. 10, i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All COM(2006) 173 p. 5 and Magnusson–Sjöberg – Nordbeck – Nordén – Westman: Rättsinformatik (2011) p. 268

[21] Lenk – Traunmüller: Broadening the Concept of Electronic Government (2007) s. 9

[22] Valtiontalouden tarkastusviraston tarkastuskertomus 9/2011 p.9

[23] Valtiontalouden tarkastusviraston vuosikertomus eduskunnalle toiminnastaan valtiopäiville 2015 s. 40–44. Valtiontalouden tarkastusvirasto on kuitenkin todennut tarkastaessaan valtion ICT–sopimuksien yhteentoimivuutta tarkastaessaan, ettei kokonaisarkkitehtuuria ole otettu osaksi julkishallinnon organisaatioiden johtamista sekä strategia– ja suunnittelutyötä sillä tavoin kuin se on tarkoitettu. Ks. Tuloksellisuuskertomus: Yhteentoimivuus valtion ICT–sopimuksissa, Valtiontalouden tarkastusviraston tarkastuskertomuksia 7/2015 s. 9

tehokkuuden tukemiseen vaan tavoitteena tulisi olla parempien toimintatapojen tai laadukkaampien palvelujen tuottaminen.[24]

Teknologian tulee olla olemassa ihmistä varten, auttaa ihmistä.[25] Tehokkuusvaatimukset sekä yksilön oikeuksien turvaaminen ja toteutuminen pitää pystyä yhdistämään. Oikeudelliset kysymykset on tunnistettava mahdollisimman aikaisessa vaiheessa.[26] Tätä korostaa myös EU–tuomioistuimen päätös koskien sähköisen viestinnän palvelun tarjoajia. Teletunnistetietojen tallennusvelvollisuus ja erityisesti objektiivisten kriteerien puuttuminen niiden säilytysajoissa rikkovat niin yksityisyyden kuin henkilötietojenkin suojaa.[27] Tehokkuusvaatimusten ja yksilön oikeuksien turvaaminen onnistuvat vain riittävän informaation avulla eli on tunnettava asiaa koskevat työprosessit, menettelyä koskeva lainsäädäntö ja itse asiaa koskeva aineellinen säännöstö – sekä koko prosessin läpi kulkeva informaatio. Se nivoo koko prosessin yhteen. Teknologiakeskeisen ajattelun sijaan keskitytään informaatioon ja informaatiovirtoihin.[28]

3. Edunvalvojan määrääminen maistraatissa informaatioprosessina

Edunvalvojan määrääminen valikoitui tarkastelun kohteeksi, koska siinä kerätään hyvin kokonaisvaltaisesti tietoa ihmisestä ja hänen elämäntilanteestaan. On selvitettävä hänen kykyään ymmärtää ja hoitaa omia taloudellisia asioitaan. Lisäksi on selvitettävä taloudellista tilannetta ja muita mahdollisia asioiden hoitotapoja eli esimerkiksi sitä, onko ihmisellä läheisiä, jotka voisivat olla apuna eikä edunvalvoja välttämättä olisi tarpeen.

Tutkimuksessa yhdistettiinkin oikeudellinen menettely ja informaatioprosessit yhdeksi kokonaisuudeksi. Prosessit kartoitettiin tutkimuksessa kokonaisuutena neuvonnasta eli ensimmäisestä yhteydenotosta siihen, kun asiaa koskeva informaatio lopulta hävitetään. Tämä oli tarpeen siitä syystä, että kysymys oli informaatioprosessin kuvaamisesta, ei esimerkiksi asiakkaasta alkavasta ja asiakkaaseen päättyvästä prosessista, jossa keskityttäisiin käytännössä vain päätöksenteon kuvaamiseen.[29] Informaatiota koskeva elinkaariajattelu eroaakin hallintomenettelyyn liitetystä elinkaariajattelusta juuri tässä suhteessa. Yksilöä koskevan informaation virta on paljon pidempi kuin hallintoprosessi vireillepanosta tai sitä edeltävistä

[24] Ks. Codagno – Osimo: Future Technology Needs for Future eGovernment Services: Services Platform Report (2008) s. 8
[25] Codagno – Osimo: Future Technology Needs for Future eGovernment Services: Services Platform Report (2008) s. 6–7
[26] Schartum: Den menneskelige faktor i elektronisk forvaltning (2010) s. 116
[27] Joined cases C–293/12 and C–594/12. *Saarenpään* jaottelussa asia sijoittuu alueelliseen yksityisyyteen, joka tarkoittaa fyysisen kotirauhan suojaamisen lisäksi myös oikeutta olla erilaisen valvonnan ulottumattomissa. Ks. Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 312
[28] Mayer–Schönberger – Lazer: From Electronic Government to Information Government (2007) p. 6
[29] Ks. prosessikuvauksen rajaamisesta JHS 152 s. 5

toimista päätöksen tiedoksiantoon.[30] Oikeudellisen menettelyn kulun lisäksi on tärkeää hahmottaa, miten informaatio liikkuu tuon prosessin sisällä, millaisia riskejä siihen liittyy ja millä tavoin asian käsittelyn kohteena olevan henkilön oikeudet otetaan huomioon ja pitäisi ottaa huomioon. Informaatioprosessi on erottamaton osa oikeudellista menettelyä.

Prosessiajattelu on ollut erityisesti mukana tietojärjestelmien kehittämisessä ja laatua koskevassa keskustelussa. Prosessien kuvaaminen nähdään niissä prosessien johtamisen, hallinnan ja parantamisen välineenä erityisesti organisaation suunnittelu– ja kehittämistyössä. Sen avulla on helpompaa hallita kokonaisuutta ja havaitaan eri prosessien väliset yhteydet.[31] Prosessien ymmärtäminen ja niiden selkeys ovat tae palvelujen laadulle.[32]

Prosessiajattelun perusajatuksen mukaan organisaation suorituskyky syntyy prosesseissa. Jos suorituskykyyn halutaan muutoksia, se vaatii muutoksia organisaation toiminnassa.[33] Prosessien kuvaamisessa tulee pyrkiä mahdollisimman yksityiskohtaiseen lopputulokseen. Tämä vaatii koko organisaation ottamista mukaan. Tapa, jolla edellinen vaihe tehdään, vaikuttaa seuraavaan. Siirtymävaiheet on eriteltävä omiksi vaiheikseen.[34]

Suorituskyvyn ja tehokkuuden parantamisessa yhtenä osa–alueena on hallinnollisten taakkojen vähentäminen.[35] Informaatioprosesseja ja informaation käsittelyä koskevaa lainsäädäntöä on arvosteltu niiden aiheuttamasta hallinnollisesta taakasta. Hallinnollinen taakka on määritelty hallintotoiminnan kustannuksiksi, jotka johtuvat oikeudellisten velvoitteiden noudattamisesta.[36] Määritelmä on tehty yritysten näkökulmasta, mutta samalla tavalla lainsäädäntö voi aiheuttaa kustannuksia ja vaikuttaa toiminnan tehokkuuteen julkisessa

---

[30] Ks. hallintomenettelyyn liitetystä elinkaariajattelusta Kulla: Hallintomenettelyn perusteet (2004) s. 55 ja Siitari–Vanne: Hallintoasioiden elinkaaren hallinta hallintolainkäytön haasteena (2010) s. 288 ja 295–296

[31] JHS 152 Prosessien kuvaaminen p. 1, Beckford: Quality (2010) p. 109–111

[32] Gaster: Quality in Public Services (1995) p. 16

[33] Laamanen – Tinnilä: Prosessijohtamisen käsitteet (2002) p. 12–13. Ks. lisäksi COM(2010) 743 final: The European eGovernment Action Plan 2011–2015 Harnessing ICT to promote smart, sustainable & innovative government SEC(2010) 1539 final.

[34] Siirtymävaiheiden suunnittelun tärkeyden huomaa parhaiten lainsäädännössä tapahtuvien muutosten voimaantulon yhteydessä. Suomessa yksi tapa on hoitaa se erityisillä siirtymäsäännöksillä, jotka löytyvät lain lopusta. Esimerkkinä käytän maakaaren 9 luvun kirjaamisasiaan säädettyjä muutoksia muutoksenhausta. Muutos tuli voimaan vuoden 2014 alusta ja se säädettiin ilman siirtymäsäännöstä. Se, mihin hakijan tulee valituksensa toimittaa, ei riipu päätöksen tekoajankohdasta vaan siitä, milloin valitus toimitetaan. Tämä vaikutti erityisesti niihin päätöksiin, jotka tehtiin joulukuussa 2013. Valitusosoitukseen piti laittaa kaksi prosessiosoitetta: jos valituksen toimitti jo ennen määräpäivää vuoden 2013 puolella, se tuli toimittaa kirjaamisviranomaiselle eli asian ratkaisseelle maanmittauslaitokselle. Jos hakija taas valitti asiastaan vuoden 2014 puolella, valitus tuli toimittaa maaoikeutena toimivalle käräjäoikeudelle. Selkeä siirtymäsäännös olisi parantanut tilannetta hakijan kannalta.

[35] The European eGovernment Action Plan 2011–2015 s. 42–43

[36] Euroopan komission Better Regulation–ohjelmaan kuuluva sanasto osoitteessa http://ec.europa.eu/enterprise/policies/better–regulation/glossary/index_enhtm

hallinnossakin. Hallinnollisten taakkojen vähentämisessä arvioimisen ei tule lähteä pelkästään taloudellisista seurauksista. Informaation käsittelyä koskeva lainsäädäntö linkittyy monilta osin ihmis– ja perusoikeuksiin. Esimerkiksi henkilötietojen suoja on tunnustettu EU:n perusoikeuskirjassa omaksi perusoikeudekseen. Henkilötietojen suojaa koskevien säännösten hallinnollisen taakan arvioimisen on lähdettävä sen ihmis– ja perusoikeusluonteesta. Henkilötietojen suojaamisen tarkoituksena on suojata luonnollista henkilöä ja hänen oikeuksiaan, ei vain häntä koskevia tietoja.[37] Suorituskyky ja tehokkuus ovat vain osa laatua, eivät yhtä kuin laatu. Laatuun liittyy aina sisällöllinen elementti. Julkista palvelua ei voi pitää oikeudellisesti laadukkaana, vaikka se olisi tehokas ja nopea, jos se on saatu aikaan loukkaamalla yksilön oikeuksia.[38] Oikeudelliseen laatuun onkin kiinnitettävä erityistä huomiota tilanteissa, joissa palvelua hakeva henkilö on heikommassa asemassa esimerkiksi terveydentilansa suhteen. Edunvalvonta–asioissa tilanne on usein tämä. Se korostaa perustuslaissa julkiselle vallalle asetettua velvollisuutta huolehtia perusoikeuksien toteutumisesta, joka toimii julkisen hallinnon oikeudellisen laadun pohjana.

Julkista hallintoa kehitettäessä suunnitteluprosessin tärkein osa on oikeudellinen suunnittelu. Tämä tarkoittaa asiaa koskevan menettelyllisen ja aineellisen lainsäädännön läpikäymistä siten, että hahmotetaan oikeudelliset raamit, joissa toimintaa tulee kehittää. Kaikki menettelysäännösten määrittämät vaiheet on löydyttävä uudesta toimintamallista. Lisäksi on huomioitava se, että menettelyllä saadaan kaikki se informaatio, jota ratkaisun tekemiseen tarvitaan.

Tähän kuuluu olennaisena osana informaatiota ja sen käsittelyä koskevan lainsäädännön kartoittaminen.[39] Tietojärjestelmäsuunnittelussa tämä kuuluu aivan alkuvaiheeseen, johon kuuluu tietojärjestelmään talletettavan tiedon identifiointi, eri tietolajien välisten suhteiden hahmottaminen ja tietolajien varastoimista koskevien rajoitusten kartoittaminen. Järjestelmän suunnittelijan tulee ymmärtää syvällisesti kysymyksessä olevan organisaation toiminnassa tarvittava tieto ja sen käyttöä koskevat rajoitukset.[40] Oikeudellisesta näkökulmasta kysymys

[37] Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 319
[38] Vrt. ECJ C–293/12 and C–594/12. Teletunnistetietojen kerääminen onnistuu kyllä direktiivin avulla tehokkaasti ja tiedot ovat myös hyvin viranomaisten käytettävissä. Säilyttämisajoille ei kuitenkaan ole objektiivisia kriteereitä, jotka ohjaisivat säilyttämään tietoja vain sen aikaa kuin on välttämätöntä.
[39] Vrt. Wahlgren: Juridisk riskanalys (2003) s. 24–37. Siinä analysoidaan ensin yleisten työtehtävien kautta tilannetta koskeva oikeudellinen säännöstö ja käsitteistö sekä rakennetaan näistä käyttökelpoinen kokonaisuus. Toisena vaiheena on todellisen tilanteen analysoiminen, jossa arvioidaan tilanteen ajantasaisuus.
[40] Connolly – Begg: Database systems (2005) s. 22. See also Saarenpää: Opennes, Access, Interoperability and Surveillance – Transparency in the new Digital Network Society. Unpublished article based on presentation in The International Legal Informatics Symposium (IRIS), Law Faculty of the University of Salzburg 20–22 February 2014.

on nimenomaan lainsäädännön asettamista rajoituksista. Tätä korostaa myös julkisen hallinnon tietohallinnon ohjauksesta annetun lain (634/2011, *tietohallintolaki*) 3.1 §:n 2 kohta. Sen mukaan tietojärjestelmällä tarkoitetaan tiettyä käyttötarkoitusta varten kerätyistä tiedoista muodostettua automaattisen tietojenkäsittelyn avulla pidettyä tiedostoa tai tietovarantoa, jonka avulla käyttäjä voi tuottaa palveluja tai suorittaa muita tehtäviä *järjestelmän käyttötarkoituksen ja tietojen käsittelyä koskevien vaatimusten mukaisesti*.[41] Tietojärjestelmäsuunnittelija tarvitsee siis avukseen myös lakimiehen.

Työprosessit ovat kehittämisen lähtökohta. Jotta olisi mahdollista kehittää, on tiedettävä, mitä kehitetään. Se vaatii erityisesti työntekijöiden mukaan ottamista suunnitteluprosessiin. Tämän tulee tapahtua mahdollisimman aikaisessa vaiheessa.[42] Jos työprosesseja ei tunneta kokonaisuutena ja yksityiskohtineen, viranomaisen toiminta ei välttämättä muutu laadukkaammaksi ja tehokkaammaksi. Työntekijät tuntevat itse parhaiten oman työnsä, joten työprosessit tulee kartoittaa heidän kanssaan. Työntekijät otetaankin usein mukaan, mutta kysymys on melkein aina rajatusta työryhmästä. Työprosessien kartoitusvaiheessa jokaisen tulee olla mukana. Vain näin on mahdollista saada riittävän tarkka kuva niistä vaiheista, joissa asia etenee voimassa olevassa tilanteessa. Lisäksi saadaan tietoa siitä, missä työntekijöiden mielestä on eniten kehittämisen tarvetta.

Suunnitteluvaiheeseen kuuluu sen todentaminen, millaista informaatiota ja missä muodossa sitä työprosesseissa liikkuu. Informaatiolajien tunnistaminen on tärkeää, koska sen kautta on mahdollista yhdistää saatu informaatio oikeudelliseen viitekehykseen.[43] Pelkkä päätöksentekoprosessin kuvaaminen ei ole riittävää, vaan prosessien kuvaamisessa tulee kattaa käsiteltävän asian ja sitä koskevan informaation elinkaari. Informaation elinkaari ei pääty asian käsittelyn päättymiseen vaan se jatkuu viranomaisen arkistossa. Näin ollen prosessien kuvaamista tulee jatkaa työprosessien kuvaamisesta informaation elinkaaren kuvaamiseen. Tämä koskee myös osaprosesseja.[44] Suomessa lainsäädännöllinen perusta löytyy viranomaisen toiminnan julkisuudesta annetusta laista (621/1999, *julkisuuslaki*). Julkisuuslain 18 §:n hyvä tiedonhallintatapa sisältää samanlaisen kokonaisvaltaisen otteen kiinnittäen informaatioprosesseissa huomiota tiedon koko elinkaareen, ei vain ääripäihin tai joihinkin informaation käsittelyn vaiheisiin. Hyvä tiedonhallintatapa velvoittaa viranomaista

[41] Kursivointi tässä.
[42] Connolly – Begg: Database systems (2005) s. 22
[43] Ks. Connolly – Begg: Database systems (2005) s. 22
[44] Arkistolaitoksen määräys KA 1486/40/2005 Asiankäsittelyjärjestelmiin sisältyvien pysyvästi säilytettävien asiakirjallisten tietojen säilyttäminen yksinomaan sähköisessä muodossa s. 5, Väätänen: Oikein ja joutuisasti (2011) s. 35–38

kuvaamaan tiedon koko elinkaarta kuvaavan prosessin aliprosesseineen.[45] Se on mahdollista vain työprosessien kartoittamisen kautta. Suunnittelun tulee olla ennakoivaa eli huomiota tulee kiinnittää julkisuuslain 18 §:n 1 momentin 3 kohdan mukaan niihin vaikutuksiin, joita toimenpiteillä voi olla asiakirjojen julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun. Suunnittelussa on ennakoitava mahdollisia häiriötilanteita ja niihin varautumista.[46] Valmisteluvaiheessa tulee ryhtyä tarpeellisiin toimenpiteisiin tietoon liittyvien oikeuksien ja tiedon laadun turvaamiseksi sekä asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suojan järjestämiseksi. Tätä ajattelutapaa täydentää valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010, *tietoturvallisuusasetus*) 6 §, jonka mukaan tietoturvallisuustoimenpiteet on suunniteltava ja toteutettava siten, että ne kattavat asiakirjan *kaikki käsittelyvaiheet* niiden laatimisesta tai vastaanottamisesta arkistointiin tai hävittämiseen mukaan lukien asiakirjan luovuttaminen ja siirtäminen sekä käsittelyn valvonta. Elinkaariajattelu koskee kaikkea julkisessa hallinnossa tapahtuvaa informaation käsittelyä. Tietoturvallisuus ei ole vain informaatiota koskeva tekninen vaatimus. Se on yksi tae yksilön oikeuksien toteutumiselle.[47] Tietoturvallisuusasetus korostaa prosessin kuvaamista. Sen 5 §:n 1 momentin 3 kohdan mukaan valtionhallinnon viranomaisen on tietoturvallisuuden toteuttamiseksi huolehdittava siitä, että asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään. Informaatioprosessien merkitys on olla osana kokonaisprosessia ja siten tärkeänä osana oikeudellista laatua.

Kysymys on siitä, mihin huomio keskitetään. Sähköisten palvelujen kehittämisessä voidaan keskittyä esimerkiksi viranomaisten työn virtavuuteen toteuttamalla "once–only"–rekisteröintiperiaatetta. Sen mukaan asiakas antaisi vain kerran omat henkilötietonsa, minkä jälkeen eri hallinnon alueet voisivat käyttää niitä uudelleen.[48] Näkökulma on selkeästi hallinnon etuja ajava. Siinä on nähtävissä ne edut, joita se hallinnolle toisi, mutta eräs ongelma liittyy siihen, mitä tietoja henkilöstä tallennetaan. Väistämätöntä on, että näin luodaan henkilötietorekisteri, jolloin tietojen käsittelyn periaatteet määrittyvät henkilötietoja sääntelevän lainsäädännön kautta. Suomen kaltaisessa kattavan väestötietojärjestelmän maassa tällainen tuntuu turhalta. Väestötietojärjestelmä on viranomaisten käytettävissä, mutta

[45] Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010 s. 23
[46] HE 30/1998 vp s. 76–80 ja VAHTI 2/2010: Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. s. 23. Vrt. Pajukoski: Preventio, sosiaalioikeus ja kunnat (2006). s. 308–309, jossa *Pajukoski* käsittelee ennakoinnin ja suunnittelun merkitystä osana varautumista, joka käsittää sekä riskien syntymisen estämisen että varautumisen epävarmuuteen.
[47] Ks. Råman: Privacy, security and lawful interception: the quest for a new balance (2008) s. 173
[48] The European eGovernment Action Plan 2011–2015 s. 42–43. Samanlaista ajattelua on edustanut myös teletunnistetietojen tallennusta koskeva direktiivi. Ks. ECJ C‑293/12 and C‑594/12.

käyttöoikeudet määritellään kunkin virkailijan työtehtävien kautta. Henkilötietolain tarpeellisuusvaatimuksen mukaan vain sellaisia henkilötietoja tulee käsitellä, jotka ovat tarpeellisia suoritettavassa tehtävässä. Jos jokainen hallinnonala ryhtyy keräämään jokaisesta käsiteltävästä asiasta sen käsittelyssä asianosaisista kerätyt tiedot talteen, hyvin helposti syntyy henkilörekistereitä, joihin sisältyy suuret määrät arkaluonteista tietoa. Tarpeellisuusvaatimuksen mukaan ne henkilötiedot tulee hävittää, jotka eivät ole enää tarpeellisia suoritettavan tehtävän kannalta. Sähköisten palvelujen kehittämisen tavoitteenasettelussakin on huomioitava informaatioprosesseja ja informaatiota koskeva lainsäädäntö, joka määrittelee kunkin informaatiolajin käsittelytavat prosessin edetessä.

Once–only–rekisteröintiperiaatteen kaikuja voi nähdä suomalaisessa julkishallinnon arkistotoiminnassa. Samalla tulee esiin se, mitä etuja once–only–periaatteesta voisi olla, jos olisi olemassa käyttöyhteys toisen viranomaisen sähköisesti arkistoimiin asiakirjoihin. Suomalaisen julkishallinon arkistoinnin periaatteena on, että vain yksi viranomainen arkistoi tietyntyyppisiä asiakirjoja. Esimerkiksi veroviranomainen arkistoi perintöverotuksesta päättäessään vainajan perukirjan. Perukirjoja tarvitaan myös muualla julkishallinnossa, kuten kirjaamisviranomaisessa. Kirjaamisviranomainen diarioi perukirjan, muttei arkistoi. Asiakkaan on toimitettava perukirja niin veroviranomaiselle kuin kirjaamisviranomaisellekin. Jos kirjaamisviranomaisen olisi mahdollista saada perukirja verohallinnon arkistoista, asiakkaan ei tarvitsisi toimittaa sitä uudelleen. Maanmittauslaitos otti käyttöön uuden kirjaamisasioiden tietojärjestelmän Kirren toukokuussa 2013. Sen myötä uudistettiin arkistointiakin. Esimerkiksi perukirjoja ei enää arkistoida kirjaamisasioita ratkaistaessa. Näin ollen asiakas joutuu toimittamaan perukirjan uudelleen, jos kuolinpesä liittyy osapuolena esimerkiksi kiinteistön kauppaan. Aikaisemmin arkistointi toteutettiin niin, että perukirjat arkistoitiin asian hävitettäviin liitteisiin, joiden säilytysaika oli kuusi vuotta. Jos tuona aikana kuolinpesä oli uudelleen kirjaamisasiassa asianosaisena, kirjaamisviranomainen sai perukirjan edellisen asian hävitettävistä liitteistä. Arkistoinnin once–only–periaate siis merkitsee tässä kohden heikennystä asiakkaan asemaan. Se voi vaikuttaa kirjaamisviranomaisen tehokkuuteen, koska se joutuu pyytämään perukirjan asiakkaalta uudelleen, kun se aiemmin saattoi löytyä omista arkistoista. Tämä on mahdollista havaita vain, jos työprosessit tunnetaan riittävän tarkasti. Arkistoinnissa säästetään kuitenkin informaation varastoinnissa eikä asiakirjan arkistoiminen kahteen kertaan ole muutenkaan järkevää. Tässä kohdin once only–rekisteröintiperiaate ei kuitenkaan mahdollista yhteistyötä kahden viranomaisen välillä vaan asiakirja on pyydettävä aina asiakkaalta.

Informaation laatu vaikuttaa niin menettelyn onnistumiseen kuin aineellisen lainsäädännön soveltamiseen yksittäistapauksessa. Oikeudellinen tiedonhaku on silloin keskeisessä asemassa. Pelkkä hakukielen komentojen tai oikeiden hakusanojen käytön osaaminen eivät riitä vaan lakimiehen tulee osata yhdistää tähän myös muu oikeudellinen ammattitaitonsa. Oikeudellinen päätöksenteko on helpompaa tehdä laadukkaasti, kun sen tueksi löydetään oikeaa informaatiota.[49] Tiedonhaussa epäonnistuminen tarkoittaa usein epäonnistumista koko työtehtävässä.[50] Tällöin puhutaan oikeuden tehokkuudesta, joka on määritelty lain reaaliseksi soveltamiseksi niissä käytännön tilanteissa, joissa se on tarkoitettu sovellettavaksi.[51] On osattava arvioida löydettyä tai saatua tietoa.

Edunvalvojan määräämisasiassa hankitaan tietoa myös muista kuin oikeudellisista tietovarannoista. Arvioinnin kohteena on ihminen. Selvitettäviä kysymyksiä ovat mm. kykeneekö hän hoitamaan omia asioitaan, onko hänellä hoidettavia asioita, ymmärtääkö hän erilaisten arjessa vastaan tulevien asioiden merkityksen. Kysymys on ihmisen arvioinnista, jolloin viranomaisen välineillä ja arviointitaidoilla, on suurta merkitystä. Ihmisellä on oikeus tulla arvioiduksi oikeassa valossa. Maistraatin on holhousviranomaisena hankittava edunvalvojan määräämisasiassa tietoa niin henkilön yksityisestä kuin julkisesta kuvasta, jotta oikea kuva on mahdollista muodostaa. Ihmisellä on oikeus tulla arvioiduksi omana itsenään. Olennaista onkin se, että päätöksenteon pohjana oleva tieto on oikeaksi todistettavissa.[52]

Edunvalvojan määrääminen informaatioprosessina tarvitsee prosessiin liittyvien riskien kartoittamista. Edellä mainitut vaiheet sisältävät oikeudellisten riskien kartoittamisen työ– ja informaatioprosesseissa samalla, kun prosessit kuvataan mahdollisimman yksityiskohtaisesti. Arviointiin tulee liittyä tilanteen vertaaminen sovellettavaan oikeudelliseen materiaaliin sekä organisaatiossa itsessään tapahtuneisiin muutoksiin. Päätöksentekoprosessien analysoiminen niin yksilö– kuin organisaatiotasolla on osa tätä kokonaisuutta. Kommunikaatioprosessien analysoimisella on merkitystä oikeudellisen soveltamisen sujuvuudelle. Yksi kommunikointiprosesseista on se, jonka osapuolina ovat oikeudellisen informaation tuottajat ja informaation vastaanottajat eli tässä tapauksessa holhousviranomainen. Olennaista on se, millaista tietoa on saatavilla, millä tavalla ja miten sitä käytetään.[53] Tässä tutkimuksessa tämä kommunikaatioprosessi on osa kokonaisprosessia. Oikeudellisen informaation tehokas

[49] Saarenpää: Oikeusinformatiikka (2012) s. 487–489
[50] Seipel: Juridik och IT (2004) s. 120
[51] Pöysti: Oikeudellinen tieto ja julkisen toiminnan tehokkuus (2010) s. 246
[52] Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 316–317 ja eduskunnan apulaisoikeusasiamiehen ratkaisu AOA 327/4/09
[53] Bing analysoi näitä kommunikaatioprosesseja väitöskirjassaan. Ks. Bing: Rettslige kommunikasjonsprosesser (1982) s. 18–25

saatavuus on yksi oikeudellisen laadun peruskivistä. Oikeudellisen laadun toteutumiseen vaikuttaa se, saadaanko oikeudellisesti relevanttia informaatiota. Edunvalvojan hakemista koskevassa asiassa tarvitaan selvitystä, jonka perusteella on mahdollista arvioida edunvalvojan määräämisen edellytyksiä. Informaation avulla holhousviranomaisen tulee pystyä arvioimaan henkilön toimintakykyä ja sitä, onko olemassa sellaisia hoidettavia asioita, joiden vuoksi edunvalvojan määrääminen on tarpeen. Viranomainen ei kuitenkaan voi hankkia tietoja keinolla millä hyvänsä vaan sen on tapahduttava menettelysäännösten ja erilaista informaatiota koskevien lakien mukaisesti. Viranomaisen tulee pystyä perustelemaan oikeudellisesti pyytämänsä tiedon tarve. Riittävän tiedonhankinnan jälkeen viranomaisen on kyettävä ratkaisemaan asia selville saatujen seikkojen valossa. Informaatioprosessi ei kuitenkaan pääty oikeudelliseen ratkaisuun tai päätökseen. Tiedon tie jatkuu arkistointiin ja lopulta arkistolainsäädännössä ja –suunnitelmissa päätettyjen määräaikojen kuluttua tiedon hävittämiseen. Tiedon tien kokonaisvaltainen hahmottaminen ja varmistaminen ovat oikeusvaltion keskeisiä lähtökohtia.[54] Oikeudellisen laadun lähtökohta on menettelyllisen, aineellisen ja eri informaatiolajeja koskevan lainsäädännön tuntemus sekä yhdistäminen käytännön toimintaan.

Viranomaisen toimintaan tulee oikeuden lisäksi yhdistää ymmärrys informaation ja informaatioympäristön suhteesta, informaatioprosesseista ja informaatioteknologiasta.[55] Kysymys ei ole vain teknisten kysymysten hahmottamisesta. Seipel antaa tästä erinomaisen esimerkin tuomioistuinten automatisoinnin tutkimuksesta. Automatisoinnin kohdalla tulee tutkia esimerkiksi sitä, millä tavalla lainmukaisuuden vaatimus turvataan, onko tarvetta hahmottaa uudelleen menettelyä koskevia säännöksiä ja oikeuslaitoksen organisaatiota ylipäänsä.[56] Kun viranomaishallintoa ryhdytään uudistamaan, toteuttamisessa on aina huomioitava oikeusvaltion vaatimukset.[57] Informaation käsittelyn oikeudellisen laadun takaamisessa ei tule keskittyä vain sähköisessä muodossa olevan informaation käsittelyyn. Suomalaisten viranomaisten kohdalla ei voida vielä puhua paperittomasta toimistosta. Välineneutraali ajattelutapa on myös suomalaisen henkilötietolain ja viranomaisten toiminnasta annetun lain 18 §:n määrittelemän hyvän tiedonhallintatavan lähtökohta.[58]

Edunvalvojan määräämisasia on hyvin informaatioriippuvainen. Tavalla, jolla erilaista informaatiota menettelyn kuluessa käsitellään, on paljon merkitystä. Avustavia ja teknisiä

[54] Saarenpää: Oikeusinformatiikka (2012) s. 461
[55] Pöysti: Communicational Quality of Law (2006) s. 465
[56] Seipel: Legal Informatics Broad and Narrow (2009) s. 28
[57] Lenk – Traunmüller: Broadening the Concept of Electronic Government (2007) s. 20
[58] HE 30/1998 vp. s. 53–58 ja HE 96/1998 vp. s. 35–36

työtehtäviäkään ei voi jättää vaatimusten ulkopuolelle. Näin on todennut oikeusasiamies ratkaisussaan dnro 941/4/07, jossa oli kysymys sosiaalipalvelukeskuksen salassapidettävien asiakirjojen käsittelystä ja luovuttamisesta henkilöllisyyttä tarkastamatta. Sosiaalipalvelukeskuksen virastomestari oli kopioinut salassapidettäviä asiakirjoja kopiokoneella, jolle yleisölläkin oli pääsy ja unohtanut ne kopiokoneen viereen. Lisäksi virastomestari oli luovuttanut tiedot niitä pyytäneelle henkilölle ilman, että oli tarkastanut tämän henkilöllisyyttä ja siten oikeutta saada kysymyksessä olevia asiakirjoja. sosiaalipalvelukeskuksessa olisi ollut mahdollisuus ottaa kopioita sellaisessakin tilassa, johon yleisöllä ei ollut pääsyä. Virastomestari vetosi kiireeseen sekä siihen, että asiakaspalvelu ja yksin henkilökunnan käytössä ollut kopiokone sijaitsivat eri kerroksissa. Oikeusasiamies korosti vastuuta suorittaa avustavatkin työtehtävät kiireestä huolimatta asianmukaisella huolellisuudella, jotta asiakkaan oikeus yksityisyyteen tulevat turvatuiksi. Tapaus tuo hyvin esille sen, että kaikkien niiden henkilöiden, jotka käsittelevät arkaluonteista ja salassapidettävää tietoa, tulee tietää informaation käsittelyä koskevista säännöksistä ja niiden vaikutuksista informaation käsittelylle. Yleisesti ottaen laadun kannalta on tärkeää, että tehdään oikeita asioita.[59] Oikeudellisessa laadussa myös tekemisen tavalla on merkitystä. Tekemisen tavan tulee viranomaistoiminnassa olla oikeudellisesti perusteltu, myös informaation käsittelyssä.

Informaation käsittely on aina prosessi, jonka kaikki vaiheet on suunniteltava etukäteen ja tätä suunnitelmaa tulee noudattaa kaikissa käsittelyn vaiheissa ja kaikissa käsittely–ympäristöissä. Suunnittelu on oikeudellisesti säänneltyä. Suomessa keskeisimmät lait ovat henkilötietolaki ja laki viranomaisten toiminnan julkisuudesta. Niissä lähtökohta on välineneutraali eli ne koskevat niin manuaalisessa informaation käsittelyä kuin informaatio– ja tietojärjestelmissä tapahtuvassa informaation käsittelyä.

Informaatiovirran kulkua tai yksittäisenkään asiakirjan kulkua on kuitenkin mahdotonta suunnitella, ellei ole olemassa ajantasaista prosessinkuvausta kaikista niistä vaiheista, joissa juuri sitä informaatiota tarvitaan. Erityisesti hiljainen tieto informaatiovirran kulusta jää tällöin saamatta.[60] Samanlainen ajattelumalli korostuu tämän tutkimuksen tavassa tarkastella oma–aloitteista edunvalvojan hakemista ja toisaalta edunvalvontavaltuutuksen vahvistamista. Jokaisen asiakkaan asian hoitaminen on oma, ainutlaatuinen prosessinsa jo siitäkin syystä, että holhoustoimilain lähtökohtana on holhousviranomaisen velvollisuus tarkastella yksilön etua

[59] Lecklin: Laatu yrityksen menestystekijänä (2006) s. 20
[6060] JHS 152 s. 3. Tässä kohden käsitän hiljaisen tiedon työntekijälle työkokemuksen ja asiantuntemuksen lisääntymisen kautta syntyneenä tietona siitä, millä tavalla informaatioprosessi todellisuudessa etenee.

tapauskohtaisesti. Kysymys ei ole epätoistuvasta prosessista, sillä menettelysäännökset merkitsevät sitä, että jokaisessa edunvalvojan määräämisasiassa kuin edunvalvontavaltuutuksen vahvistamisasiassakin toistuvat tietyt vaiheet.[61] Menettelysäännökset tuovat muodon osaksi prosessia.[62] Tapauskohtaisuus tulee ilmi informaatiossa, jota kulloinkin käsillä olevassa tapauksessa on tarpeen hankkia. Henkilötietojen kohdalla henkilötietolain (523/1999) 9 §:n 1 momentin tarpeellisuusvaatimus edellyttää tapauskohtaista harkintaa. Edunvalvojaa määrättäessä ei juuri muunlaisia tietoja kerätäkään. Viranomaisen toiminnan oikeudellinen laatu on tällöin avainasemassa. Henkilötietojen suojan rooli ihmisen perusoikeuksien suojaajana korostuukin edunvalvojan määräämisasioissa.[63]

4. Oikeudellinen laatu

Edunvalvojan määräämisessä informaatioprosessien tarkastelussa tulee tutkia, miten jokainen prosessin vaihe saadaan toimimaan niin, että yksilön oikeudet ovat toiminnan arkipäivää.[64] Informaatioprosessin jokainen vaihe on tiedostettava ja tarkasteltava yksilön oikeuksien näkökulmasta. Edunvalvojan määräämisasiassa se on henkilö, joka hakee itselleen edunvalvojaa tai henkilö, jonka tekemän edunvalvontavaltuutuksen nojalla valtuutettu hakee valtuutuksen vahvistamista. Näkökulma tulee suunnata määrällisten tavoitteiden sijasta siihen, mitä laatu on sisällöltään oikeudellisessa ympäristössä.

Oikeudelliseen laatuun kuuluvat prosessin ulkoiset puitteet, kuten toimivaltakysymykset ja menettelysäännökset, ja prosessin konkreettinen sisältö, joissa oikeudellinen harkinta ja laintulkinta ovat arkipäivää, sekä informaatiota ja informaatioprosesseja koskeva sääntely. Kun tämä kokonaisuus on hahmotettu, on mahdollista selvittää, miten yksilön oikeudet toteutuvat.

---

[61] *Lillrankin* mukaan meiltä puuttuu vielä kunnollinen teoria laadusta juuri epätoistuvien prosessien osalta. Ks. Lillrank: Laadun kehitys ja tietoyhteiskunta (2001) s. 35

[62] Ks. Muukkonen: Muotosäännökset (1958) ja erityisesti s. 26 ja 31–43. *Muukkonen* määrittelee muotosäännöksen sellaisiksi välittömästi sopimuksen solmimiseen liittyviksi oikeustosiasioiksi, jotka ilmaisevat, missä järjestyksessä sopimus on tehty tai on tehtävä. Tämä määritelmä sisältää *Muukkosen* mukaan muodoksi katsottavien oikeustosiasiain yleistunnusmerkistön. Erikoistunnusmerkistötapaukset taas muodostuvat usein erikoislakien kautta muodostaen hyvin heterogeenisen joukon. Tätä taustaa vasten hallintolain menettelysäännökset voitaisiin nähdä yleistunnusmerkistöksi ja holhoustoimilain edunvalvojan hakemista ja edunvalvontavaltuutuslain vahvistamista koskevat säännökset voitaisiin nähdä erikoistunnusmerkistönä.

[63] Ks. Saarenpää: Henkilö– ja persoonallisuusikeus (2012) s. 319. *Saarenpään* mukaan henkilötietojen suoja on samalla muiden perusoikeuksien suojaa.

[64] Asiakkuudessakin tulisi kiinnittää erityistä huomiota kokonaisuuteen, ei vain yksittäisiin kohtaamisiin. Vain näin voidaan ymmärtää asiakkuuden prosessiolemus. Ks. Storbacka – Lehtinen: Asiakkuuden ehdoilla vai asiakkuuden armoilla (2002) s. 20.

Perusoikeudet velvoittavat viranomaistoiminnassa nykypäivänä.[65] Toimiva ja hyvä hallinto on avainasemassa kehitettäessä oikeusvaltiota, koska hallinnon toiminta koskettaa lähes kaikkia.[66] Ihmis– ja perusoikeuksien voimakas esiinmarssi korostaa yksilön itsemääräämisoikeutta, onhan osa sitä suojaavista perusoikeuksista luonnehdinnaltaan nimenomaisesti vapausoikeuksia.[67] On perusteltua puhua ihmis– ja perusoikeusvelvoitteisesta demokraattisesta oikeusvaltiosta, jossa kaiken julkisen vallan käytön lähtökohtana tulee olla yksilön ihmis– ja perusoikeudet oikeudenmukaisuuden mittarina. Tähän kuuluu käsitys yksilön itsemääräämisoikeudesta ja sen kunnioittamisesta kaikissa tilanteissa – myös silloin, kun yksilö ei enää itse kykene huolehtimaan omista asioistaan. Yksilön oikeuksien yhtenä tehtävänä on rajata tätä oikeutta määrätä itse omasta tahdostaan.[68]

Ihmis– ja perusoikeusvelvoitteisuus tulee lisäksi toteutua kaikissa viranomaisen toimintaympäristöissä. Nykyisin tämä tulee muistaa erityisesti sähköisiä palveluja rakennettaessa. Näihin liittyviä infrastruktuureja rakennettaessa, palveluja suunniteltaessa ja toteutettaessa tulee huolehtia yksilön oikeuksien turvaamisesta oikeusvaltioajattelun mukaisesti.[69] Odotamme eri instituutioiden toiminnalta yhä parempaa oikeudellista laatua, joka rakentuu vahvasti tehokkaasti toteutettavissa olevien yksilön oikeuksien varaan. Tämä on myös osa oikeudellista hyvinvointia.[70]

Itsemääräämisoikeuteen puuttumisen tulee perusoikeusvelvoitteisessa, demokraattisessa oikeusvaltiossa aina perustua lakiin, jonka ihmis– ja perusoikeuksien mukaisuus on asianmukaisesti arvioitu lain valmisteluvaiheissa. Toisaalta, perustuslaissa voitaisiin velvoittaa lainsäätäjää pidättäytymään sellaisten säännösten tekemisestä, jotka puuttuvat jollakin tavalla yksilön oikeuksiin.[71]

Oikeudellisesti laatu on ollut pitkään läsnä. Oikeudellista päätöksentekoa koskeva keskustelu on esimerkkinä tästä.[72] Oikeudellista tiedonhakua ja sen merkitystä koskeva keskustelu on täydentänyt kuvaa oikeudellisesta laadusta. Oikeudellisten sääntöjen

---

[65] Perusoikeusvelvoitteisuudesta on kirjoittanut *Saarenpää* artikkelissaan ”Oikeusvaltio ja verkkoyhteiskunta” (2002). Ks. erityisesti s. 114. Perusoikeuksien sitovuus viranomaisten osalta ei aina ole ollut itsestään selvää. Ks. Hidén: Perusoikeudet Hallitusmuodon II luvussa (1971) s. 19–20.
[66] Hallberg: The Rule of Law (2004) s. 288
[67] Habermas: Between Facts and Norms (1996) s. 82 ja Saarenpää: Kansalainen, yksilö kaiken keskipisteenä (2010) s. 84
[68] Habermas: Between Facts and Norms (1996) s. 82–83
[69] Ks. Saarenpää: Oikeusvaltio ja verkkoyhteiskunta (2002) s. 119 ja It i människans tjänst – en digital agenda för Sverige (2011) s. 9
[70] Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 227
[71] Ks. SOU:2008:3 s. 16. Ruotsalaisessa keskustelussa ei ole pidetty riittävänä perustuslaissa yksityisyyden suojan tai henkilökohtaisen integriteetin suojan kohdalla valittua tapaa velvoittaa lainsäätäjä ja julkisen vallan käyttäjät vain kunnioittamaan näitä oikeuksia.
[72] Ks. Makkonen: Oikeudellisen ratkaisutoiminnan ongelmia (1981)

soveltaminen, esimerkiksi oikeudellisen päätöksenteon tilanteissa, on helpompaa, kun sen tueksi löydetään oikeaa informaatiota.[73] Oikean informaation merkitys tulee ilmi korkeimman oikeuden ratkaisusta KKO:2011:63. Asiassa oli toimitettu sähköpostitse valitus käräjäoikeuden sähköpostiin. Palvelin oli kuitenkin luokitellut viestin roskapostiksi ja viesti siirtyi vasta määräajan jälkeen käräjäoikeuden sähköpostiin. Korkein oikeus katsoi, ettei hovioikeus olisi saanut hyväksyä käräjäoikeuden päätöstä hankkimatta selvitystä valituksen saapumisesta tietojärjestelmiin. Korkein oikeus tähdensikin, että asiassa olisi tullut hankkia selvitystä tuomioistuimen tietojärjestelmien asianmukaisesta toiminnasta. Kysymys on toisaalta olemassa olevan tiedon tarkistamisesta, toisaalta riittävän selvityksen hankkimisesta ratkaisun tueksi erityisesti silloin, kun asianosainen on tuonut ilmi seikkoja, jotka horjuttavat viestin saapumisajankohtaa koskevan tiedon luotettavuutta.[74]

Oikeudellisilla tiedonhakutaidoilla on suuri laadullinen merkitys oikeudellisen työn onnistumisen kannalta: tiedonhaun epäonnistuminen tarkoittaa usein epäonnistumista koko työtehtävässä.[75] Kysymys on oikeuden tehokkuudesta, jonka *Pöysti* on määritellyt lain reaaliseksi soveltamiseksi niissä käytännön tilanteissa, joissa se on tarkoitettu sovellettavaksi. Oikeuden tehokkuus tarvitsee toteutuakseen hyviä, oikeudellisen informaation ja tietovarannon laatuvaatimukset täyttäviä informaatioresursseja eli tietovarantoja sekä ymmärrettävää, helposti saavutettavaa ja luotettavaa oikeudellista viestintää.[76] Viranomaisten tietojenkäsittelyssä asia tiivistyy informaatioprosesseihin ja niiden järjestämiseen julkisuuslain 18 §:n mukaisen hyvän tiedonhallintatavan mukaisesti. [77] Oikeudellisen laadun alkupiste on informaatiossa ja sen laadussa, josta se etenee tietovarantojen laatuun ja lopulta oikeudelliseen viestintään. Oikeudellisessa laadussa on kysymys informaatioprosessin laadusta kaikissa informaation ilmenemismuodoissa. Viranomaisen velvollisuutena on huolehtia, ettei esimerkiksi henkilötietoja kerätä tarpeettomasti tai ilman oikeudellista perustetta ja että niitä käsitellään oikeudellisesti kestävällä ja laadukkaalla tavalla *jokaisen* työntekijän toimesta. Ja tämä vaatimus koskee kaikenlaista tietojenkäsittelyä – myös paperimuodossa olevan informaation käsittelyä, jota edelleen julkishallinnossa on. Tämä unohtuu helposti keskityttäessä vain sähköiseen hallintoon informaatiohallinnon sijasta.

Oikeudellisen työn laadun parantamisessa on aina kysymys riskien arvioimisesta. Maistraatin edunvalvojanmääräämisprosessissa arvioidaan yksilön oikeuksiin kohdistuvia

[73] Saarenpää: Oikeusinformatiikka (2012) s. 487.
[74] Ks. myös KKO:2005:3
[75] Seipel: Juridik och IT (2004) s. 120
[76] Pöysti: Oikeudellinen tieto ja julkisen toiminnan tehokkuus (2010) s. 246
[77] Pöysti: Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet (2002) s. 73

riskejä. Edunvalvontaa tulee tarkastella niiden tosiasiallisten vaikutusten kautta, joita sillä yksilölle on. Ne aiheutuvat joiltain osin suoraan holhoustoimilain säännöksistä, osa taas johtuu lain tulkintatavoista.

5. Viestintä informaatioprosessin ja oikeudellisen laadun osatekijänä

Oikeus on riippuvainen informaatiosta ja viestinnästä oikeudellisten toimijoiden ja asianosaisten välillä.[78] Edunvalvojan määräämisessä riippuvuus oikeudellisen viestinnän onnistumisesta ja sen oikeusturvaan vaikuttavasta luonteesta tulevat hyvin esille. Hakemuksen oma–aloitteisuutta selvitettäessä keskeisiä asioita ovat hakijan motiivit ja lähtökohdat hakemuksen tekemiselle. Tässä keskeisenä välineenä on kuuleminen. Oikeus tulla kuulluksi on keskeinen osa oikeusturvaa, jota suojataan perustuslain 21.2 §:n säännöksellä. Se on myös yksi hyvän hallinnon tae.[79]

Haettaessa edunvalvojaa oma–aloitteisesti kuulemisen tarkoituksena on selvittää hakemuksen oma–aloitteisuutta ja henkilön ymmärryskykyä asian vaikutuksista. Hallinto–oikeudellisesti kysymys on *hakijan* kuulemisesta. Hakija käyttää asiassa itsemääräämisoikeuttaan ja hänen näkemyksillään tulisi olla, erityisesti silloin, kun hänen katsotaan ymmärtävän asian merkityksen, suuri painoarvo.[80] Kuuleminen on myös osa asian huolellista ja totuudenmukaista selvittämistä.[81]

Myös kuulemisessa on otettava huomioon edunvalvontaoikeuden periaatteet. Erityisesti tulee huomioida edunvalvonnan yksilöllisyyden periaate. Yleisellä tasolla keskusteltaessa esimerkiksi samoja kysymyksiä sisältävät keskustelun rungot ovat hyvä lähtökohta, mutta maistraatin on tiedettävä ennen kuulemista tarpeeksi, jotta se voisi päästä riittävän yksilölliselle tasolle.

Yksilöllisyyden huomioimiseen kuuluu myös kuulemistavan valinta. Holhoustoimilain 86 §:n mukaan holhousviranomaisen on kuultava henkilökohtaisesti häntä, jolle edunvalvojan määräämistä harkitaan. Henkilökohtaisuus voidaan kuitenkin toteuttaa myös virka–apuna tapahtuvalla kuulemisella tai teknisen käyttöyhteyden avulla. Erityisesti teknistä käyttöyhteyttä harkittaessa tulee huomioida myös kuultavan mielipide ja toisaalta myös muut asiaan vaikuttavat seikat. Jos henkilö kokee teknisen käyttöyhteyden käyttämisen epämukavaksi,

[78] Katsh: Law in a Digital World (1995) s. 7
[79] HE 309/1993 vp. s. 72–74
[80] *Helin* on korostanut ihmisen näkemyksien arvostamista erityisesti keskusteltaessa edunvalvojan tehtävän rajoista oma–aloitteisessa hakemuksessa. Helin: Edunvalvojan päätösvallan rajoista (2001) s. 1075
[81] Laakso – Suviranta – Tarukannel: Yleishallinto–oikeus (2006) s. 170

kuulemisella ei välttämättä saada kaikkea sitä tietoa, jota tarvitaan. Toisaalta se voi vaikuttaa myös henkilön ymmärryskyvyn arvioimiseen.

Holhoustoimilain 86 §:n 2 momentti ja sen perustelut eivät kuitenkaan annan tukea yksilöllisyyden huomioimiselle. Säännös on selkeän viranomaislähtöinen: kuuleminen joko virka–apuna tai teknisen yhteyden avulla on mahdollista, jos se on pitkien etäisyyksien tai muun syyn vuoksi tarpeen. Tällainen muu syy voi olla esimerkiksi se, että kuultava on suljetussa laitoshoidossa. Matkustaminen kuultavan luo voi perustelujen mukaan viedä huomattavan paljon työaikaa, minkä vuoksi virka–apuna suoritettava kuuleminen tai teknisen yhteyden välityksellä tapahtuva kuuleminen ovat vaihtoehtoina tarpeen.[82] Säännös on yksi esimerkki viranomaisen toiminnan tehostamisesta, mikä sinänsä on järkevääkin. Mutta asian pohtiminen tulee aloittaa ja lopettaa sen henkilön näkökulmaan, jota kuullaan. Edunvalvontaoikeudessa tämä tarkoittaa päämiehen edun arvioimista asiankäsittelyn jokaisessa vaiheessa – myös kuulemisessa.

Jos kuuleminen toimitetaan teknisten apuvälineiden avulla, holhoustoimilain 86 §:n 2 momentin perustelujen mukaan virkamiehen ja kuultavan on oltava sekä puhe– että näköyhteydessä toisiinsa. Pelkkää puhelimitse kuulemista ei pidetä riittävänä, koska se ei anna samanlaista havainnointimahdollisuutta kuin näköyhteys. Kuulemisen toteuttavan virkamiehen arvioitavaksi jää, onko teknisten apuvälineiden avulla saavutettu kuulemiselle asetetut tavoitteet. Jos ei ole, on kuuleminen suoritettava 86 §:n 1 momentin määrittämällä tavalla henkilökohtaisesti.[83] Teknisen yhteyden kautta kuuleminen voi tarkoittaa esimerkiksi videoneuvotteluyhteyden avulla tapahtuvaa kuulemista. Oli valittu tekninen tapa mikä hyvänsä, maistraatin tulee ottaa kuulemistilanteessa huomioon laitteistosta johtuvat seikat. Ääni voi tulla hitaammin kuin kuva, jolloin vaikutelma vieraasta henkilöstä voi vääristyä täysin. Kuultava voi jännittää teknisiä laitteita ja tilanteen outoutta niin, ettei sen vuoksi kykene antamaan itsestään oikeaa kuvaa. Teknisen yhteyden käyttämisessä pitäisikin ensin kysyä kuultavalta, mitä mieltä hän on tällä tavoin järjestettävästä kuulemisesta.

Kuuleminen on viestintätapahtuma, johon kuulemistavan ja –paikan valitsemisen lisäksi vaikuttaa viestinnän sisältö ja sen laatu. Henkilökohtaisesti tapahtuvassa hakijan kuulemisessa tai virka–apuna suoritetussa kuulemisessa tilanne rakentuu käytännössä kokonaan läsnä olevien henkilöiden varaan. Silloin on kiinnitettävä huomiota viestintään ja sitä koskeviin

[82] HE 203/2010 vp. s. 25

[83] HE 203/2010 vp. s. 25–26. Vaikka perustelujenkin kanta on selkeä, maistraateissa saatetaan hoitaa kuuleminen esimerkiksi asian kiireellisyyden vuoksi puhelimitse. Puhelinkuuleminen on kuitenkin poikkeuksellista ja sitä käytetään lähinnä tilanteissa, joissa henkilö on jo tuttu.

perusperiaatteisiin. *Wiio* tarkoittaa viestintä–sanalla ihmisten välisten sanomien, tietojen vaihdantaa niin kielellisessä kuin sanattomassakin mielessä. Viestinnän onnistumista tavoiteltaessa tulee huomioida se tilanne, jossa viestintä tapahtuu sekä se, kenelle viestitään. Sanoma on laadittava vastaanottajaa varten. *Wiio* näkee kielen ymmärrettävyyden oikeusturvakysymyksenä erityisesti viranomaisissa toimittaessa.[84] Sama pätee tietysti teknisin apuvälinein toteutettavaan kuulemiseen. Viestin sisällön lisäksi on testattava välineiden toimivuus ja vaikutus puheeseen.

Wiion mukaan viestin ymmärtämiseen vaikuttavat ihmisen kokemukset. Tästä syystä kaksi ihmistä ei voi ymmärtää samaa asiaa samalla tavalla, sillä sanojen merkitys riippuu nimenomaan kokemuksesta. Ja koska kokemukset ovat erilaisia, merkityksetkin ovat erilaisia. Ymmärtämiseen vaikuttavat vastaanottajan asenteet ja odotukset. Viestinnän onnistumisen kannalta olennaisempaa on se, mitä viestitään, ei se, kuinka paljon viestitään. Mitä enemmän viestitään, sitä nopeammin lisääntyvät väärinymmärrykset.[85] Käytännössä tätä on pyritty välttämään osassa maistraatteja niin, että hakijan kuulemistilaisuuteen osallistuu esittelijän lisäksi esimerkiksi osastosihteeri tai henkikirjoittaja. Vaikka toinen olisikin enemmän kuuntelijan ja muistiinpanojen tekijän roolissa, voi hän huomata tai muistaa jotakin, mikä toiselta menee ohi.

Henkilön hakiessa oma–aloitteisesti edunvalvojaa on lisäksi selvitettävä se, että hakemus on nimenomaan hänen oma ja aito tahdonilmaisunsa. Tällä on merkitystä maistraatin toimivallan kannalta, sillä holhoustoimilaki rajoittaa maistraatin toimivallan vain oma–aloitteisten hakemusten käsittelyyn. Jos henkilön pyyntöä ei ole mahdollista pitää oma–aloitteisena, se kuuluu tuomioistuimen käsiteltäväksi.

Jotta pyynnön oma–aloitteisuudesta voidaan varmistua, tarvitaan selvitystä henkilön olosuhteista ja kaikista muista asian arviointiin vaikuttavista seikoista, kuten henkilön omasta käsityksestään tarvitsemastaan tuesta, hänen identiteetistään ja toimintansa rakentumisen logiikasta. Pelkkä juridisista perusteista lähtevä kuuleminen ei ole riittävää vaan henkilöä on aidosti ja avoimesti kuunneltava.[86]

Kuuleminen oikeudellisena viestintätapahtumana on edunvalvojan määräämisasiassa kaksisuuntaista. Maistraatin on saatava selville se, mitä henkilö jo tietää edunvalvojan

[84] Wiio: Wiion lait – ja vähän muidenkin (1978) s. 18–19
[85] Wiio: Wiion lait – ja vähän muutakin (1978) s. 23–26
[86] Walin – Vängby: Föräldrabalken (2009) 11:47. Avoimuudella viitataan tässä erityisesti siihen, että kuuntelemisen pitäisi olla vapaa erilaisista ennakko–odotuksista ja stereotypioista, jotka helposti estävät henkilön näkemisen oikeassa valossa, omana itsenään. Ks. myös Juhila: Sosiaalityöntekijöinä ja asiakkaina (2006) s. 251

määräämisestä ja edunvalvojan roolista suhteessa päämieheen. Tämän lisäksi kysymys on maistraatin velvollisuudesta antaa tietoa aiheesta. Maistraatin on varmistuttava siitä, että hakija ymmärtää edunvalvojan määräämisen merkityksen. Jos hakija ei ymmärrä, maistraatti ei ole toimivaltainen ratkaisemaan asiaa.

Se, ymmärtääkö hakija edunvalvojan määräämisen merkityksen, vaatii riittävän informaation antamista ennen kuin ymmärryskykyä voidaan tarkastella. Tämä vaihe kuuluu luontevasti neuvontavaiheeseen, joka voi ajallisesti tapahtua ennen hakemuksen vireilletuloa ja vireillä oloaikana esimerkiksi kuulemistilanteessa. Henkilön tulee olla tietoinen asiasta, jota hän hakee ja ymmärtää sen merkitys oman jokapäiväisen elämänsä kannalta. Tilannetta voidaan verrata potilasoikeudessa tunnettuun ajatteluun tietoisesta suostumuksesta. Suostumuksen tulee olla kelpoisuuden omaavan henkilön antama ja henkilön tulee olla kykenevä ymmärtämään suostumuksen merkitys. Henkilön tulee antaa suostumus vapaaehtoisesti ja vakavan harkinnan tuloksena. Jotta tämä on mahdollista, suostumusta antavalle henkilölle on tullut antaa täydellinen kuva asiaan vaikuttavista seikoista.[87] Samalla tavalla kuin tietoinen suostumus on luonteeltaan tietyntyyppinen valtuutus puuttua potilaan ruumiilliseen koskemattomuuteen[88], edunvalvojan hakeminen oma–aloitteisesti on eräänlainen valtuutus puuttua henkilön itsemääräämisoikeuteen. Sen selvittäminen, missä laajuudessa edunvalvonta siihen vaikuttaa, on maistraatin tehtävä.

Maistraatti ei saa pyrkiä informoinnillaan vaikuttamaan edunvalvojaa itselleen harkitsevan henkilön päätöksentekoon. Oikeudellisessa viestinnässä puhutaan usein viestin vaikuttavuudesta. Tällöin on usein kysymys retoriikkaan eli puhetaitoon liittyvästä vaikuttavuudesta, jolla pyritään tiettyyn lopputulokseen esimerkiksi oikeudenkäynnissä. Tällaisen vaikuttavuuden tuominen henkilön kuulemiseen merkitsee asian käsittelyn luonteen muuttumista niin, ettei kysymys ole enää välttämättä aidosti oma–aloitteisesta hakemuksesta.[89] Maistraatin ei tule kuulemistilanteessa ottaa kantaa tarpeeseen eikä henkilön elämäntilanteeseen muutoinkaan, sillä hakemuksen oma–aloitteisuuden vaatimus ei välttämättä silloin toteudu. Henkilön on itsenäisesti ilman sitä edistävää myötävaikutusta tehtävä päätös hakemuksen tekemisestä ja hakemuksensa sisällöstä, jotta maistraatti olisi toimivaltainen sen käsittelemään. Kaikissa muissa tapauksissa toimivalta kuuluu käräjäoikeudelle. Viestinnässäkin on tunnistettava eri osapuolten asemat sekä niihin liittyvät

[87] Rynning: Samtycke till medicinsk vård och behandling (1994) s. 168
[88] Faden – Beauchamp: A History and Theory of Informed Consent (1986) s. 300–304
[89] Ks. retoriikasta ja viestinnän vaikuttavuudesta Mattila, Heikki E.S.: Vertaileva oikeuslingvistiikka (2002) s. 52–54

oikeudet ja velvollisuudet. Ilman kokonaisvaltaista prosessien tuntemusta se on hyvin hankalaa, jollei jopa mahdotonta.

6. Tietojärjestelmä oikeudellisen laadun ympäristönä

Informaatioteknologia ei ole pelkkä apuväline, vaan sen avulla voidaan luoda oikeudellisia ympäristöjä. Nykyinen informaatio– ja tietojärjestelmäriippuvainen yhteiskunta merkitsee yhä suurempaa tarvetta yhdistää oikeus ymmärrykseen informaation ja informaatioympäristön suhteesta, informaatioprosesseista ja informaatioteknologiasta.[90] Eräs esimerkki tästä on holhousasioiden rekisteri, jota maistraatit käyttävät edunvalvontaa koskevissa asioissa. Se on tässä mielessä tyypillinen informaatioyhteiskunnan digitaalinen työväline.[91] Huomio tulee kohdistaa tietojärjestelmässä käsiteltäviin ja siihen kerättäviin tietoihin, niiden elinkaareen, sekä erityisesti niihin vaikutuksiin, joita järjestelmällä on päämiehiin, heidän oikeuksiinsa ja jokapäiväiseen elämäänsä.

Tietojärjestelmä oikeudellisena ympäristönä tulee suunnitella oikeudellisesti. Informaatiota koskeva lainsäädäntö ohjaa informaatiovirtoja. Tämä ohjaus käsittää perusoikeuksien asettamat tiukat rajat.[92] Oikeudellisen suunnittelun tulee sijoittua tietojärjestelmäsuunnittelun alkuvaiheeseen, jossa vasta hahmotetaan, millaista informaatiota sisältävää järjestelmää ollaan rakentamassa.[93] Holhouskirjojen siirtäminen holhousasioiden rekisteriin tehtiin lainsäädännöllisesti mahdolliseksi holhoustoimilain säätämisellä vuonna 1999. Lainsäädännössä paalutettiin peruslähtökohdat siirrolle, mutta varsinaista suunnitelmaa siirron käytännön toteuttamisesta ei tehty. Holhoustoimilain 101 §:n mukaan maistraatin tuli ennen holhoustoimilain voimaantuloa siirtää holhousasioiden rekisteriin tiedot niistä holhouskirjaan merkityistä voimassa olevista holhouksista ja uskotun miehen toimista, joiden valvonta siirtyi maistraatille holhoustoimilain voimaantulon jälkeen. Holhouskirjaa pitävän käräjäoikeuden tuli huolehtia tarvittavien tietojen luovuttamisesta maistraatille ja vastata siitä, että luovutettavat tiedot olivat oikeat. Lisäksi käräjäoikeuden tuli tarkastaa tiedot holhouslautakunnan edustajan kanssa holhouksien vaarinpidosta sisältävän julistuksen (34/1898) 10 §:ssä tarkoitetulla tavalla.[94] Tarkempi suunnittelu olisi ollut ensiarvoisen tärkeää, koska holhouskirjojen merkinnöissä oli jo aiemmin todettu olleen puutteita. Alioikeudet eivät olleet riittävällä tavalla huolehtineet omien holhouskirjojensa ja holhouslautakunnan pitämien

[90] Pöysti: Communicational Quality of Law (2006) s. 465
[91] Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 284
[92] Bing: Information Law? (2004) p. 37
[93] Connolly – Begg: Database Systems (2005) s. 22
[94] HE 146/1998 vp. 76

holhouskirjojen yhdenmukaisuuden tarkastamisvelvollisuudesta.[95] Yhtä päämiestä koskevien merkintöjen kokoamista vaikeutti sekin, että holhouskirjoja oli pidetty aikajärjestyksessä. Itse tiedonsiirtoa hankaloitti kuitenkin holhouskirjojen pitämisessä käytettyjen lomakkeiden vanhanaikaisuus. Ne eivät soveltuneet edes järjestelmälliseen konekirjoitukseen.[96] Vaikka julkisuuslaki, jossa suunnitteluvelvollisuudesta säädetään, tuli voimaan samana päivänä kuin holhoustoimilakikin, näiden kahden lakimuutoksen vaikutukset toisiinsa olisi tullut kartoittaa valmisteluvaiheessa. Tietojärjestelmäsuunnittelun toteuttaminen laadukkaasti vaatii oikeudellista suunnittelua, joka sisältää myös tulossa olevien uudistusten selvittämisen ja niiden vaikutusten arvioimisen. Kysymys on lainsäädännöstä johtuvien velvoitteiden selvittämisestä ja tietojärjestelmän rakentamisesta niitä vastaavaksi. Julkisten tietojärjestelmien rakentamisessa tämä ei saa hämärtyä esimerkiksi siksi, että keskitytään vain tehokkuuden parantamiseen tai kuten holhouskirjojen kohdalla, pelkkään toiminnan tietotekniseen toteuttamiseen.[97] Laatu ei ole ominaisuus, joka voidaan lisätä järjestelmään sen jo valmistuttua, vaan se tulee rakentaa osaksi sitä.[98]

Holhousasioiden rekisteri on osa suomalaista valtakunnallista perusrekisteriä eli väestötietojärjestelmää. Perusrekistereillä tarkoitetaan yhteiskunnan perusyksiköt yksilöiviä tietojärjestelmiä. Perusrekisterit kuvaavat sekä perusyksikön tilan että tapahtumat, joissa tila on muuttunut. Perusyksiköitä ovat luonnolliset henkilöt, yhteisöt, rakennukset ja kiinteistöt.[99] Perusrekistereiksi luetaan henkilötietojärjestelmä, yritys–, yhteisö– ja säätiötietojärjestelmä, kiinteistötietojärjestelmä ja rakennustietojärjestelmä. Väestötietojärjestelmä ja holhousasioiden rekisteri ovat osa henkilötietojärjestelmää.[100]

Holhousasioiden rekisterinpidolle on kaksi tarkoitusta. Rekisterin avulla tehdään mahdolliseksi edunvalvojan toiminnan valvonta. Toisena tarkoituksena holhousasioiden rekisterille on kolmansien oikeuksien turvaaminen eli vähentää edunvalvontatilanteisiin liittyviä oikeustoimiriskejä.[101] Rekisterin avulla on mahdollista saada tieto siitä, kuka on tietyn

[95] Rautiala: Holhousoikeus (1952) p. 74. Ks. myös Välimäki: Edunvalvontaoikeus (2013) s. 193. Vanhan holhouslain aikainen järjestelmä oli vanhanaikainen ja hajanainen, sillä ulkopuolisen tahtoessa selvittää esimerkiksi sopimuskumppaninsa holhousoikeudellisen aseman, hänen täytyi selvittää asiaa sekä väestörekisteristä että paikallisesta alioikeudesta.
[96] Ks. Rautiala: Holhousoikeus (1952) p. 74 alaviite 132 ja Holhouslakitoimikunnan mietintö 1989:50 p. 53
[97] Ks. Magnusson–Sjöberg: Rättsautomation (1992) p. 479–480
[98] Berki – Georgiadou – Holcombe: Requirements Engineering and Process Modelling in Softwear Quality Management – Towards a Generic Process Metamodel (2004) p. 270
[99] Karimaa (toim.): Perustrekisterit (2001) p. 14–15, Valtion maksuperustelain seurantaprojektin loppuraportti (1996) Liite 3, p. 11, JUHTA 4/1996 p. 7 ja JUHTA 3/1997 p. 4
[100] Perusrekisterien palvelustrategia (2000) p. 9
[101] Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 284

henkilön laillinen edustaja tai onko henkilö kelpoinen tekemään käsillä olevan oikeustoimen.[102]

Mikä vaikutus rekisterillä on päämieheen? Holhoustoimesta annetun asetuksen 2 §:n mukaan holhousasioiden rekisteriin merkitään päämiestä koskevia tietoja: hänen nimensä, henkilötunnuksensa, osoitteensa, kotikuntansa ja tieto siitä, onko hänen toimintakelpoisuuttaan rajoitettu. Jo pelkkä merkintä holhousasioiden rekisteriin kertoo sen, että päämies on edunvalvonnassa eli siitä, että jonkinlaisia puutteita hänen toimintakyvyssään on. Se on rinnastettavissa tietoon sosiaalipalveluiden käytöstä, joka on Suomessa voimassa olevan henkilötietolain mukaan arkaluonteinen tieto.[103]

Toimintakelpoisuutta koskeva merkintä taas kertoo sen, missä määrin päämies voi itse hoitaa asioitaan. Holhoustoimilain 67 §:n mukaan jokaisen on mahdollista saada tieto siitä, onko henkilö edunvalvonnassa ja jos on, kuka hänen edunvalvojansa on ja mikä on hänen tehtävänsä. Se, ettei henkilöä ole merkitty edunvalvontaan määrätyksi, ei tarkoita, ettei henkilöllä voisi olla edunvalvojaa. Holhoustoimilain 65 §:n 2 momentin mukaan edunvalvontaa ei merkitä holhousasioiden rekisteriin, jos edunvalvojan tehtävä ei sisällä omaisuuden hoitamista tai oikeuden valvomista jakamattomassa kuolinpesässä. Esimerkiksi erityistä oikeustoimea varten määrätty edunvalvonta ei aiheuta merkintää holhousasioiden rekisteriin. Holhousasioiden rekisteriin tehty merkintä edunvalvonnasta ei tarkoita suoraan sitä, että henkilö ei voisi itse hoitaa asioitaan. Lähtökohta on, että vasta toimintakelpoisuuden rajoittaminen aiheuttaa muutoksia päämiehen rinnakkaiseen toimivaltaan edunvalvojan kanssa. Tosiasia kuitenkin on, että ne päämiehet, joiden toimintakelpoisuutta ei ole määräämisvaiheessa rajoitettu, muodostavat hyvin heterogeenisen ryhmän. Heidän tilanteensa vaihtelee täysin toimintakykyisistä, vain tukea tarvitsevista päämiehistä täysin dementoituneisiin vanhuksiin. Näin ollen heidänkään kohdalla ei voi tehdä selkeitä johtopäätöksiä pelkän holhousasioiden rekisteriin tehdyn merkinnän perusteella.

Holhousasioiden rekisteri on perustavanlaatuinen osa holhousviranomaisen informaatiojärjestelmää.[104] Sillä on kuitenkin merkittävä vaikutus myös rekisteröinnin kohteena oleviin henkilöihin eli päämiehiin. Edunvalvonnan merkitseminen holhousasioiden rekisteriin merkitsee tosiasiallisia vaikutuksia päämiehen itsemääräämisoikeuteen. Rekisterimerkinnän kautta erilaiset yksityiset palvelutarjoajat saavat tiedot edunvalvojan määräämisestä henkilölle. Yhtenä esimerkkinä ovat pankit, joille on rakennettu

[102] HE 146/1998 vp. p. 60
[103] Saarenpää: Henkilö– ja persoonallisuusoikeus (2012) s. 285
[104] Connolly – Begg: Database Systems (2005) s. 283

holhoustoimilakiin perustuva mahdollisuus puuttua tosiasiallisesti päämiehen toimintakelpoisuuteen, vaikka edunvalvojaa määrättäessä siihen ei olekaan puututtu. Holhoustoimilain 31 §:n 2 momentin mukaan edunvalvojan tulee ilmoittaa pankille, kuka tai ketkä saavat käyttää päämiehen tiliä. Tämän säännöksen perusteella pankki voi odottaa edunvalvojan ilmoitusta ja estää päämiestä käyttämästä tiliään ennen kuin on selvää, saako päämies itsekin esimerkiksi nostaa sieltä varoja. Säännöksen perusteluissa korostetaan päämiehen suojaamista varojen hukkaantumiselta.[105] Säännöksessä ei ole eritelty niitä tilanteita, joissa ilmoituksen tekeminen ei ole tarpeen, jolloin se tulee sovellettavaksi periaatteessa aina, kun edunvalvoja määrätään. Turhia rajoituksia päämiehen tilinkäyttöoikeuteen saattaa vähentää vuonna 2004 holhoustoimilakiin lisätty 64 §:n 5 momentti, jolla annettiin mahdollisuus saada tietoja holhousasioiden rekisteristä teknisen käyttöyhteyden avulla. Oikeus saada käyttöyhteys on sellaisella valtion tai kunnan viranomaiselle, yhteisölle tai elinkeinonharjoittajalle, joka toiminnassaan jatkuvasti tarvitsee rekisterin tietoja hyväksyttävää tarkoitusta varten. Ennen luovuttamista hakijan on esitettävä selvitys tietojen suojaamisesta.[106] Vaikka käyttöyhteyden kautta saatavat tiedot ovat holhoustoimilain 67 §:n 1 momentin mukaisia julkisia tietoja, käyttöyhteyden saajan on ymmärrettävä, että holhoustoimilain mukaisesti tietoja henkilön mahdollisesta edunvalvonnasta tulee tiedustella lähtökohtaisesti maistraatilta. Käyttöyhteyden tarkoituksena on palvella sen saaneen toimijan omaa toimintaa. Osana asianmukaista suojaamista käyttöyhteyden saajan tulee selvittää se, millä tavalla huolehditaan siitä, että tiedot ovat organisaatiossa vain työtehtävien perusteella niitä tarvitsevien työntekijöiden käytettävissä henkilötietolain 9 §:n mukaisen tarpeellisuusvaatimuksen mukaisesti.

7. Oikeudellisen laadun mittaaminen ja kehittäminen edunvalvonnassa

Oikeudellinen laatu edunvalvojaa määräämistä koskevassa asiassa voidaan tiivistää voimassaolevan oikeuden mukaiseksi menettelyksi, jossa koko prosessi toteutetaan yksilön oikeuksia optimaalisimmin toteuttavalla tavalla – ihmis– ja perusoikeusvelvoitteista laintulkintatapaa käyttäen.

Oikeudellisen laadun perusta on lainsäädännön laadussa. Edunvalvontaa koskevassa lainsäädännössä suurin oikeudelliseen laatuun liittyvä puute on ihmis– ja perusoikeusvaikutusten arvioinnin puuttuminen. Holhoustoimilain avulla puututaan yksilön itsemääräämisoikeuteen ja siksi laissa tehtyjä ratkaisuja tulee arvioida perusoikeuksien

[105] HE 146/1998 vp. P. 44
[106] Ks. lisäksi HE 123/2004 vp. p. 22

rajoitusedellytysten kautta. Suomalaisessa järjestelmässä tämä tarkoittaa käytännössä sitä, että eduskunnan perustuslakivaliokunta arvioi lain perusoikeusvaikutukset. Vuonna 1999 voimaan tullutta kokonaisuudistusta valmisteltaessa näin ei tehty.

Palvelun laadun mittaamisen yhtenä haasteena on kehittää mittaristosta sellainen, että se mittaa kaikkia olennaisia osa–alueita. Mittariston kehittämisessä riskinä on sen suppeus.[107] Näkökulman kapeus voi jättää esimerkiksi asiakkaiden kannalta tärkeitä asioita pimentoon, mutta myös oikeudelliset seikat voivat jäädä vähälle huomiolle. Määrällinen mittaaminen on jo yksi tulosjohtamisen välineistä. Käsittelyajat ovat tärkeitä hyvään hallintoon sisältyvän viivytyksettömän käsittelyn vaatimuksen kannalta, mutta niihin keskittyminen voi aiheuttaa sen, ettei palvelu vastaa niihin tarpeisiin, joita varten sitä tarjotaan.[108] Käsittelyn viivytyksettömyys on vain yksi hyvän hallinnon takeista. Huonosti toteutettuna viivytyksettömyys voi tarkoittaa selkeää oikeusturvariskiä.

Holhoustoimen palvelut asettavat laadun mittaamiselle ja seurannalle omat erityisvaatimuksensa jo siksi, että jokaisen asiakkaan tilanne aiheuttaa oman ainutlaatuisen informaatioprosessinsa. Jokainen tämän prosessin vaiheista tulee olla mittaamisen ja seurannan piirissä. Se tarkoittaa siten niin sisäisten prosessien kuin suoraan asiakkaaseen kohdistuvien tai asiakkaan kanssa tapahtuvien prosessien mittaamista. Keväällä 2003 toteutetussa holhoustoimen arvioinnissa tarkasteltiin holhoustoimen prosesseja holhoustoimilain uudistuksen toimivuuden valossa. Siinä asiakas nähtiin perinteisemmällä tavalla eli ulkoisina asiakkaina. Tässä roolissa olivat erilaisten sidosryhmien edustajat, kuten Nuoret lesket ry. ja Kehitysvammaisten tukiliitto.[109]

Holhoustoimen arviointi– tutkimuksessa näkyy vanhan holhouslain mukaiseen järjestelmään kuulunut asennemalli. Edunvalvojia pidetään päämiesten edustajina niin vahvasti, ettei holhoustoimen palvelujen arvioinnissakaan päämiesten mielipidettä tuoda muutoin esille. Päämies nähdään itseilmaisuun kyvyttömänä tai muutoin kyvyttömänä esittämään sellaista tietoa, jolla voisi olla relevanssia laadun mittaamisen ja seurannan osalta. Tältä osin tehtävä jää ylimpien laillisuusvalvojien ja tuomioistuinten tehtäväksi.

Päämiesten elämäntilanne ja yksilölliset ongelmat vaihtelevat suuresti. Päämies voi olla alaikäinen tai täysi–ikäinen, joka ei ymmärrä asioiden merkitystä eikä kykene olemaan kontaktissa ulkomaailman kanssa. Näiden väliin mahtuu kuitenkin joukko, joka on edelleen jollain tavalla kiinni arkipäivässä ja ymmärtää omasta parhaastaan jotakin. Erityisesti tällainen

[107] Gaster: Quality in Public Services. p. 2
[108] Gaster: Quality in Public Services. p. 51. *Gaster* korostaa tätä erityisesti osana *value for money*– ajattelua.
[109] Holhoustoimen arviointi. Liite 3.

tilanne on niiden päämiesten kohdalla, jotka ovat omatoimisesti hakeneet itselleen edunvalvojan. Päämiesten kokemukset edunvalvonnasta antaisivat hyödyllistä tietoa holhoustoimen palveluiden kehittämistä ajatellen ja pohdittavaa oikeudellisen laadun kannalta.

Aikuisten päämiesten kokemuksia ei ole selvitetty, mutta lasten kokemuksia lastensuojelussa käytettävästä edunvalvojasta selvitettiin Pelastakaa Lapset ry:n tekemässä selvityksessä.[110] Myös ikääntyneiden, muistisairaiden asiakkaiden elämänlaatua ympärivuorokautisessa hoidossa on tutkittu.[111] Päämiehiltä puuttuu kuitenkin kolmannen sektorin toimija, joka arvioisi edunvalvonnan toimivuutta päämiehen edun turvaajana. Erilaisissa tilanteissa oleville päämiehille on omat järjestösektorin toimijansa, mutta kaikkien päämiesten asiaa ajava järjestö Suomesta puuttuu. Tämä on varmasti yksi syy sille, miksi päämiehet jäävät huomiotta palvelujen laatua kehitettäessä. Päämiesten lisäksi muiden toimijoiden kokemuksia edunvalvonnasta tulisi selvittää. Näitä muita toimijoita ovat läheiset, henkilön toimintakyvystä lausuntoja antavat lääkärit, hoivakotien henkilökunta, sosiaalihuollon henkilökunta ja ulosottoviranomainen. Päämiesten, heidän läheistensä ja hoivakotien henkilökunnan mielipiteiden selvittäminen on erityisen tärkeää nyt, kun ostopalveluiden käytöstä edunvalvonnassa on käytännön kokemuksia. Julkisuuteen on jo tullut tietoja vakavista puutteista päämiesten asioiden hoidossa niissä tilanteissa, joissa oikeusaputoimisto on päätynyt kilpailutuksen kautta siirtämään edunvalvontojaan tarjouskilpailun voittaneelle palveluntarjoajalle.[112]

Palvelun laadun mittaamisessa lähtökohtana tulee pitää vähintään hyvän hallinnon perusteiden osa–alueiden mittaamista. Mitattaviksi tulevat hallintolain mukaisesti palvelujen asianmukaisuus, neuvonta, viranomaisen kielenkäyttö ja viranomaisten yhteistyö. Kaikkia näistä voidaan mitata maistraattien omilla arvioinneilla sekä päämiesten, läheisten ja muiden viranomaisten mielipiteitä selvittämällä. Palvelujen asianmukaisuuteen kuuluu sisällön lisäksi ympäristö, jossa palveluja annetaan ja se, miten palveluun pääsy on järjestetty. Tässä selvitys kohdistuu sekä maistraatin toimipisteessä annettavaan palveluun että sähköisenä tarjottaviin palveluihin. Kokonaisuutena arvioiden on kysymys palvelun vakuuttavuudesta, vastuullisuudesta, viestintätaidoista sekä halusta auttaa ja palvella asiakasta.[113] HAUS

[110] Laakso – Marjomaa – Peltoniemi (toim.): Edunvalvoja – se on minua varten (2012)
[111] Ks. Räsänen: Ikääntyneiden asiakkaiden elämänlaatu ympärivuorokautisessa hoivassa sekä hoivan ja johtamisen laadun merkitys sille (2011)
[112] Ks. ostopalveluista oikeusministeriön julkaisu Edunvalvonnan ostopalvelut oikeusaputoimistoissa, Mietintöjä ja lausuntoja 86/2010 s. 14
[113] Bergman – Klefsjö: Quality: From Customer Needs to Customer Satisfaction (2010) p. 329–331

kehittämiskeskus Oy:n tekemä Holhoustoimen arviointi keväällä 2003 sisälsi yhtenä tutkittavana osa–alueena viranomaisyhteistyön.[114]

Hyvän hallinnon osa–alueiden mittaamiseen tulee yhdistää informaatioprosessien toimivuus sekä ihmis– ja perusoikeuksien mukaisuus. Hallinnon sisäisesti toteutettu tutkimus ei riitä vaan tässäkin on otettava mukaan muut prosessissa mukana olevat tahot: terveydenhuolto, ulosotto, sosiaalipalvelut, edunvalvojaksi ehdotettu henkilö, päämies, päämiehen läheiset. Näin maistraattien on mahdollista tietoa esimerkiksi siitä, mitä kehitettävää on lausumapyyntöjen selkeydessä tai kuulemistilanteiden toteuttamisessa.

Oikeudellisten tulkintamenetelmien kehittäminen ei ole niinkään laadun mittaamisen kehittämistä vaan oikeudellisen laadun toteutumisesta huolehtimista laintulkinnassa ja –soveltamisessa. Edunvalvonnassa tulisi kehittää ihmis– ja perusoikeusvelvoitteista laintulkinta– ja soveltamismenetelmää. Ensi vaiheessaan tämä merkitsee näkökulman kääntämistä aidosti päämiehen etuun kaikissa edunvalvontaa koskevissa asioissa, myös hallinnon ja sen informaatioprosessien kehittämisessä.

Informaatioprosessit ovat osa palvelun laatua jo viestinnän kautta. Informaatioprosessien oikeudelliselle laadun mittaaminen erikseen on kuitenkin tarpeen. Suomalaisessa viranomaisympäristössä pohjan mittariston luomiselle saa henkilötietolaista ja julkisuuslaista. Henkilötietojen käsittelyn yleiset periaatteet ja julkisuuslain 18 §:n hyvä tiedonhallintatapa ovat erityisesti ne, joilla päästään käsiksi informaatiohallinnon oikeudelliseen laatuun. Yhtenä hyvänä mittarina voi käyttää henkilötietojen käsittelyyn luotuja käytännesääntöjä, joiden tekemiseen henkilötietolain tavoite itseohjautuvuuteen kannustaa. Hyvä tiedonhallintatapa perustuu riittävään suunnitteluun ja tilanteisiin varautumiseen. Se sitoo mukaan viranomaisessa käytettävän tietojärjestelmät. Ne ja niissä tehtävät muutokset tulee suunnitella, jolloin järjestelmäsuunnittelu ja siihen liittyvät oikeudelliset aspektit tulee integroida toisiinsa mahdollisimman aikaisessa vaiheessa.[115]

Kaikki alkaa ihmisestä ja kaikki päättyy ihmiseen. Jotta oikeudellinenkin laatu toteutuisi koko organisaation toiminnassa, koko organisaatio eli kaikki siellä työskentelevät ihmiset tulee saada sitoutumaan sen rakentamiseen. Esimerkiksi suomalaisessa tuottavuusohjelmassa on havaittu, ettei ministeriökeskeinen valmistelu ole onnistunut edistämään laitostason tuottavuutta parantavia toimia eli uudistamaan työjärjestelyjä ja –

[114] Holhoustoimen arviointi (2003) p. 20–22
[115] Magnusson –Sjöberg: Introduction to law in a digital environment (2005) p. 9 and Connolly – Begg: Database Systems (2005) p. 22 and 286

menetelmiä.[116] Myös tietojärjestelmäsuunnittelussa tulee ottaa mukaan yhteistyö eri alojen asiantuntijoiden välillä. Tähän lukeutuvat myös he, jotka tekevät joka päivä töitä näiden tietojärjestelmien varassa. He ovat oman työnsä ja tietojärjestelmävaikutusten asiantuntijoita, joihin oikeudellinen asiantuntemus ja tietojärjestelmäsuunnittelu tulee yhdistää. Näin esimerkiksi erilaisista käyttöä ohjaavista standardeista tai ohjeistuksista saadaan käytännössä toimivia, mutta myös lainsäädännön vaatimukset täyttäviä.[117] Tarvitaan motivoivia ja asenteita muokkaavia lähestymistapoja. Yksi näistä on se, että työntekijät ovat alusta asti mukana laatutyössä. Oikeudellisen laadun rakentaminen on aloitettava kokonaisuuden kartoittamisesta, jolloin jokaisen työntekijän aseman on tärkeä. Työnkuvan selvittäminen tapahtuu parhaiten kysymällä sitä henkilöltä, joka kysymyksessä olevaa työtä tekee. Näin pystytään selvittämään tiedon tie ja mahdolliset päällekkäisyydet työtehtävissä. Avain on oppimisessa, tiedon vaihdossa ja yhteisessä ratkaisujen etsimisessä. Parhaan tavan löytäminen näin sisältää demokraattisen virran, jossa johdon tehtäväksi sen arvioiminen, sopiiko valittu toimintatapa palvelun tarkoitukseen.[118] Oikeudellisesta laadusta puhuttaessa se tarkoittaa aina sen arvioimista, sopiiko se yksilön oikeuksille asetettuihin vaatimuksiin.

[116] Valtiontalouden tarkastuskertomus 9/2011 p. 8
[117] Connolly – Begg: Database Systems (2005) p. 286–287
[118] Stoker: Public Value Management – A New Narrative of Networked Governance (2006) p. 51–52

KANSAINVÄLISEN INFORMAATION TARPEEN JA SAANNIN MUUTOS YHTEISKUNNAN MUUTTUESSA VERKKOYHTEISKUNNAKSI

Tuulikki Mikkola

Professor Dr. of Law, University of Turku, tuulikki.mikkola@utu.fi

Abstract: *Cross–border legal relationships give rise to legal questions, which require a profound knowledge of the doctrines in the field of private international law. However, it is a challenging field, because it requires sound research skills in both substantive law and comparative law. Private international law – as a legal discipline within a system of municipal law – is an area to which comparative law is most logically and essentially linked. In this paper, my goal has been to produce knowledge about how the method of comparative law can be tapped in applying private international law and researching substantive law. Over the last years, information technology has made possible faster searches of global legal information. The result has been broader researching capabilities in the area of comparative law. However, in this paper I also try to warn readers of the numerous problems, which acquiring reliable comparative knowledge and comparative insights can entail.*

One should also note that procedural law has a key function in international civil proceedings. It determines how foreign law is ascertained in each system and it also sets the standard for evaluating the sufficiency of the proof provided. This is why I also focus on pleading and proof of foreign law in a court process. I explain the Finnish rules that determine the questions of to what extent and by which means a judge is allowed to examine the content of foreign law. I also explain whether the judge is obliged to apply conflict rules ex officio and what is party autonomy with regard to this issue. My conclusion is that contrary to what practice seems to be, Finnish courts should take comparative law more seriously since they must be able to truly access the laws of several nations.

1. Johdanto

Oikeudellinen informaatio ei rajaudu valtioiden rajojen mukaisesti, eikä sitä voi tällä tavoin aidata. Maailma kansainvälistyy kovaa vauhtia. Yhä useammalla yrityksellä ja yksityisellä henkilöllä on oikeudellisesti merkityksellisiä liittymiä ulkomaisiin oikeusjärjestelmiin. Nämä liittymät vaikuttavat kansainvälisen yksityisoikeuden säännösten välityksellä siihen, missä valtiossa tiettyyn oikeussuhteeseen liittyvä riitaisuus tulee ratkaista ja minkä valtion oikeutta soveltaen. Kolmanneksi kansainvälisen yksityisoikeuden soveltaminen antaa vastauksen siihen, millaiset oikeusvaikutukset vieraassa valtiossa annetulla

ratkaisulla on Suomessa. Joissakin tapauksissa on myös tärkeä ottaa selko siitä, millaiset oikeusvaikutukset suomalaisen viranomaisen ratkaisulla on ulkomailla.

Kansainväliset liittymät aktivoivat siten kansainvälisen yksityisoikeuden säännösten soveltamisen. Kansainvälinen yksityisoikeus on nimestään huolimatta kansallista oikeutta ja siksi oikeussuhteiden kokonaisvaltainen hallitseminen edellyttää, että lainsoveltaja joutuu perehtymään sekä kansallisiin että vieraan oikeusjärjestelmän kansainvälisen yksityisoikeuden alaan kuuluviin säännöksiin. Jos Suomen kansalainen esimerkiksi viettää pitkiä aikoja Espanjassa sijaitsevassa huoneistossaan ja palaa Suomeen vain kesäkuukausiksi, ei ole mitenkään selvää, että tämän henkilön perimykseen tulisivat sovellettavaksi suomalaiset perintökaaren säännökset tai että edes perinnönjako tulisi tehtäväksi Suomessa. Koska henkilöllä on tässä tapauksessa merkittäviä liittymiä asumisen ja omistuksen kautta Espanjaan, tulee lukuun ottaa myös se, miten Espanjassa on säännelty rajat ylittävät perimystilanteet. Jotta tätä koskevasta informaatiosta tehtävät johtopäätökset olisivat mahdollisimman oikeasuhtaiset, tulee lainsoveltajan kääntää näkökulma Espanjan oikeuteen ja tulkita Espanjan oikeuden yksittäisiä säännöksiä siten kuin niitä Espanjassa sovellettaisiin. Kysymys on oikeusvertailun perusideasta: siitä, että tulkintaympäristönä on säännösten kotijärjestelmä.

Kansainvälinen yksityisoikeus sisältää vahvoja siteitä oikeusvertailuun. Jos yksityisoikeudellisella oikeussuhteella on rajat ylittäviä liittymiä, tulee sen oikeusvaikutusten näkökulmasta ottaa lukuun kaikkien näiden valtioiden kansainvälisen yksityisoikeuden alaan kuuluvat säännökset. Vain yhdestä näkökulmasta tehtävä tarkastelu on epäammattimaista. Vaikka asia tulisikin ratkaistavaksi Suomessa ja Suomen oikeuden mukaan, tulevat vieraan valtion säännökset merkityksellisiksi viimeistään siinä tilanteessa, jossa tulee pohtia suomalaiselle ratkaisulle annettavia oikeusvaikutuksia ulkomaisissa oikeusjärjestelmissä. Kansainvälinen yksityisoikeus on siten välttämättä usein vertailun kohteena, jos henkilöllä tai hänen omaisuudellaan on tosiasiallisia liittymiä vieraisiin valtioihin.

Kansainvälisen yksityisoikeuden sidokset oikeusvertailuun näkyvät myös toisella tavalla. Jos lainvalintasäännökset osoittavat vieraan valtion oikeuteen, tulee suomalaisessa viranomaisessa/tuomioistuimessa ratkaistavana olevassa asiassa soveltaa vieraan valtion aineellisia säännöksiä. Vaatimukset, jotka vieraan valtion oikeudesta annetun informaation on näissä tapauksissa täytettävä, johdetaan kansainvälisen yksityisoikeuden yleisistä opeista. Vieraan oikeuden selvittäminen on sen sijaan oikeusvertailua.

Oikeudellinen viestintä ulottuu siten välttämättä kansallisvaltioita ja myös jopa EU:ta laajemmalle. Jos oikeaa oikeudellista viestiä on joskus vaikea löytää kansallisista lähteistä, on helppo ajatella, miten vaikeaa sen löytäminen on vieraan valtion oikeutta koskevista lähteistä.

Verkkoyhteiskuntaan siirtyminen epäilemättä on tuonut helpotusta siihen tilanteeseen verrattuna, jossa painetun informaation lukeminen oli lähes ainoa tie vieraan valtion oikeuden selvittämiseen. Kirjoittaessani 1990–luvulla väitöskirjaani, ei vieraan valtion oikeuden selvittämiseksi ollut muuta keinoa kuin matkustaa tutkimuksen kohteena olevaan valtioon ja tehdä selvittäminen käsityönä kirjallisia lähteitä ja haastatteluita hyväksi käyttäen. Oikeudellinen verkkoviestintä onkin avannut teoriassa nopean ja tasa–arvoisen tien vieraan valtion oikeuden selvittämiseen. Mutta vain teoriassa. Informaation haettavuus on näet sidoksissa haettavan oikeussäännöksen kotijärjestelmään, oikeuskulttuuriin ja oikeudelliseen systematiikkaan. Näitä vierasta oikeutta koskevan informaation haettavuuden haasteita käsittelen seuraavassa jaksossa.

2. Epäaidosta kuvailusta oikeasuhtaiseen tietoon

Digitaalisen toimintaympäristön yksi suurimmista haasteista – oikeusvertailun näkökulmasta – liittyy laatuun. Mistä kaiken keskenään ristiriitaisen informaation joukosta löytää laadullisesti kelvollisen materiaalin? Kaikki verkossa esiintyvä informaatio ei ole oikeaa, laadukasta tai ajantasaista. Siksi informaatiota on lähestyttävä kriittisesti ja niin, että kriittisyyden mittarit haetaan informaation kotisysteemistä. Jokainen oikeusjärjestelmä on omanlaisensa ja ilman siihen perehtymistä ei vieraan valtion oikeutta koskeva informaatio voi saavuttaa laadullista oikeasuhtaisuutta tai olla ymmärrettävää sellaiselle lukijalleen, jonka kotisysteemi on kohdesysteemistä eroava.

Oikeusvertailussa tavoitteena on aina oikeuden autenttinen, lojaali tulkitseminen. Tätä tavoitetta ei muuta se, että oikeusvertailussa vierasta oikeutta voidaan tarkastella usealta kantilta, riippuen siitä, mitkä ovat vertailulle asetetut funktiot. Vaikka kyse olisi vieraan oikeusjärjestelmän yksittäisen säännöksen selvittämisestä ja tulkitsemisesta, tai toisaalta vieraan oikeusjärjestelmän yleisten oppien selvittämisestä, on tavoitteena aina sisäisen näkökulman saavuttaminen. Informaatiota on lähestyttävä kuten sitä lähestyttäisiin kotijärjestelmässään. Lojaalin tulkitsemisen saavuttaminen voi jäädä puolitiehen, jos esitettävä aineisto on vain pintapuolista ja informaatio sirpalemaista – yksittäisten informaatiolähteiden esittelyä ilman, että aineistosta voisi saada kokonaiskuvan selvitettävänä olevasta oikeusjärjestyksestä. Kokonaiskuvan saamiseksi oikeusjärjestys on selvityksessä liitettävä oikeusjärjestelmään, yksittäiselle säännökselle on luotava konteksti.

Kun kontekstia haetaan, yksi tärkeimmistä huomioon otettavista tekijöistä on se, mitkä ovat oikeutta koskevat informaatiolähteet ja miten niitä on tulkittava. Suomessa on omanlaisensa oikeuslähdeoppi ja omanlaisensa tulkintametodit. Se, mikä asema

oikeuskäytännöllä on meillä oikeuslähteenä, ei kerro vielä mitään siitä, mikä asema tuomioistuinten ratkaisuilla on vieraissa oikeusjärjestelmissä. Lainsoveltajan olisi vierasta informaatiota etsiessään ja tulkitessaan irrottauduttava ajatuksesta, että voimassa olevan oikeuden sisältö ratkeaisi samojen lainalaisuuksien perusteella kuin Suomessa. Jo se voi yllättää, että oikeuden systematiikka, oikeudenalat ja käytetyt käsitteet voivat olla oikeusjärjestelmäkohtaiset. Oman oikeutemme käsite saattaa puuttua kokonaan vieraasta oikeudesta tai se saatetaan ymmärtää eri tavoin kuin Suomen oikeudessa. Yleinen väärinkäsitys vieraita oikeuskieliä luettaessa on se, että tietyn termin puuttuminen tarkoittaa myös vastaavan käsitteen puuttumista kyseisestä oikeudesta.[1] Käsitys ei pidä paikkaansa vaan edellyttää pintatason alle sukeltavan oikeusvertailun tekemistä. Oikeusvertailun kohteena olevaan järjestelmään perehtymällä voi selvitä, että suomalaista käsitettä vastaava käsite esiintyy vieraassa oikeudessa eri nimellä kuin Suomen oikeudessa. Ja sama toisinpäin: vaikka termi olisi sama, käsitteellisesti vieraan oikeuden instituutio voidaan ymmärtää hyvin eri tavoin kuin Suomen oikeudessa. Hyvänä esimerkkinä tästä on se, mitä katsotaan kuuluvan kiinteään omaisuuteen eri oikeusjärjestelmissä. Wolfgang Mincke onkin todennut sattuvasti, että käsitteet olisi ymmärrettävä erisnimien tavoin, koska niillä on oikeusjärjestelmäkohtainen merkitys. Jos tätä ei ota lukuun, muodostuu vierasta oikeutta koskevan informaation kokoamisesta – saatikka tulkitsemisesta – mahdoton tehtävä.

Toisaalta totta on sekin, että oikeusvertailun kautta autenttisten lopputulosten saavuttaminen on vaikeaa, jos ei suorastaan mahdotonta, koska yleensä lainsoveltaja pitää aina nenällään oman oikeusyhteisönsä silmälaseja: maailmankuva, kieli, kulttuuri, oikeusperinne vaikuttavat meissä vaikeuttaen vieraisiin oikeusjärjestyksiin tutustumista ja niiden säännösten soveltamista. Lopputulokseen vaikuttavien tekijöiden tiedostaminen ja huomioon ottaminen kuitenkin tekee oikeusvertailun tekemisestä aitoa, eikä jää luonteeltaan vain kuvailevaksi.[2] Kovin positiivisesti en suhtaudu tutkimuksiin, joissa on mukana vertailevaa aineistoa, mutta joissa kirjoittaja käyttää vastuuvapauslauseketta todeten, ettei tee ”aitoa” oikeusvertailua. Kuitenkin, aina kun tarkastelu siirretään vieraan valtion yhteenkin säännökseen, näkökulma on siirrettävä saman tien säännöksen kontekstiin. Tarkasteluun otettavien vieraan valtion säännösten vähäinen määrä ei tarkoita, että näkökulma voisi jäädä kansalliseksi ja vertailu täten ”epäaidoksi”.

[1] Termi on käsitteen ilmiasu ja käsite on ajatuksellinen abstraktio, josta ks. Mattila, Heikki E.S., Vertaileva oikeuslingvistiikka (2002) s. 170–171.
[2]Kuvailuun liittyy yleensä jollain tasolla pintapuolisuus ja samalla harhaanjohtavuus. Informaatiosta ei ole pääsyä tietoon, ks. Mikkola, Tuulikki, Oikeudellisen tiedon yhtenevyys ja sen esteet 1999 s. 379–387.

Tietoverkkojen merkitystä oikeudelliselle elämälle voidaan luonnollisesti pohtia yksilö tai yhteisötasolla. Yksilötasolla oikeus tietoon ja sen saamisen haasteet kietoutuvat kysymykseen yksilön itsemääräämisoikeudesta, kuten Ahti Saarenpää on usein kirjoittanut. Yksilötason lisäksi se, että tietoverkot ovat verkkoyhteiskuntamme arkipäivää, vaikuttaa – tai tämän tulisi vaikuttaa – myös viranomaisten ja tuomioistuinten toimintaan, ja siihen, miten ja millaista selvitystä rajat ylittävissä asioissa esitetään vieraan valtion oikeudesta.

3. Vieraan oikeuden selvittäminen käytännössä

Kansainvälisen yksityisoikeuden soveltamisen perusteella voidaan viranomaisessa tai tuomioistuimessa päätyä tilanteeseen, joissa asiassa sovellettaviksi *aineellisiksi* säännöksiksi tulevat vieraan valtion säännökset. Luonteva kysymys näissä tapauksissa on, kuka vieraan valtion oikeuden sisällön (tulkintaperiaatteineen) selvittää, millaista tämän selvityksen tulee olla (laatukysymys) ja mitä tapahtuu, jos esitetty selvitys ei ole riittävän laadukasta. Meillä on oikeudenkäymiskaaressa säännös (17:3), jossa osittain näihin kysymyksiin vastataan. Se kuuluu seuraavasti:

> Seikkaa, joka on yleisesti tunnettu tai jonka oikeus viran puolesta tietää, ei tarvitse toteen näyttää. Näyttö siitä, mitä laki säätää, ei myöskään ole tarpeen. Jos vieraan valtion lakia on sovellettava eikä oikeus tunne sen sisällystä, tulee oikeuden kehoittaa asianosaista esittämään siitä näyttöä.
>
> Jos määrätyn tapaukseen varalta on erikseen säädetty, että oikeuden tulee hankkia selvitys asiassa sovellettavan ulkomaan lain sisällyksestä, noudatettakoon sitä.
>
> Jos jossakin asiassa olisi sovellettava vieraan valtion lakia, mutta sen sisällyksestä ei saada selvitystä, on Suomen lakia sovellettava. (6.3.1998/165)

Oikeudenkäymiskaari asettaa siten lähtökohdaksi sen, että asianosaiset selvittävät vieraan valtion oikeuden sisällön. Tuomioistuin voi tältä osin jättäytyä passiiviseksi niin halutessaan. Sen tulee kuitenkin kontrolloida esitetyn selvityksen sisältö ja pohtia, onko selvityskynnys ylittynyt. Oikeudenkäymiskaaren mukaan näet voi syntyä tilanne, jossa vieraan valtion oikeudesta ei saada riittävää selkoa. Näissä tilanteissa voidaan soveltaa Suomen lakia ja sivuuttaa lainvalintasäännösten osoittama vieraan valtion oikeus. Oikeuskirjallisuudessa tätä on kutsuttu varaventtiililausekkeeksi.

Kun oikeudenkäymiskaaren 17:3 tulee sovellettavaksi, on tulkinnallisena lähtökohtana ja menettelyä ohjaavana perusperiaatteena oltava yksilön oikeusaseman. Lainvalinnalla on merkittävät seuraamukset nimenomaan asianosaisten oikeusaseman näkökulmasta.

Aineellisten lakien erotessa osin suurestikin toisistaan, on selvitystä koskevalla keskustelulla selkeä liityntä asianosaisten oikeusturvaan ja oikeudenmukaisen oikeudenkäynnin –käsitteeseen. Koska vieraan valtion oikeuden selvittämistä koskeva oikeudenkäymiskaaren säännös on suppea, on sen ymmärtämiseksi hyvä kääntää katseet muuhun oikeuslähdeaineistoon, ennakkoratkaisuihin ja oikeuskirjallisuuteen. Kirjallisuudessa vieraan valtion selvittämistä koskevaa problematiikkaa on käsitellyt itseni lisäksi Risto Koulu, joka on katsonut, ettei OK 17:3 ole kirjaimellisesti tulkittuna enää tätä päivää. Eikä olekaan. Esimerkiksi varaventtiililauseke säädettiin aivan eri maailmassa kuin millainen nykyinen verkkoyhteiskunta on. Selvitysvastuun sälyttäminen asianosaisen harteille on sekin ollut tietynlaisessa maailmassa tehty ratkaisu, jonka ajantasaisuutta lainsäätäjän tulisi miettiä vakavasti uudestaan. Tämä uudelleen miettiminen on tarpeen siksikin, että ennakkoratkaisujen tosiasiallinen käytännön merkitys on ollut kasvamaan päin. Ennakkoratkaisujen perusteella on kuitenkin valitettavasti mahdollista tehdä se johtopäätös, että vieraan valtion oikeuden selvittämiseen ei tarvitse suhtautua vakavasti. Toisaalta vierasta oikeutta koskevan informaation osalta voi asian ratkaisemiseksi kelvata vähäisempi oikeudellinen tieto kuin vastaavan kansallisen asian ratkaisemiseksi. Oikeudellisen lähdesyvyyden voi siten sivuuttaa, kun kyse on rajat ylittävistä asioista! Tällä on suora vaikutus kansalaisen oikeusturvaan ja oikeudenmukaisen oikeudenkäynnin toteutumiseen: ylenkatsova asenne vieraan valtion oikeuden selvittämistä kohtaan on kansalaisen perusoikeuksien vastaista.

Oikeuskirjallisuudessa on ehdotettu, että asianosaisten sijasta tai rinnalla tuomioistuimella tulisi olla aktiivinen rooli vieraan valtion oikeuden selvittämisessä. Vastaväite on tuttu, ja sitä on perusteltu resurssipulalla. Sillä, että tuomioistuimella tai viranomaisilla ei ole resursseja vieraan valtion oikeuden selvittämiseen. Väite ei ole pitävä, jos ajatellaan että tuomioistuimella on jo nyt rooli vierasta oikeutta koskevan informaation laadun ja oikeasuhtaisuuden kontrolloijana. Rooli edellyttää aktiivisuutta, vieraan oikeusjärjestelmän oma–aloitteista selvittämistä, jotta esitetyn informaation sisältö on vahvistettavissa. Tuomioistuimella on myös käytettävissään useita vaihtoehtoisia tapoja, joiden kautta informaatio olisi mahdollista saada. Jos tuomioistuin suhtautuu esitetyn informaation kontrollointiin vakavasti, en näkisi että selvitysvastuu asianosaisen rinnalla olisi mikään suuri työmäärän lisäys. Tiedän minulle kerrotun mukaisesti, että osassa tuomioistuimia tuomarit ovat ottaneet vieraan valtion oikeuden selvittämiseen hyvinkin aktiivisen roolin, joka osoittaa samalla, että vieraan valtion oikeutta koskevan informaation selvittämiseen suhtaudutaan vakavasti. Esimerkiksi Helsingin hovioikeuden päätös, joka koski ulkomaisen sijaissynnytysjärjestelyn vahvistamista Suomessa, osoitti perusteluidenkin tasolla, että

hovioikeus otti itse aktiivisen roolin vieraan oikeuden selvittämisen ja asianosaisten ja ulkoasianministeriön toimittaman selvityksen kontrollin suhteen (HelHO 2013:4). Tiedän myös, että useissa tapauksissa ensimmäisenä portaana tuomarilla on joku verkkosivusto, jonne on koottu vertailevaa tietoa tai linkkilistoja yksittäisten valtioiden lainsäädännöstä.

Kun tietoa haetaan tietyn oikeusjärjestelmän säännöksistä, tuohon järjestelmään sisälle pääsemiseksi olisi päästävä sisälle kohdejärjestelmän peruspalikoihin, järjestelmän rakenteisiin. Eurooppalaisittain hyvä ponnahduslauta tässä suhteessa on komission ylläpitämä Euroopan oikeusportaali (e–justice.europa.eu). Se pyrkii helpottamaan tiedon saantia EU:n jäsenvaltioiden oikeusjärjestelmistä. Sivusto on hyvä lähtökohta, mutta käytännössä riittämätön esimerkiksi tietyn vieraan säännöksen soveltamiseksi. Se edellyttää lisätiedon hankkimista kohdejärjestelmän tulkinnallisista perusperiaatteista. Yksittäisten oikeusalojen osalta maininnan ansaitsee eurooppalaisten notaarien työstämä verkkosivusto, jossa selostetaan eurooppalaisia perintöjärjestelmiä (www.successions–europe.eu). Tämäkin sivusto on oikeusvertailun näkökulmasta liian suppea ja siksi vain yksi kievari matkalla kohden vieraan valtion oikeuden todellista selvittämistä. Verkossa olevien sivustojen kautta voi – niiden puutteista tai muista ongelmista huolimatta – saada juonesta kiinni sillä tavoin, että oikeasuhtaisen informaation etsiminen helpottuu tai tehostuu. Kannattaa kuitenkin aina muistaa se, että lisäongelmia em. kaltaisten sivustojen osalta tuottavat yleensä laadultaan heikot käännökset, josta syystä alkuperäkielisen tekstin lukeminen on aina suositeltavaa.

Koska kieli on verkkomaailman ankkuri, voi kansainvälistä informaatiota etsivälle suositella myös sivustoa, joka kantaa nimeä InterActive Terminology for Europe (www.iate.eu). Se on **monikielinen termitietokanta,** jota käytetään Euroopan toimielimiin liittyvissä käännöksissä. IATE:n verkkosivustolla on **hakukone,** jolla voidaan etsiä kaikilla Euroopan unionin toimialoilla käytössä olevia termejä ja ilmauksia. Verkossa olevista, oikeusvertailijaa auttavista sanastoista voi tässä yhteydessä mainita vielä Euroopan oikeudellisen verkoston verkkosivustolla olevan sanaston sekä EUROVOC:in, joka on Euroopan unionin toiminta–alat kattava **monikielinen tesaurus** eli vastaavuussuhteita usealla kielellä ilmaiseva asiasanasto. On kuitenkin huomattava, että hakukoneiden tarkoituksenmukainen käyttö vaatii melko ammattimaista kohdekielen osaamista ja edellyttää myös oikeuskielen hallintaa. Oikeuskielen ymmärtäminen ja oikeusvertailevan työn loppuunsaattaminen edellyttää tietoa vertailun kohteena olevan järjestelmän keskeisistä rakenteista ja instituutioista, oikeudellisista toimijoista ja prosessijärjestelmästä. Heikki E.S. Mattila onkin korostanut oikeuslingvistiikan ja oikeusvertailun välistä tiivistä ja vuorovaikutteista suhdetta.

Tietoverkkojen lisääntymisestä huolimatta osa tuomioistuimista – korkein oikeus näiden muassa – on kuitenkin päätynyt ylläpitämään hyvinkin passiivista roolia vieraan valtion oikeuden osalta. Asianosaisten selvitys otetaan vastaan ja vapaan todistusteorian perusteella tuomioistuin on oikeutettu ratkaisemaan, minkä merkityksen selvitys asiassa saa. Risto Koulu on kirjoittanut jakautuvasta selvitystaakasta, joka tuntuu olevan eräs niistä argumentaatiomalleista, joita käytännössä on sovellettu. Jakautuva selvitystaakka tarkoittaa, että jos toinen asianosaisista esittää selvitystä vieraan valtion oikeudesta ja vastapuoli sen hyväksyy, tuomioistuin tekee asiaratkaisun esitettyyn aineistoon perustuen. Perusoikeuksien näkökulmasta on kuitenkin hämmentävää, että vierasta oikeutta pidetään sillä tavoin ”erityisenä oikeutena”, että sen osalta tuomioistuimen argumentaatio voi olla ”kevyempää” kuin kansallisen oikeuden osalta. Toisin sanoen, eikö epäoikeutta ole se, että kansallinen vastaava asia ratkaistaan raskaammalla tietoarsenaalilla kuin kansainväliseen informaatioon perustuva asia? Kirjaamisviranomaisessa tätä epäsuhtaa on sentään edes kahvipöytäkeskusteluissa pohdittu.

4. Johtopäätökset

Kun mietitään asianosaisten selvitysvelvollisuutta ja tuomioistuimen kontrollivelvollisuutta, tuntuu joskus siltä, että verkkoyhteiskunta on pikemminkin vienyt tiedon kauemmaksi sen etsijästä kuin tuonut lähemmäksi. Vieraan valtion oikeutta koskevan informaation osalta ongelma on selkeästi siinä, ettei oikeusvertailun perusoppeja hahmoteta tai ymmärretä. Oikeus tietoon on vain utopistinen haave, jos verkkomateriaalia ei osaa asettaa osaksi kontekstia. Osin ongelmat johtuvat siitä, että oikeusvertailu on – osin ansaitustikin – saanut teoreettisen näpertelyn leiman. Yksin teoreettinen käsitteillä kikkailu ei tuo vertailevan informaation lukemiseen välttämättä mitään apua. Kuitenkin, näkisin itse tämän niin, että oikeusvertailun lainalaisuudet ovat suhteellisen helposti ymmärrettävät, kunhan ne tulevat avatuiksi konkreettisten esimerkkien kautta. Näin suhtautuminen vieraan valtion oikeutta kohtaan voisi käydä luontevammaksi, jolloin samalla oikeusvertailun leimautuminen tieteelliseksi näpertelyksi ehkä unohtuisi. Samalla oikeuskirjallisuudessa näkyvät kommentit siitä, ettei kyse ole aidosta oikeusvertailusta vaan ”kevytvertailusta” jäisivät kirjallisuuden historiallisiksi dinosauruksiksi.

Erityisesti viranomaistoiminnassa ja tuomioistuinprosesseissa vieraan valtion oikeuden näkeminen jonain erityisenä oikeutena, johon suhtautuminen voi erota siitä, miten kansalliseen oikeuteen ja sitä koskevaan lähdesyvyyteen tulee ja voi suhtautua, on hyvin vaarallista. Kun joka vuosi rajat ylittävien liittymien määrä kasvaa, myös niiden tapausten määrä kasvaa, joissa

sovellettavaksi saattavat tulla vieraan oikeuden säännökset. Lainvalintasäännösten lisääntyvä merkitys luo suuremman tarpeen kansainvälisen informaation etsimiselle. Oikeusvertailu ei ole, eikä saa olla, teoreettista puuhastelua, vaan taito etsiä ja soveltaa vierasta oikeutta tavalla, joka ei eroa säännöksen kotijärjestelmän oikeudellisten toimijoiden tavasta tulkita oikeutta. Oikeusvertailevan informaation etsiminen tai tulkitseminen ei saisi johtaa miltään osin in casu –harkintaan viranomais– tai tuomioistuinprosesseissa. Ihmis– ja perusoikeuksiin asti ulottuva oikeus oikeudenmukaiseen oikeudenkäyntiin edellyttää, että otamme vieraan oikeuden (oikeusvertailua koskevien perusoppien) soveltamisen vakavasti niin oikeuskirjallisuuden kannanotoissa kuin käytännön ratkaisutoiminnassakin.

SUOMEN TIETOSUOJAVIRANOMAISET

Katsaus tietosuojavaltuutetun ja tietosuojalautakunnan historiaan, nykytilaan ja tulevaisuuteen

Juhana Riekkinen

Researcher, University of Lapland, Faculty of Law, juhana.riekkinen@ulapland.fi

I Johdanto

1. Tutkimuksen lähtökohdat

1.1 Taustaa

Henkilötietojen suoja ja sitä koskeva oikeudellinen sääntely eli tietosuoja ovat olleet jo hyvän aikaa ollut polttavia kysymyksiä, ja niiden merkityksen ei voida ennustaa ainakaan laskevan tulevaisuudessa. Päinvastoin, yhteiskunnan toimintojen siirtyessä entistä enemmän tietoverkkoihin on tietosuojan merkityksen jatkuva korostuminen helposti arvattavissa oleva kehityssuunta. Kehittynyt tietosuoja on verkkoyhteiskunnassa välttämättömyys.

Suomessakin, kuten ympäri maailmaa, henkilötietojen suojan merkityksen kasvu on tuonut mukanaan myös tarpeen säädellä aihetta ja valvoa sääntelyn noudattamista. Tietosuojalainsäädäntö ulottuu maassamme perustuslain (PL, 731/1999) tasolle. Keskeinen yleislaki on henkilötietolaki (HetiL, 523/1999), joka tuli voimaan 1.6.1999 korvaten ensimmäisen aihetta säädelleen yleislakimme, vuoden 1988 alusta voimaan tulleen henkilörekisterilain (HRekL, 471/1987). Tämän lisäksi tietosuojasta on annettu kasvava määrä erityislainsäädäntöä, josta tärkeimpinä esimerkkeinä voidaan mainita sähköisen viestinnän tietosuojalaki (SävTSL, 516/2004), laki yksityisyyden suojasta työelämässä (TYksL, 759/2004) ja luottotietolaki (LTL, 527/2007).

Henkilörekisterilain säätämisen yhteydessä perustettiin lakia valvoviksi viranomaisiksi tietosuojavaltuutettu ja tietosuojalautakunta, joista ensimmäinen aloitti toimintansa jo kaksi kuukautta ennen lain voimaantuloa ja jälkimmäinen piti järjestäytymiskokouksensa 7.12.1987. Näin Suomeen luotiin kaksitasoinen viranomaisvalvonnan organisaatio.[1] Viranomaisista tietosuojalautakunta oli sitovaa päätösvaltaa käyttävä elin, tietosuojavaltuutettu taas lähinnä ohjaava, neuvova ja valvova viranomainen, joka ei tehnyt sitovia päätöksiä.[2] Sittemmin henkilötietolain voimaantulon jälkeen myös tietosuojavaltuutettu tekee sitovia, valituskelpoisia päätöksiä tarkastusoikeus– ja virheenoikaisuasioissa henkilötietolain 40.2 §:n mukaisesti. Myös tietosuojalautakunnan toimivalta on kokenut muutoksen alkuperäisestä. Sen

[1] *Nurmi*, Tietosuojalautakunta toiselle vuosikymmenelle, Tietosuoja 4/1997 s. 7.
[2] TK 1987–1988 s. 9–10.

pääasiallinen tehtävä on edelleen sitovien päätösten tekeminen, mutta aiempaa harvemmissa asioissa.[3]

Vuotta 2013 sävyttivät paljastukset yksittäisiin kansalaisiin ulottuvasta, laajamittaisesta ja rajat ylittävästä verkkotiedustelusta sekä erilaisista tietomurroista. Tietosuoja ja tietoturva ovat nousseet entistäkin näkyvämmin otsikoihin myös Suomessa. Vaikka tietosuoja on keskustelunaiheena ehkä ajankohtaisempi kuin koskaan, se ei suinkaan ole enää uusi asia. Siksi sitä valvovien viranomaisten toiminnasta on jo kertynyt siinä määrin kokemuksia ja materiaalia, että niiden arviointi on sekä tarpeellista, mielenkiintoista että mahdollista. Tutkimuksen ensisijainen tarkoitus onkin tarkastella tietosuojavaltuutetun ja tietosuojalautakunnan toiminnan kehitystä niiden syntyhistoriasta nykyhetkeen. Myös tietosuojavaltuutettua tukeva asiantuntijaorganisaatio, tietosuojavaltuutetun toimisto, on tutkimuksen kohteena.

Tutkimus on osa professori *Ahti Saarenpään* johtamaa kansainvälistä NETSO–tutkimusprojektia (*Network Society as a Paradigm for Legal and Societal Thinking*).[4]

1.2 Tutkimuskysymykset ja rakenne

Tutkimuksen tavoitteena on selvittää, miten tietosuojaviranomaisten toiminta on kehittynyt niiden toiminnan alusta 80–luvulta nykyhetkeen eli 2010–luvulle saakka, erityisesti kun yhteiskunta ja oikeus ovat kokeneet sellaisia suuria muutoksia kuten tietoteknologian nopea kehitys, Internetin ja tietoverkkojen nousu, yleinen kansainvälistyminen, lainsäädännön määrän kasvaminen sekä perusoikeusajattelun korostuminen. Tarkastelu kohdistuu erityisesti siihen, millaisia kehityslinjoja on havaittavissa tietosuojavaltuutetun ja tietosuojavaltuutetun toimiston

1) asiamäärissä, ratkaisutoiminnassa ja sen painottumisessa;
2) viestinnässä sekä yleisohjaus– ja tiedotustoiminnassa;
3) sidosryhmäyhteistyössä ja käytännesääntöihin liittyvässä toiminnassa;
4) osallistumisessa pohjoismaiseen, eurooppalaiseen ja muuhun kansainväliseen yhteistyöhön; sekä
5) muussa toiminnassa.

Tietosuojalautakunnan suppeamman toimenkuvan vuoksi tutkimuksen tietosuojalautakuntaa koskevan osion tutkimuskysymykset painottuvat sen toiminnan keskeisimpään osaan eli ratkaisutoimintaan. Erityisesti tarkoitus on selvittää

[3] HE 96/1998 vp. Ks. myös Henkilötietojen käsittelyä koskeva lainsäädäntö muuttui 1.6.1999 lukien, Tietosuoja 2/1999 s. 13–14 sekä *Rantalankila*, Tietosuojalautakunnan toimivalta täsmentyi, Tietosuoja 2/1999 s. 38–41.
[4] http://www.ulapland.fi/Suomeksi/Yksikot/Oikeustieteiden_tiedekunta/Tutkimus_ja_jatko–opinnot/Instituutit/Oikeusinformatiikan_instituutti/NETSO–tutkimusprojekti_2010%E2%80%932013_%28englanniksi%29.iw3, viitattu 20.11.2013.

6) miten tietosuojalautakunnan rooli on muuttunut henkilötietolain voimaantulon aiheuttaman toimivallan muutoksen myötä;

7) miten tietosuojalautakunnan käsittelemien asioiden määrä on kehittynyt;

8) millaisia asioita on saatettu tietosuojalautakunnan käsiteltäväksi ja keiden toimesta; sekä

9) miten muutoksenhakuinstanssit ovat suhtautuneet tietosuojalautakunnan päätöksiin.

Tutkimuksen esitysjärjestys ja rakenne noudattelevat pääosin edellä kuvattua tutkimuskysymysten jaottelua. Kuten listasta ilmenee, tutkimuksen kohteena on nimenomaisesti suomalainen viranomaistoiminta, ei sen sijaan Suomen kansallisen eikä sen enempää EU:n tietosuojalainsäädännön sisältö. Johdanto–osan toiseen lukuun olen kuitenkin sisällyttänyt suppean, tutkimusta taustoittavan yleiskuvauksen henkilörekisterilain säätämiseen ja Suomen tietosuojaviranomaisten perustamiseen johtaneista tapahtumista sekä tietosuojalainsäädännön myöhemmästä kehityksestä.

Tutkimuksen II osa vastaa yllä mainittuja tutkimuskysymyksiä 1–5 ja koskee tietosuojavaltuutetun ja tietosuojavaltuutetun toimiston toimintaa. Tietosuojavaltuutettua koskevassa osassa tietosuojalautakuntaan liittyviä tietoja mainitaan vain ohimennen. Viittaukset tietosuojalautakunnan toimintaan ovat kuitenkin tarpeen, koska tietosuojaviranomaisten toiminta kietoutuu tiiviisti yhteen. Tutkimuksen III osa käsittelee tietosuojalautakuntaa ja vastaa siten tutkimuskysymyksiä 6–9. Laajuudeltaan tämä osa on II osaa suppeampi. Tämä on seurausta siitä, että tietosuojalautakunnan tehtävät ovat luonteeltaan huomattavasti tarkkarajaisemmat ja suppeammat kuin tietosuojavaltuutetun. Kummankin osan alussa on jakso, joka sisältää perustietoa muun muassa viranomaisten resursseista ja organisaatiosta. Tietosuojavaltuutetun toimiston osalta käsittelen resurssien käytön kehitystä myös eri toimintamuotoja käsittelevissä jaksoissa. Tutkimuksen IV osassa luon lyhyen, kokoavan yleiskatsauksen menneeseen ja tietosuojan viranomaisvalvontaa kohtaaviin tuleviin haasteisiin.

1.3 Tutkimusote, menetelmät ja aineisto

Tutkimuksen kohteena ei ole suoranaisesti oikeussäännösten sisältö, vaan tietosuojaviranomaisten toteutunut, reaalimaailmassa havainnoitavissa oleva toiminta niiden koko toiminta–aikana.[5] Tämän vuoksi tutkimus toteutettiin pääsääntöisesti empiiristä tutkimusotetta ja empirismin metodeja hyödyntäen.[6] Aineistoa analysoitiin sekä kvalitatiivisesti että kvantitatiivisesti, riippuen kunkin tutkimuskysymyksen asettamista vaatimuksista. Toisaalta tutkimuksessa voidaan tunnistaa selkeä historiallinen –

[5] Luonnollisesti tätä toimintaa on kuitenkin arvioitu olemassa oleva lainsäädännöllinen kehikko ja sen muutokset huomioiden.
[6] Empirismistä ja empiirisestä tiedosta oikeustieteessä yleisesti ks. esim. *Ervasti*, Eräitä näkökohtia empiirisen tiedon hyväksikäyttämisestä oikeustieteessä, LM 3/1998 s. 364–388.

oikeushistoriallinen – tiedonintressi ja sitä vastaava tutkimusote: pyrkimys kuvata muutosta, löytää käännekohtia ja selittää niiden syitä.[7]

Tutkimuksen keskeisimmän aineiston ja tietolähteen muodostivat tietosuojavaltuutetun vuosi– ja toimintakertomukset ja niihin sisältyvät toimintatilastot. Lisäksi tutkimuksessa tarkasteltiin tietosuojavaltuutetun toimiston julkista diaaria, toimiston tuottamia julkaisuja ja muuta kirjallista materiaalia, verkkosivuja[8], Tietosuoja–lehteä[9], tietosuojaa koskevaa lainvalmisteluaineistoa sekä jonkin verran oikeuskirjallisuutta. Erityisesti tietosuojalautakuntaa koskevaan aineistoon kuuluivat tietosuojalautakunnan päätökset ja päätöslyhennelmät sekä tietosuojalautakunnan pitkäaikaisen puheenjohtajan *Pekka Nurmen* haastattelu.[10]

Tutkimuksessa tarkasteltu materiaali on suurelta osin tutkimuksen kohteena olevien viranomaisten itsensä tuottamaa. Tämän voi nähdä aiheuttavan luotettavuusongelman: tutkija arvioi viranomaisen toimintaa viranomaisen itsensä tuottaman materiaalin perusteella. Tällaisessa tilanteessa tutkimusaineistoa on tarpeen tarkastella erityisen kriittisesti. Luonnollisesti kriittisesti on suhtauduttava kaikenlaisiin viranomaisten itsensä esittämiin laadullisiin arvioihin omasta toiminnastaan ja sen onnistuneisuudesta. Kuitenkaan kaikkien esimerkiksi toimintakertomuksissa esitettyjen fakta– ja tilastotietojen luotettavuutta ei ole mielekästä kyseenalaistaa. Olen tässä tutkimuksessa lähtenyt siitä, että viranomaismateriaalissa esitetyt fakta– ja tilastotiedot ovat lähtökohtaisesti luotettavia. Tietyissä erityistapauksissa tietojen epäjohdonmukaisuus, esittämistapa, esittämättä jättäminen taikka tilastoinnissa käytetyt metodit, luokittelut ja kategoriat herättävät epäilyksiä joko tiedon virheellisyydestä tai siitä, ettei se pohjaudu sellaiseen mittariin, joka on mielekäs sen asian tarkasteluun, jota tiedolla on tarkoitus kuvata. Näistä huomioista olen erikseen maininnut tutkimusraportissa.

Huomionarvoista on, että tutkimuskysymyksen 2 (tutkimusraportin II osan luku 3) osalta viranomaisten julkaisemat verkkosivut, Tietosuoja–lehti ja oppaat eivät olleet pelkästään kriittisesti tarkasteltavia informaatiolähteitä, vaan tutkimuskohde itsessään. Viestinnällisten materiaalien laatu ja niissä mahdollisesti olevat puutteet kertovat osaltaan siitä, miten tietosuojavaltuutetun toimisto on onnistunut tutkimuksen kohteena olevassa lakisääteisessä tiedotustehtävässään.

---

[7] Ks. *Jyränki*, Toiset työt, toiset metodit, teoksessa *Häyhä* (toim.), Minun metodini (1997) s. 81–83 sekä yleisesti *Kekkonen*, Oikeudellisen muutoksen tutkimisesta – minun metodini, teoksessa *Häyhä* (toim.), Minun metodini (1997) s. 131–150.

[8] http://www.tietosuoja.fi, viitattu 9.5.2014.

[9] http://www.tietosuoja–lehti.fi, viitattu 28.1.2014.

[10] Tutkimuksen alkuperäiseen suunnitelmaan kuului myös tietosuojavaltuutetun päätöksien ja kannanottojen tarkempi sisällöllinen analysointi, mitä ei kuitenkaan tutkimusekonomisista ja käytännöllisistä syistä pystytty toteuttamaan tässä yhteydessä. Tämä olisi vaatinut erityisesti valikoitua otosta tietosuojavaltuutetun ratkaisuista ja kannanotoista.

2. Yleistä tietosuojasta ja tietosuojaviranomaisista

2.1 Lyhyesti tietosuojan sääntelyhistoriasta

Tietosuojaa koskevat kysymykset nousivat esiin 1960–1970–lukujen taitteessa.[11] Ensimmäisenä tietosuojalakina maailmalla pidetään Saksan liittotasavallan Hessenin osavaltion tietosuojalakia (*Datenschutzgesetz*, hyväksytty 7.10.1970, voimaan 13.10.1970). Alun perin 17–pykäläisessä, vain osavaltion julkisia orgaaneja koskeneessa, nykynäkökulmasta varsin suppeassa laissa säädettiin myös lakia valvovasta asiamiehestä (*Datenschutzbeauftragte*).[12] Ensimmäinen valtakunnallinen tietosuojalaki oli soveltamisalaltaan laajempi, myös yksityisiä tahoja koskenut Ruotsin *datalag* (SFS 1973:289), jota valvomaan perustettiin *Datainspektionen*–virasto.[13] Lisäksi samana vuonna Ruotsissa hyväksyttiin luottotietoja koskeva erityislaki *kreditupplysningslag* (SFS 1973:1173). Näitä ja muita ns. ensimmäisen sukupolven tietosuojalakeja oli kuitenkin edeltänyt jo hivenen varhemmin alkanut kansainvälinen keskustelu ja selvitystyö.[14]

OECD:n piirissä tietosuoja–asioiden selvitystyö alkoi 1960–luvun lopussa, ja tuloksena oli vuonna 1980 hyväksytty tietosuoja–asioiden perusperiaatteita koskeva suositus[15]. Euroopan neuvostossa hyväksyttiin lähes samaan aikaan sisällöltään samansuuntainen tietosuojasopimus[16]. Sekä OECD:n suosituksen että tietosuojasopimuksen taustalla vaikuttivat Euroopan neuvoston asiantuntijakomitean valmistelemat suositukset tietosuojasta yksityisellä ja julkisella sektorilla vuosilta 1973 ja 1974.[17] Euroopan neuvosto on sittemmin antanut useita tietosuoja–asioita koskevia suosituksia muun muassa henkilötietojen käytöstä automaattisessa suoramarkkinoinnissa, poliisitoimen tietosuojasta, henkilötietojen keräämisestä työelämässä ja lääketieteellisten tietojen keräämisestä ja käsittelystä.[18] Tietosuojakysymykset olivat 1980–

[11] Syistä Suomessa ja maailmalla ks. *Korhonen*, Perusrekisterit ja tietosuoja (2003) s. 112, erityisesti av. 310.
[12] Koko Saksan liittotasavallan tietosuojalaki *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* hyväksyttiin 27.1.1977 ja tuli voimaan 1.1.1978. Nykyään useaan otteeseen muutettu laki tunnetaan nimellä *Bundesdatenschutzgesetz*. Muita 1970–luvulla hyväksyttyjä eurooppalaisia tietosuojalakeja olivat Tanskan *lov om private register m.v.* ja *lov om offentlige mydigheders registre* (1978), Norjan *lov om personregistre mm.* (1978), Itävallan *Datenschutzgesetz* (1978), Ranskan *loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (1978) ja Luxemburgin *loi réglementant l'utilisation des données nominatives dans les traitements informatiques* (1979).
[13] *Datalagin* ja Hessenin *Datenschutzgesetzin* välisistä lähtökohtaisista eroista ja muista *datalagin* esikuvista ks. *Söderlindh*, Personlig integritet som informationspolitik (2009) s. 206–208.
[14] Tietosuojalainsäädännön kansainvälisestä ja kansallisesta varhaishistoriasta tarkemmin ks. *Konstari*, Henkilörekisterilaki (1992) s. 3–9, 15–35, *Wallin – Nurmi*, Tietosuojalainsäädäntö (1991) s. 1–7, 16–20 ja *Korhonen*, Perusrekisterit ja tietosuoja (2003) s. 112–116. Tämä alaluku perustuu näihin lähteisiin niiltä osin, kun erikseen ei ole toisin mainittu. Tässä suppeassa esityksessä tavoitteena on antaa tiivis kuva lainsäädäntöhistorian vaiheista, ei niinkään tietosuojalainsäädännön sisällöllisestä kehityksestä.
[15] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data, 23.8.1980. Ks. myös KM 1981:66 s. 67–68.
[16] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (108/1981).
[17] KM 1980:66 s. 58.
[18] Tietosuojavaltuutetun toimiston sivuilla useat näistä suosituksista ovat saatavilla myös epävirallisina suomenkielisinä käännöksinä, ks.

luvun lopusta lähtien esillä myös YK:ssa.[19] Pohjoismaiden neuvostossa tietosuoja–asioita käsiteltiin 1970– ja 1980–luvulla useaan kertaan. Valtiokohtaiset tietosuojalait nähtiin kuitenkin yhtenäistä pohjoismaista lainsäädäntöä tai tietosuojakonventiota toteuttamiskelpoisempana ratkaisuna.[20]

Suomessa tietosuojaa koskevan kansallisen lainsäädännön valmistelu alkoi varsin varhaisessa vaiheessa, marraskuussa 1971. Tuolloin oikeusministeriö asetti kuusijäsenisen toimikunnan selvittämään aiheeseen liittyvää ongelmakokonaisuutta.[21] Toimikunnan tuli myös laatia ehdotus asian käsittelyä jatkamaan perustettavan komitean toimeksiannoksi.[22] Tietosuojatoimikunnaksi itseään kutsunut toimikunta antoi mietintönsä[23] maaliskuussa 1972. Tämän mietinnön pohjalta valtioneuvosto asetti saman vuoden toukokuussa huomattavasti laajemman komitean, joka nimesi itsensä tietojärjestelmäkomiteaksi.[24] Sen tehtävä oli tutkia tietojen hankintaa, tallentamista ja jakelua sekä yksilön persoonallisuuden suojaa ja oikeusturvaa.[25] Tietojärjestelmäkomitea julkaisi osamietinnön[26] vuonna 1974, mutta sen kesken jäänyt työ ei johtanut lainsäädäntötoimenpiteisiin. Komitea lakkautettiin poliittisista syistä toukokuussa 1975. 1970–luvun jälkipuolella oikeusministeriön marraskuussa 1976 asettama virkamiestyöryhmä (henkilörekisterityöryhmä) seurasi yksityisyyden suojaa koskevan lainsäädännön ulkomaista ja kansainvälistä valmistelua ja kehitystä.[27] Lisäksi työryhmän toimeksiantoon kuului laatia selvityksiä ja mahdollisuuksien mukaan valmistella säännöksiä yksityisyyden suojasta henkilörekistereissä.[28] Työryhmän väliraportti[29] ja siitä

http://www.tietosuoja.fi/fi/index/lait/kansainvalisetnormitjaohjeet/euroopanneuvostonantamiasuosituksia.html, viitattu 9.5.2014. Ks. myös KM 1981:66 s. 58–61 ja HE 96/1998 vp s. 13–15.

[19] Ks. esim. päätöslauselmat 44/132/1989 ja 45/95/1990 sekä jälkimmäisessä hyväksytty raportti E/CN.4/1990/72 (Revised version of the guidelines for the regulation of computerized personal data files prepared by Mr. Louis Joinet, Special Rapporteur).

[20] Ks. KM 1981:66 s. 48.

[21] Toimikunnan puheenjohtaja oli Matti Savolainen ja muina jäseninä toimivat Kettil Bruun, Heikki Immonen, Tuomas Kotovirta, Georg Luther ja Osmo A. Wiio. Sihteerinä toimi Timo Konstari. Lisäksi toimikunta kuuli lukuisia asiantuntijoita.

[22] Tarkalleen ottaen toimikunnan tehtävänä oli 1.3.1972 mennessä ”selvittää, minkälainen ongelmakokonaisuus liittyy yksityiseen ihmiseen, julkiseen toimintaan ja elinkeinoelämään kohdistuvaan tietojen hankintaan ottaen erityisesti huomioon yksityiselämän suojan sekä kehittyneet tiedonhankinta– ja tallennusmenetelmät; selvittää, minkälainen ongelmakokonaisuus liittyy hankittujen tietojen jakeluun ja luovuttamiseen kiinnittäen erityisesti huomiota yksityisen ihmisen oikeusturvaan; selvittää yleispiirteisesti ongelmaryhmien yhteyksiä jo säänneltyihin oikeusalueisiin; sekä laatia edellä mainittujen selvitysten pohjalta ehdotus asetettavan komitean toimeksiannoksi.” KM 1972:B 31 s. II.

[23] KM 1972:B 31.

[24] Komitean puheenjohtajaksi kutsuttiin Antero Jyränki ja muiksi jäseniksi Gunnar Asplund, Lars Bruun, Ilkka Hyppönen, Jouko Kajanoja, Teuvo Kallio, Timo Konstari, N. Seppo Koskinen, Simo Kärävä, Juha Partanen, Sylvester Perret, Ilkka Saraviita, Juhani Luukkonen ja tietosuojatoimikunnan puheenjohtajana toiminut Matti Savolainen. Lars Bruunin korvasi elokuussa 1972 Eila Hyppönen. Komiteaan kutsuttiin lisäksi joukko pysyviä asiantuntijoita. Yleissihteerinä toimi Jyrki Tala helmikuuhun 1973 saakka ja tämän jälkeen Elina Suominen, minkä lisäksi komitealla oli muitakin sihteereitä.

[25] KM 1974:110 s. 1.

[26] KM 1974:110.

[27] Työryhmän puheenjohtaja oli Kari Sinisalo ja muut jäsenet Matti Savolainen, Heikki Immonen, Martti Leistén, Juhani Pöyhönen ja Hannu Tulkki. Sihteerinä toimi Ilpo Virtanen.

[28] OMLJ 10/1978 s. 33.

[29] OMLJ 10/1978.

annetuista lausunnoista koostettu tiivistelmä[30] julkaistiin oikeusministeriön lainvalmisteluosaston julkaisusarjassa.[31]

Toukokuussa 1980 valtioneuvosto asetti uuden komitean (tietosuojakomitea), jolle se antoi tehtäväksi valmistaa hallituksen esityksen muotoon laaditun ehdotuksen henkilötietojen rekisteröinnissä noudatettaviksi säännöiksi.[32] Komitea jätti mietintönsä[33] oikeusministeriölle joulukuussa 1981. Lausuntokierroksen ja virkatyönä tehdyn jatkovalmistelun jälkeen hallituksen esitys henkilörekisterilaiksi ja siihen liittyviksi laeiksi[34] annettiin 30.4.1986. Esitys sisälsi henkilötietojen käsittelyä koskevan, henkilörekisterilaiksi nimetyn yleislain, tietosuojaviranomaisia koskevan lain nimeltä laki tietosuojalautakunnasta ja tietosuoja–asiamiehestä[35] sekä lait yleisten asiakirjain julkisuudesta annetun lain (83/1951), hallintomenettelylain (598/1982) 20 §:n ja leimaverolain (916/1983) 10 §:n muuttamisesta. Eduskunta hyväksyi esityksen vähäisin, lakivaliokunnan ehdottamin muutoksin 4.2.1987, ja tasavallan presidentti vahvisti hyväksytyt lait 30.4.1987 (471–475/1987). Samalla annettiin lakeihin liittyvät asetukset (476–477/1987).

Henkilörekisterilain periaatteet noudattivat melko suurelta osin tietosuojakomitean ehdotusta, mutta aiheen kiistanalaisuuden vuoksi pitkäksi venynyt jatkovalmistelu toi säännöksiin myös useita muutoksia. Laki koski sekä viranomaisten että yksityisten pitämiä, manuaalisia ja atk–pohjaisia rekistereitä. Sitä on kansainvälisessä katsannossa luonnehdittu ns. toisen polven tietosuojalaiksi.[36]

Henkilörekisterilakiin tehtiin sen yli kymmenen vuoden mittaisena voimassaoloaikana muutoksia kolmeen otteeseen. Lain 7 §:n 5 kohta kumottiin jo vuoden 1990 alusta nimikirjalain säätämisen yhteydessä (1011/1989, voimaan 1.1.1990). Merkittävämpi päivitys tehtiin vuonna 1994 (387/1994, voimaan 1.7.1994). Tällöin mm. tiedotusvälineiden toimitukselliset rekisterit rajattiin useimpien lain säännösten soveltamisalan ulkopuolelle, ja matrikkelien kokoamista ja sukututkimuksen tekemistä helpotettiin.[37] Samalla vanhat tietosuojalautakunnasta ja

---

[30] OMLJ 19/1977.
[31] 1970–luvun tietosuojaa koskevista oikeusministeriön julkaisuista ks. myös OMLJ 22/1975.
[32] Tietosuojakomitea oli kokoonpanoltaan lähes yhtä laaja kuin tietojärjestelmäkomitea. Sen puheenjohtajaksi valittiin Tapani Taskinen ja muiksi jäseniksi Heikki Immonen, Marjo–Riitta Lahelma, Ilmari Pietarinen, Aulis Pöyhönen, Kirsti Palanko–Laaka, Risto Rusama, Timo Silenti, Göran Strengell, Aimo Törn ja Heikki Varjo. Strengellin korvasi sittemmin Heikki Salmi. Päätoimisena sihteerinä toimi Kalervo Niskakoski. Myös tietosuojakomitea kuuli suurta joukkoa asiantuntijoita.
[33] KM 1981:66.
[34] HE 49/1986 vp.
[35] Hyväksytyn lain nimeksi tuli kuitenkin laki tietosuojalautakunnasta ja tietosuoja*valtuutetusta*.
[36] *Korhonen*, Perusrekisterit ja tietosuoja (2003) s. 114, *Konstari*, Henkilörekisterilaki (1992) s. 8 ja *Saarenpää*, Finland, teoksessa *Blume* (toim.), Nordic Data Protection Law (2001) s. 43.
[37] Ennen lainmuutosta etenkin matrikkeliasiat olivat tietosuojalautakunnassa usein esillä ja veivät paljon lautakunnan aikaa. Matrikkelirekistereitä tai vastaavia luetteloita koskevia tapauksia oli käsitelty lautakunnassa 22 kappaletta vuoden 1991 loppuun mennessä. Ks. *Konstari*, Henkilörekisterilaki (1992) s. 120–121. Sukututkimuksen kannalta on erikseen huomautettava, että niin henkilörekisterilain kuin nykyisen henkilötietolainkin on katsottu koskevan myös kuolleiden henkilöiden henkilötietoja, vaikka henkilötietodirektiivissä ei tällaista edellytetäkään eikä laissa nimenomaisesti säädetä kuolleiden henkilöiden

tietosuojavaltuutetusta annetut laki ja asetus korvattiin uusilla. Rikoslainsäädännön kokonaisuudistuksen yhteydessä henkilörekisterilakiinkin tehtiin muutos (630/1995, voimaan 1.9.1995), jonka myötä rangaistussäännöksiä uudistettiin ja siirrettiin rikoslakiin (39/1889).[38] Lakia täydentänyttä henkilörekisteriasetusta (476/1987) päivitettiin neljä kertaa vuosina 1987, 1988, 1993 ja 1994.

Henkilörekisterilain muutosten ohella merkittävänä henkilötietojen suojaa koskevana lainsäädännöllisenä tapahtumana voidaan pitää sitä, että vuoden 1995 perusoikeusuudistuksen yhteydessä laissa säädettävästä henkilötietojen suojasta otettiin maininta uuteen yksityiselämän suojaa koskevaan hallitusmuodon (94/1919) 8.1 §:ään (969/1995), joka sittemmin siirrettiin uuden perustuslain (731/1999) 10.1 §:ään.[39] Lisäksi 1990–luvulla eurooppalaisen yhteistyön merkitys tietosuoja–asioissa kasvoi. Suomi liittyi edellä mainittuun Euroopan neuvoston tietosuojasopimukseen vuonna 1992.[40] Euroopan unionin jäseneksi Suomi liittyi vuonna 1995, ja saman vuoden lokakuussa hyväksyttiin EU:n henkilötietodirektiivi (95/46/EY). Lainsäädännön sopeuttamista direktiiviin asetettiin pohtimaan henkilötietotoimikunta, jonka mietintö[41] valmistui vuonna 1997.[42] Hallituksen esitys henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi[43] annettiin jatkovalmistelun jälkeen seuraavana vuonna. Sen pohjalta direktiivi implementoitiin henkilörekisterilain korvanneella, 1.6.1999 voimaan tulleella henkilötietolailla ja muilla samassa yhteydessä hyväksytyillä laeilla (523–526/1999).[44] Implementointi tosin myöhästyi direktiivissä määrätystä aikataulusta.[45]

---

tiedoista. Ks. WP 29:n lausunto 4/2007 henkilötietojen käsitteestä (WP 136) s. 21. Ks. myös Helsingin HAO 8.12.2009 T 09/1083/3 (lainvoimainen), jossa kuolleiden nauttimaa suojaa kuitenkin tulkittiin hyvin suppeasti.

[38] Näistä muutoksista tarkemmin ks. HE 57/1989 vp, HE 311/1993 vp ja HE 94/1993 vp.

[39] Perusoikeusuudistuksesta ks. KM 1992:3 ja HE 309/1993 vp. Yksityiselämän suojaa koskevan perusoikeussäännöksen lisäämistä ei esitöissä juurikaan perusteltu, vaan säännöksen tarvetta pidettiin ilmeisesti itsestään selvänä. Vrt. Lissabonin sopimuksen myötä sitovaksi tulleen EU:n perusoikeuskirjan 8 artikla, jossa henkilötietojen suojasta on tehty nimenomainen ja yksityiselämän kunnioittamisesta (7 artikla) erillinen perusoikeus.

[40] Suomi allekirjoitti sopimuksen 10.4.1991 ja ratifioi sen 2.12.1991. Sopimus tuli voimaan Suomen osalta 1.4.1992. Kaikki sopimukseen liittyneet valtiot on listattu EN:n verkkosivuilla, ks. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG, viitattu 30.9.2013.

[41] KM 1997:9.

[42] Henkilötietotoimikunnan puheenjohtajana toimi tietosuojalautakunnan puheenjohtaja Pekka Nurmi. Jäseninä toimivat Synnöve Amberla, Timo Konstari, silloinen tietosuojavaltuutettu Jorma Kuopus, Hannu Rautiainen, Timo Räty, Ahti Saarenpää, Tuula Sario, Marja–Terttu Tyynelä ja Miliza Vasiljeff. Sihteereinä toimivat Leena Rantalankila, Jaana Mecklin ja Leena Vettenranta. Toimikunnan pysyvien asiantuntijoiden joukkoon lukeutui myös nykyinen tietosuojavaltuutettu Reijo Aarnio.

[43] HE 96/1998 vp.

[44] Hallituksen esitykseen sisältyivät lait tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain ja rikoslain 38 luvun 9 §:n muuttamisesta. Hallintovaliokunnan aloitteesta myös yleisten asiakirjain julkisuudesta annetun lain 18 a §:ää muutettiin, ks. HaVM 26/1998 vp.

[45] *Muttilainen*, Suomalaiset ja henkilötietojen suoja (2006) s. 8–9 ja *Korhonen*, Perusrekisterit ja tietosuoja (2003) s. 116. Direktiivin 32 artiklan 1 kohdan mukaan jäsenvaltioiden oli saatettava direktiivin soveltamiseksi tarvittavat lait, asetukset ja hallinnolliset määräykset voimaan viimeistään kolmen vuoden kuluttua sen hyväksymisestä. Direktiivi hyväksyttiin 24.10.1995, joten aikarajana oli 24.10.1998. Suomi ei suinkaan ollut ainoa myöhästyjä, ks. *Korhonen*, Perusrekisterit ja tietosuoja (2003) s. 94, av. 232.

Henkilörekisterilaki oli ja henkilötietolaki on *toissijainen yleislaki*. Tällainen laki tulee sovellettavaksi, kun muussa laissa ei asiasta toisin määrätä. Henkilötietoja koskevia erityissäännöksiä löytyykin suuresta joukosta muita lakeja. Erityislakien määrä oli huomattava jo ennen henkilötietolain säätämistä, ja merkittäviä uusia erityissäädöksiä ja –säännöksiä on annettu myös 2000–luvulla.[46] Usein kyse on yksittäisistä pykälistä, mutta lainsäädännöstämme löytyy myös lakeja, jotka sisältävät merkittävässä määrin tietosuojasäännöksiä. Tämänkaltaisia, nykyisin voimassa olevia lakeja ovat EU:n sähköisen viestinnän tietosuojadirektiivin (2002/58 EY) implementoinut sähköisen viestinnän tietosuojalaki, laki yksityisyyden suojasta työelämässä ja luottotietolaki. Näistä kaksi ensimmäistä koskevat kaikkia toimialoja, ja luottotietolaissa on kyse toimialakohtaisesta erityislaista. Näiden lakien suhde henkilötietolakiin käy ilmi viittaussäännöksistä, joissa todetaan, että henkilötietojen käsittelyyn sovelletaan henkilötietolakia, jollei kyseisessä laissa toisin säädetä (SävTSL 3.4 §, TYksL 2.3 § ja LTL 1.2 §).

Henkilötietolakiin nähden erityislaki on eräiltä osin myös julkisuuslaki (laki viranomaisten toiminnan julkisuudesta, 621/1999), joka määrittää henkilötietojen luovuttamista viranomaisten henkilörekistereistä. Lisäksi henkilötietojen käsittelyn kannalta merkityksellisiä ovat etenkin julkisuuslain tietojen salassapitoa koskevat säännökset (erityisesti 24 §) ja hyvää tiedonhallintotapaa määrittävä 18 §.[47] Julkisuuslaissa 11 ja 12 §:ssä säädetään myös erikseen asianosaisen tiedonsaantioikeudesta ja jokaiselle kuuluvasta oikeudesta saada tieto itseään koskevasta viranomaisen asiakirjasta. Henkilötietolain ja julkisuuslain välisen suhteen selventää henkilötietolain 8.4 §, jonka mukaan oikeudesta saada tieto ja muusta henkilötietojen luovuttamisesta viranomaisen henkilörekisteristä on voimassa, mitä viranomaisten asiakirjojen julkisuudesta säädetään.

Merkittävä erityislakien ryhmä ovat myös ns. rekisterilait, joissa kyseiseen rekisterinpitoon liittyvästä käsittelystä on säädetty kattavasti tai ainakin keskeisimmiltä osin. Näitä ovat esimerkiksi laki terveydenhuollon valtakunnallisista henkilörekistereistä (556/1989), rikosrekisterilaki (770/1993), laki henkilötietojen käsittelystä poliisitoimessa (761/2003), laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009) sekä laki arvo–osuusjärjestelmästä ja selvitystoiminnasta (749/2012).[48]

Lakien lisäksi on syytä huomata myös alemmantasoiset erityissäännökset ja ohjeet. Esimerkiksi tietosuojaan keskeisesti kuuluvasta tietoturvasta ei edelleenkään ole säädetty yleisesti lain tasolla, mutta tietoturvasta on kuitenkin annettu valtionhallintoa koskeva asetus

[46] Ks. HE 96/1998 vp s. 9.
[47] Tietojärjestelmien yhteensopivuutta turvannut 18 §:n 2 momentti tosin kumottiin vuonna 2011 samalla kun säädettiin laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011). Ks. HE 246/2010 vp s. 32.
[48] Erityislainsäädännöstä ks. myös http://www.tietosuoja.fi/fi/index/lait/erityislainsaadanto.html, viitattu 9.5.2014.

(valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 681/2010).[49] Lisäksi tietoturvan kannalta keskeisiä ovat Valtionhallinnon tietoturvallisuuden johtoryhmän eli VAHTI:n laatimat tietoturvaohjeet.[50]

Erityislainsäädännön runsaudesta ja moninaisuudesta huolimatta lainsäädäntöömme ei kuitenkaan sisälly yhtään erityislakia tai muutakaan erityissäännöstä, joka syrjäyttäisi kaikki henkilötietolain määräykset ja jonka rinnalla henkilötietolaki ei siten tulisi lainkaan sovellettavaksi.[51] Henkilötietolaki on siis kaiken henkilötietojen käsittelyn ehdoton lainsäädännöllinen perusta.

Henkilötietolakia itseään on päivitetty 2000–luvulla kuusi kertaa. Ensimmäinen muutoksen (986/2000, voimaan 1.12.2000) tarkoituksena oli ottaa henkilötietolain säännöksissä huomioon EU:n henkilötietodirektiivin mukainen komission päätöksenteko siitä, onko kolmannen maan tietosuojan taso riittävä tietojen siirtämistä varten. Lakiin lisättiin tällöin uusi 22 a § ja 23 §:n poikkeusperusteita muokattiin.[52] Toista muutosta (528/2007, voimaan 1.11.2007) saatiin odottaa vuoteen 2007, jolloin luottotietoja koskeva sääntely siirrettiin erilliseen luottotietolakiin.[53] Tämän lain voimaantulosäännöksen 2 momentti, joka jätti lailla kumotun 20.4 §:n osittain voimaan, kumottiin vajaata vuotta myöhemmin (lainmuutos 512/2008, voimaan 1.9.2008).[54] Neljäs muutos (294/2010, voimaan 1.5.2010) hyväksyttiin maksupalvelulain (290/2010) säätämisen yhteydessä, ja sen kohteena oli henkilötunnuksen käsittelyä koskeva 13 §.[55] Viidennellä muutoksella (1049/2010, voimaan 3.12.2010) kumottiin lain 2.4 §, jolla henkilötietolain soveltamisalan ulkopuolelle oli rajattu henkilörekisterit, jotka sisältävät vain tiedotusvälineessä julkaistua aineistoa sellaisenaan. Säännös oli Euroopan yhteisöjen tuomioistuimen ennakkoratkaisun ja Euroopan komission Suomelle antaman huomautuksen myötä todettu henkilötietodirektiivin vastaiseksi.[56] Kuudes ja viimeisin, luonteeltaan tekninen muutos (457/2011, voimaan 17.5.2011) liittyi syyttäjälaitoksen uudistukseen.[57]

Henkilötietolain muutokset ovat siis olleet pääasiassa varsin pieniä ja lakiteknisiä. Muutokset ovat johtuneet joko muiden lakien säätämisestä ja henkilötietolain yhteensovittamisesta niiden kanssa taikka EU–oikeuden vaatimuksista. Lain perusratkaisuihin ei sen yli 13 vuoden

[49] Tästä asetuksesta ks. myös VAHTI:n laatima Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010).
[50] Ks. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/, viitattu 29.4.2014.
[51] *Saarenpää*, Henkilö– ja persoonallisuusoikeus, teoksessa *Tammilehto* (toim.), Oikeusjärjestys. Osa 1 (2012) s. 329–330.
[52] Ks. HE 137/2000 vp.
[53] Ks. HE 241/2006 vp. Samalla lakiin tietosuojalautakunnasta ja tietosuojavaltuutetusta lisättiin maininnat luottotietolaista (lainmuutos 529/2007). Uuden lain valvonta annettiin tietosuojavaltuutetun tehtäväksi.
[54] Ks. HE 19/2008 vp.
[55] Ks. HE 169/2009 vp.
[56] Ks. HE 202/2010 vp, KHO 2007:9, KHO 2009:82 ja EYT:n tuomio 16.12.2008, C–73/07.
[57] Ks. HE 286/2010 vp. Sana ”virallisen” poistettiin HetiL 41 §:stä sanan ”syyttäjän” edeltä.

voimassaoloajan aikana ole ollut tarvetta puuttua, vaan henkilötietolaki näyttää teknologianeutraalisti kirjoitettuna yleislakina kestäneen aikaa melko hyvin, vaikka tietosuojaan liittyvät ilmiöt ja teknologia ovatkin kehittyneet.

Euroopan unionissa on tällä hetkellä käynnissä merkittävä tietosuojalainsäädännön uudistushanke. Komissio antoi tammikuussa 2012 ehdotuksen uudeksi yleiseksi tietosuoja–asetukseksi[58], joka korvaisi vanhan direktiivimuotoisen sääntelyn. Kokonaisuuteen liittyy myös uusi direktiivimuotoinen poliisi– ja rikosasioita koskeva ehdotus[59]. Koska uusi yleinen säädös olisi muodoltaan asetus, olisi se jäsenvaltioissa suoraan voimassaolevaa oikeutta. Sitä ei olisi tarvetta implementoida jäsenvaltioissa. Vaikkei tällainen asetus välttämättä tekisi kansallisia henkilötietojen käsittelyä koskevia yleislakeja tyystin tarpeettomiksi, vähentäisi se ainakin huomattavasti niiden merkitystä. Ehdotuksesta äänestettiin lokakuussa 2013 Euroopan parlamentin oikeus– ja sisäasioiden valiokunnassa, [60] ja maaliskuussa 2014 parlamentti äänesti selvin numeroin (621–10–22) uudistuksen puolesta. Parlamentin äänestyksessä hyväksymään kantaan sisältyy joitakin muutoksia komission ehdotukseen nähden, mutta uudistuksen pääpiirteet ovat ennallaan.[61]

2.2 Tietosuojaviranomaisia koskeva sääntely ja työnjako Suomessa

2.2.1 Organisaatiomallin valinta ja sääntelyn kehitys

OECD:n, Euroopan neuvoston, YK:n ja Pohjoismaiden neuvoston piirissä käydyissä varhaisissa keskusteluissa ja niiden tuloksena syntyneissä asiakirjoissa ei juurikaan otettu kantaa tietosuoja–asioiden viranomaisvalvonnan järjestämiseen tai tietosuojaviranomaisten organisaatioon, vaan asia jätettiin kansallisen lainsäädännön varaan.[62] Suomessa mielenkiinto ei kohdistunut asiaan aivan valmistelun alkuvaiheessa. Tietosuojatoimikunnan mietinnössä ja tietojärjestelmäkomitean osamietinnössä ei tarkasteltu viranomaisvalvonnan järjestämistä, mutta henkilörekisterityöryhmän väliraportti sisälsi jo huomioita viranomaisvalvonnan

[58] Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja–asetus). COM(2012) 11 final.
[59] Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta. COM(2012) 10 final.
[60] Ks. henkilötietodirektiivin 29 artiklan mukaisen työryhmän (WP 29) lehdistötiedote 22.10.2013. Saatavilla http://www.tietosuoja.fi/uploads/rz25k5ifyunkt8.pdf, viitattu 29.10.2013.
[61] Ks. Euroopan komission lehdistötiedote 12.3.2014 (Progress on EU data protection reform now irreversible following European Parliament vote, MEMO/14/186). Saatavilla http://europa.eu/rapid/press–release_MEMO–14–186_en.htm, viitattu 20.3.2014.
[62] Mainitulla YK:n päätöslauselmalla 45/95/1990 hyväksyttyjen ohjeiden kohdassa 8 kuitenkin edellytetään jokaisen maan asettavan viranomaisen valvomaan ohjeiden noudattamista. Ks. myös OECD:n tietosuojasuosituksen kohta 19 ja EN:n tietosuojasopimuksen valvontaviranomaisia koskeva lisäpöytäkirja (Strasbourg 8.11.2001), joka on Suomessa saatettu voimaan 1.11.2012 (SopS 77–79/2012).

järjestämisestä eri maissa.[63] Työryhmä myös pyysi lausunnonantajilta käsityksiä siitä, minkä mallin pohjalta viranomaisia koskevaa lainsäädäntöä olisi kehitettävä. Kolmena päävaihtoehtona nähtiin 1) henkilörekisteriviranomaisen perustaminen, 2) valvontatehtävien hajauttaminen niille organisaatioille, jotka huolehtivat muutoinkin asianomaisesta toiminnasta, ja 3) valvontatehtävien antaminen yleisille oikeudenhoidon viranomaisille. Eniten kannatusta sai hajauttamisvaihtoehto, ja vain noin neljänneksessä lausunnoista katsottiin tarpeelliseksi perustaa erityinen valvontaviranomainen.[64] Tämä lienee johtunut ainakin osittain siitä, ettei henkilötietojen käsittelyn merkitystä vielä ymmärretty tai haluttu ymmärtää.

Myös tietosuojakomitean mietinnössä pohdittiin viranomaisvalvonnan järjestämistä hajautetun tai keskitetyn mallin mukaisesti. Alueellisessa hajautuksessa henkilötietolainsäädäntöä koskevat tehtävät olisi annettu silloisille lääninhallituksille. Asiallisella hajautuksella tarkoitettiin mallia, jossa rekisterien valvonnasta ja muista ehdotetusta henkilörekisterilaista johtuvista tehtävistä olisivat huolehtineet ne toimielimet, jotka jo muutoinkin valvoivat kyseisten rekisterinpitäjien toimintaa. Alueellista hajautusta ei pidetty mahdollisena ehdotetun henkilörekisterilain soveltamisalan laajuuden vuoksi, ja asialliseen hajautukseen nähtiin liittyvän lukuisia ongelmia. Ongelmallista oli mm. löytää valvovaa viranomaista sellaisille yksityisille rekisterinpitäjille, joita mikään viranomainen ei valmiiksi valvonut. Muina ongelmina mainittiin viranomaisten omien rekisterien asema, soveltamiskäytännön yhdenmukaisuuden vaarantuminen, koordinoinnin vaatimat hallinnollinen lisätyö ja kustannukset sekä riittävän asiantuntemuksen turvaaminen. Niinpä komitea päätyi esittämään keskitettyä hallintomallia.[65]

Vaihtoehtoina tämän mallin sisällä oli tehtävien ohjaaminen oikeusministeriöön tai uudelle perustettavalle tietosuojaviranomaiselle. Komitean näkemyksen mukaan tehtävien antaminen oikeusministeriölle olisi joka tapauksessa vaatinut lautakuntatyyppisen asiantuntijaelimen perustamista oikeusministeriön yhteyteen. Lisäksi oikeusministeriön oma rekisterinpito nähtiin ongelmaksi. Komitea korosti myös sitä, että viranomaisen on oltava yleisesti tunnettu, helposti lähestyttävä ja asiantunteva.[66] Niinpä komitean ehdotukseksi tuli järjestää tarvittava henkilöstö erilliseksi, oikeusministeriön hallinnonalalla toimivaksi tietosuojaviranomaiseksi. Erityisemmin asiaa perustelematta komitean ehdotuksessa päädyttiin kaksijakoiseen viranomaiseen, jonka olisivat muodostaneet tietosuojalautakunta ja tietosuoja–asiamies. Ehdotettu ratkaisu poikkesi mietinnön ulkomaista oikeutta koskevassa katsauksessa esitellyistä viranomaisvalvonnan organisaatiomalleista.[67] Ensisijaisesti valitun linjan taustalla olivatkin

[63] Ks. OMLJ 10/1978 s. 4 (Ruotsi), 8–9 (Tanska), 11 (Norja), 13–14 (Saksan liittotasavalta), 16 (Itävalta), 18 (Hollanti), 19–20 (Belgia), 20–21 (Ranska), 22 (Espanja), 25 (Kanada ja Englanti).
[64] OMLJ 19/1977 s. 53–62.
[65] KM 1981:66 s. 39–43. Yhdessä kolmesta mietintöön jätetystä eriävässä mielipiteessä esitettiin että erillisten, keskitettyjen valvontaviranomaisten perustamisesta voitaisiin kokonaan luopua, tai että perustettavilla viranomaisilla tulisi olla ainoastaan ohjaava ja neuvova luonne, ks. KM 1981:66 s. 174–176.
[66] KM 1981:66 s. 43–44.
[67] Ks. KM 1981:66 s. 48–70.

ilmeisesti kotimaiset viranomaismallit kirjanpidon ja kuluttajansuojan saralla.[68] Vuonna 1974 voimaan tulleessa kirjanpitolaissa oli perustettu kirjanpitolautakunta, jonka päätehtävä oli varsin samankaltainen kuin tietosuojalautakunnalla: antaa ohjeita ja lausuntoja kirjanpitolain soveltamisesta sekä myöntää eräissä tapauksissa poikkeuksia ja lupia.[69] Kuluttajansuojassa taas oli vuonna 1978 omaksuttu malli, jossa viranomaiskoneiston ytimen muodostivat kuluttajavalituslautakunta (nykyisin kuluttajariitalautakunta) ja kuluttaja–asiamies.[70] Kuluttajavalituslautakunta ei tosin tehnyt sitovia päätöksiä, vaan sen ratkaisut olivat luonteeltaan suosituksia, kuten nykyisen kuluttajariitalautakunnankin. Identtisestä mallista ei siis ollut kyse kummassakaan tapauksessa.

Komitean ehdotuksen mukaan tietosuoja–asiamiehen tehtävänä olisi ollut seurata, valvoa ja ohjata henkilörekisterien perustamista, pitämistä ja siinä olevien tietojen luovutusta. Tietosuoja–asiamiehen toiminnan luonteen oli tarkoitus suuntautua henkilörekisterilain vastaisen menettelyn lopettamiseen ja ennaltaehkäisemiseen. Tietosuoja–asiamiehen tehtävien ei katsottu välttämättä vaativan oikeustieteellistä tutkintoa, koska hänen tehtäviinsä ei sisältynyt päätöksentekoa.[71] Lainvastaiseen menettelyyn hänen oli tarkoitus reagoida ensisijaisesti ohjaavasti tai neuvovasti taikka saattamalla asia tietosuojalautakunnalle tai syytteeseen panoa varten. Komitean käsityksen mukaan tietosuoja–asiamiehellä olisi tullut olla toimisto, jossa olisi ollut tarpeellinen määrä esittelijöitä ja muita henkilökuntaa. Vähimmäismääräksi arvioitiin kuusi virkaa tai tointa, joista yksi tai kaksi olisivat olleet varattuja toimistohenkilöille.[72]

Tietosuojalautakunnan rooliksi komitea taas suunnitteli velvoitteista ja kielloista päättämistä. Palkkioperusteisesti toimivan lautakunnan kokoonpanoksi ehdotettiin puheenjohtajaa ja kuutta jäsentä. Puheenjohtajalta olisi edellytetty henkilörekisteriasioihin perehtyneisyyden lisäksi oikeustieteen kandidaatin tutkintoa, ja jäsenten olisi tullut edustaa tasapuolisesti rekisteröityjen ja rekisterinpitäjien näkemyksiä.[73] Yhteensä viranomaisorganisaation kustannuksiksi arvioitiin noin 900 000 – 950 000 markkaa vuodessa.[74]

Tietosuojakomitean mietinnöstä hankituissa lausunnoissa ehdotettu malli kohtasi edelleen vastustusta, ja hajautetulla mallilla oli vieläkin kannattajansa. Talouselämän järjestöt jopa totesivat, että komitea oli ”selvästikin yliarvioinut tietosuojakysymyksiä koskevan asiantuntemuksen merkityksen”. Useat tahot myös katsoivat, että organisaatiokysymystä oli

[68] Tietosuojavaltuutettu Reijo Aarnion haastattelu, 5.5.2014, Helsinki, ja Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki.
[69] Ks. kirjanpitolaki (655/1973) ja asetus kirjanpitolautakunnasta (784/1973).
[70] Ks. kuluttajansuojalaki (38/1978), laki kuluttaja–asiamiehestä (40/1978) ja laki kuluttajavalituslautakunnasta (42/1978).
[71] Vrt. OMLJ 10/1982 s. 95.
[72] KM 1981:66 s. 46.
[73] KM 1981:66 s. 123–125.
[74] KM 1981:66 s. 47.

tarkemmin selvitettävä, ja toiset epäilivät ehdotettujen resurssien riittävyyttä. Enemmistö lausunnonantajista kuitenkin kannatti komitean ehdottamaa mallia ainakin periaatteessa.[75]

Pitkälti tietosuojakomitean mietinnössä esitetyn kaltainen viranomaismalli omaksuttiin sittemmin hallituksen esityksessä henkilörekisterilaiksi ja siihen liittyviksi laeiksi[76]. Viranomaisia koskevaa säätelyä oli kylläkin hienosäädetty. Esimerkiksi tietosuoja–asiamieheltä vaadittiin nyt oikeustieteellistä tutkintoa.[77]

Myös hallituksen esitykseen sisältyi katsaus ulkomaiseen lainsäädäntöön. Katsauksen varsinaisina kohteina olivat Ruotsi, Norja, Tanska, Saksa ja Ranska, ja siinä käytiin läpi myös viranomaisvalvonnan järjestäminen näissä maissa. Huomiota kiinnitettiin tietosuoja–asioista vastaavien viranomaisten kokoonpanoon ja tehtäviin.[78] Kaikissa mainituissa maissa toimi tietosuoja–asioihin erikoistunut viranomainen tai viranomaisia.[79] Erityisviranomaisen perustamisen välttämättömyyttä perusteltiinkin muiden maiden ratkaisuilla.[80] Missään mainituista maista viranomaisvalvontaa ei kuitenkaan ollut järjestetty siten, että viranomaisina olisivat toimineet valvova, ohjaava ja neuvova asiamies sekä päätösvaltaa käyttävä lautakunta. Kuluttajaoikeudesta ja kirjanpitolaista lainattu viranomaismalli oli siis tuolloin – ja on mitä ilmeisimmin edelleenkin – varsin ainutlaatuinen tietosuojan saralla.

Lisäperusteena valitulle mallille oli epäilemättä myös ajatus siitä, että haluttiin välttää kaiken tietosuoja–asioihin liittyvän vallan jääminen yksiin käsiin. Asiamies ja lautakunta nähtiin toisiaan tasapainottavina instituutioina.[81] Tasapainottamisajattelu on käytännössä heijastunut myös lautakunnan sisällä sen kokoonpanoon ja jäsenvalintoihin, vaikka eri intressiryhmille ei määrätty laissa nimenomaista edustusta tai kiintiöjäseniä.[82]

Hallituksen esitys sisälsi myös karkeat arviot viranomaisten odotetuista työmääristä. Tietosuoja–asiamiehen toimiston resurssien määrittelyssä lähtökohtana oli arvio noin 200 vuosittaisesta ilmoituksesta, 250 kertaluonteisesta ilmoituksesta ja 50 vuosittaisesta tarkastuksesta. Näiden lukujen katsottiin edellyttävän yhdeksän viran perustamista: yhdet toimistopäällikön, ylitarkastajan ja esittelijän virat sekä kaksi tarkastajan virkaa ja neljä virkaa toimistotehtäviä varten. Palkkamenoissa näiden ja tietosuojalautakunnan sihteerin viran arvioitiin tarkoittavan vajaata 1,2 miljoonaa markkaa vuosittain. Tietosuojalautakunnan vireille tulevien asioiden määräksi ennakoitiin vajaata sataa, ja palkkioihin arvioitiin kuluvan noin

[75] OMLJ 10/1982 s. 88–94.
[76] HE 49/1986 vp.
[77] HE 49/1986 vp s. 61.
[78] HE 49/1986 vp s. 88–97 (liite 4). Muiden kuin mainittujen maiden tietosuojalainsäädäntöä käsittelevässä lyhyessä kappaleessa ei käsitelty viranomaisvalvontaa.
[79] Ruotsissa Datainspektionen, Norjassa Datatilsynet, Tanskassa Registertilsynet, Saksassa liittovaltion sekä osavaltioiden tietosuojavaltuutetut ja Ranskassa 17–jäseninen automaattisen tietojenkäsittelyn ja vapauksien komissio.
[80] HE 49/1986 vp s. 17.
[81] Tietosuojavaltuutettu Reijo Aarnion haastattelu, 5.5.2014, Helsinki.
[82] Ks. III.1.

150 000 markkaa vuodessa. Jälkikäteen on helppo todeta, etteivät arviot olleet kovinkaan tarkkoja. Tietosuojavaltuutetun toimiston henkilöstötarve ja kustannukset kasvoivat nopeasti arvioita suuremmiksi, ja toisaalta ilmoituksia ei alkuvuosina saapunut ennakoitua määrää eikä tarkastuksien määrässä ylletty hallituksen esityksen lukemiin. Lautakunnan käsittelemät asiamäärät osoittautuivat todellisuudessa huomattavasti etukäteisarviota pienemmiksi.[83]

Hallituksen esitys hyväksyttiin, kuten jo edellisestä alaluvusta käy ilmi, eräin vähäisin muutoksin. Muutoksista epäilemättä näkyvin koski toisen viranomaisen nimikettä: vielä hallituksen esityksessä puhuttiin tietosuoja–asiamiehestä, mutta nimike muuttui valiokuntakäsittelyn jälkeen tietosuoja*valtuutetuksi*. Niinpä myös ehdotetut säädösnimet muuttuivat, ja henkilörekisterilain yhteydessä hyväksyttiinkin laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (TSL–TSVL–1987, 474/1987) ja annettiin sitä täydentävä asetus tietosuojalautakunnasta ja tietosuojavaltuutetusta (TSL–TSVA–1987, 477/1987). Viranomaisia koskeneet laki ja asetus tulivat pääosin voimaan 1.10.1987, siis kolme kuukautta ennen henkilörekisterilain voimaantuloa. Lyhyt, 12 pykälää kattanut laki sisälsi säännökset tietosuojalautakunnan kokoonpanosta, tehtävistä ja päätösvaltaisuudesta, jäsenten kelpoisuusvaatimuksista ja virkavastuusta sekä tietosuojavaltuutetun kelpoisuusvaatimuksista, nimittämisestä ja toimiston esittelijöistä. Lisäksi laissa oli säännökset tietosuojaviranomaisten oikeudesta pyytää lausuntoja, poliisin velvollisuudesta antaa virka–apua ja tietosuojaviranomaisten salassapitovelvollisuudesta. Lakia täydentänyt asetus sisälsi tarkemmat säännökset viranomaisten tehtävistä, asioiden käsittelystä, kelpoisuusehdoista, virkojen ja tehtävien täyttämisestä, palkkioista ja eräistä muista seikoista.

Vaikka tietosuojavaltuutetun nimike muuttui, kelpoisuusvaatimukset ja tehtävä pysyivät lopullisessa laissa ennallaan. Häneltä vaadittiin oikeustieteellistä tutkintoa ja hyvää perehtyneisyyttä tietosuoja–asioihin (TSL–TSVL–1987 6.1 §).[84] Lain tasolla tietosuojavaltuutetun tehtävät määritettiin vain hyvin yleisellä tasolla. Tietosuojavaltuutetun tehtävänä oli ratkaista ne asiat, jotka henkilörekisterilain mukaan kuuluivat hänen päätettävikseen, sekä seurata, valvoa ja ohjata henkilötietojen keräämistä ja tallettamista henkilörekistereihin, henkilörekisterien käyttöä ja suojaamista sekä rekisterissä olevien tietojen luovutusta (7 §). Tarkemmin tehtävistä säädettiin lakia täydentävän asetuksen 2 §:ssä, jonka sanamuotoja oli jonkin verran täsmennetty hallituksen esityksen liitteenä olleesta asetusluonnoksesta.[85]

Tietosuojalautakunnan kokoonpanoksi tuli esitetyn mukaisesti puheenjohtaja, varapuheenjohtaja ja viisi jäsentä. Puheenjohtajalta, varapuheenjohtajalta ja yhdeltä jäseneltä sekä tämän varajäseneltä edellytettiin oikeustieteellistä tutkintoa ja kahdelta jäseneltä sekä

[83] HE 49/1986 vp s. 18. Ks. II.2.2, II.6.1 ja III.3.
[84] Ks. HE 49/1986 vp s. 61.
[85] Ks. ja vrt. HE 49/1986 vp s. 61 ja 86–87 (liite 3).

heidän varajäseniltään hyvää tietotekniikan asiantuntemusta (TSL–TSVL–1987 2.1–2 §).[86] Lautakunnan tehtävä oli lain 3 §:n mukaan ratkaista asiat, jotka henkilörekisterilain mukaan kuuluivat sen päätettäviksi, sekä käsitellä henkilörekistereihin liittyviä, lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä.

Nykyinen laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (TSL–TSVL, 389/1994) tuli voimaan 1.7.1994. Syinä uuden lain säätämiselle esitettiin valtion virkamieslainsäädännön voimaantulo ja tarve selkeyttää säätelyä. Varsinaisia viranomaisten toiminnassa havaittuja ongelmia ei ollut taustalla.[87] Kuten edeltäjänsä, laki on 12 pykälän mittainen.[88] Se sisältää pääasiassa samat säännökset kuin aiempikin laki, joskin viranomaisten tehtävien määrittelyä on siirretty asetuksesta lain tasolle. Lautakunnan kokoonpanoa ja asettamista sekä lautakunnan jäsenten ja tietosuojavaltuutetun kelpoisuusvaatimuksia koskeva sääntely taas on siirretty aiemman asetuksen korvanneeseen samannimiseen asetukseen (TSL–TSVA, 432/1994).

Lakia on sittemmin muutettu viisi kertaa. Ensimmäinen muutos (631/1995, voimaan 1.9.1995) liittyi rikoslain kokonaisuudistuksen toiseen vaiheeseen ja koski lain 10 §:ää, joka sisälsi rangaistussäännöksen tietosuojaviranomaisen salassapitovelvollisuuden rikkomisesta. Henkilötietolakia säädettäessä myös viranomaisia koskevan lain viittauksia ja tehtävänmäärittelyjä tarkistettiin (524/1999, voimaan 1.6.1999). Julkisuuslain säätämisen yhteydessä 10 §:n rangaistussäännös kumottiin ja viranomaisten salassapitovelvollisuutta ja tietojen luovuttamista poliisiviranomaisille koskevaa 9 §:ää muutettiin (628/1999, voimaan 1.12.1999). Vuonna 2000 tehdyllä muutoksella (197/2000, voimaan 1.3.2000) tietosuojavaltuutetun nimittäminen siirrettiin tasavallan presidentiltä valtioneuvostolle. Viimeisin muutos (529/2007, voimaan 1.11.2007) tehtiin luottotietolain säätämisen yhteydessä. Lain nojalla annettua asetusta on päivitetty kahdesti, vuonna 1999 henkilötietolain säätämisen yhteydessä ja kaksi vuotta myöhemmin vuonna 2001.[89]

2.2.2 Tehtävien määrittely voimassaolevassa lainsäädännössä

Vuoden 1994 laki ja siihen tehdyt muutokset sen enempää kuin henkilötietolain säätäminenkään eivät muuttaneet sitä lähtökohtaa, että tietosuojavaltuutettu on lähinnä

[86] Ks. HE 49/1986 vp s. 61. Jälkimmäinen vaatimus poistettiin vuoden 1994 uudistuksessa, mutta siinäkin edellytettiin, että lautakunnassa tulee myös olla edustettuna hyvä tietotekniikan asiantuntemus (vuoden 1994 A tietosuojalautakunnasta ja tietosuojavaltuutetusta 1.2 §). Tämä kokoonpanoa koskeva säännös on säilynyt vuodesta 1994 muuttumattomana.

[87] HE 311/1993 vp s. 12: ” Tietosuojalautakunnasta ja tietosuojavaltuutetusta annetut säännökset ehdotetaan tarkistettaviksi korvaamalla niistä annettu laki uudella lailla ja siirtämällä nykyään laissa olevia säännöksiä asetukseen. Ehdotettu laki sisältää vain muutamia asiallisia muutoksia nykyisiin säännöksiin. Suurin osa niistä on lakiteknisiä tarkistuksia. Ehdotetut muutokset johtuvat osaksi siitä, että eräät nykyisen lain säännökset ovat käyneet valtion virkamieslainsäädännön voimaantulon jälkeen tarpeettomiksi, ja osaksi tarpeesta muutoinkin selkiyttää nykyistä sääntelyä.”

[88] Lain 10 § on tosin kumottu lainmuutoksella 628/1999.

[89] Näistä muutoksista tarkemmin ks. hallituksen esitykset HE 94/1993 vp, HE 96/1998 vp, HE 30/1998 vp, HE 176/1999 vp ja HE 241/2006 vp.

ennaltaehkäisevään toimintaan keskittyvä, neuvova ja ohjaava valvontaviranomainen, kun taas tietosuojalautakunta on ennen kaikkea päätösvaltaa käyttävä lupaviranomainen.[90] Nykyisen tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain 5 §:ssä määritetään tietosuojavaltuutetun tehtäviksi seuraavat:

1) käsitellä ja ratkaista henkilötietojen ja luottotietojen käsittelyä koskevat asiat siten kuin henkilötietolaissa ja luottotietolaissa säädetään sekä hoitaa muut mainituista laeista johtuvat tehtävät;
2) seurata henkilötietojen ja luottotietojen käsittelyn yleistä kehitystä ja tehdä tarpeelliseksi katsomiaan aloitteita;
3) huolehtia toimialaansa kuuluvasta tiedotustoiminnasta; sekä
4) huolehtia henkilötietojen käsittelyyn liittyvästä kansainvälisestä yhteistyöstä.

Saman lain 2 §:ssä määritellään vastaavasti tietosuojalautakunnan tehtävät, jotka ovat seuraavat:

1) käsitellä ja ratkaista asiat, jotka henkilötietolain mukaan kuuluvat sen päätettäviksi; sekä
2) seurata henkilötietojen käsittelyä koskevan lainsäädännön kehittämistarvetta ja tehdä tarpeelliseksi katsomiaan aloitteita.

Tietosuojaviranomaisten tehtävät eivät käy tyhjentävästi ilmi näistä säädöksistä. 5 §:n 1 kohdan ja 2 §:n 1 kohdan merkitystä määrittää luonnollisesti henkilötietolaki, erityisesti sen 9 luku, jossa on tehtävien määrittämisen lisäksi säännöksiä myös niiden hoitamiseen tarvittavista oikeuksista, joita ovat tietosuojaviranomaisten laaja, salassapitosäännökset ohittava tiedonsaanti– ja tarkastusoikeus (HetiL 39 §) sekä mahdollisuus tehostaa tiedonsaantioikeutensa toteutumista ja päätöstensä noudattamista uhkasakoilla (HetiL 46 §). Vaikka henkilötietolain säätäminen ei viranomaisten perusrooleja muuttanutkaan, oli se kuitenkin merkittävin viranomaisten tehtäviin vaikuttanut uudistus. Henkilötietolain tuomia viranomaisten tehtävien ja toimivallan muutoksia käsittelen tarkemmin muualla tässä tutkimuksessa. Jo tässä yhteydessä on kuitenkin aiheellista mainita henkilötietolain 38 §, jonka 1 momentissa säädetään tietosuojavaltuutetun yleisestä ohjaus–, neuvonta ja valvontatehtävistä sekä todetaan myös, että tietosuojavaltuutettu käyttää päätösvaltaa siten kuin henkilötietolaissa säädetään. 2 momentissa tietosuojalautakunnan todetaan päätösvallan käyttämisen lisäksi käsittelevän henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä.

38 §

Tietosuojaviranomaiset

Tietosuojavaltuutettu antaa henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa sekä valvoo henkilötietojen käsittelyä tämän lain tavoitteiden toteuttamiseksi ja käyttää päätösvaltaa siten kuin tässä laissa säädetään.

[90] HE 96/1998 vp s. 71.

> Tietosuojalautakunta käsittelee henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä ja käyttää päätösvaltaa tietosuoja–asioissa siten kuin tässä laissa säädetään.
>
> Tietosuojaviranomaiset voivat käyttää tässä luvussa tarkoitettuja toimivaltuuksia silloinkin, kun henkilötietojen käsittelyyn ei 4 §:n mukaisesti sovelleta tätä lakia. Tietosuojaviranomaiset toimivat yhteistyössä muiden Euroopan unionin jäsenvaltioiden tietosuojaviranomaisten kanssa ja antavat tarvittaessa virka–apua.

Kuten tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain 5 §:n 1 kohdasta käy ilmi, tietosuojavaltuutetun tehtäviä määrittää lisäksi luottotietolain sisältö, erityisesti sen 8 luku. Luottotietolain valvonnassa yleistoimivalta kuuluu tietosuojavaltuutetulle (LTL 33 §). Lisätehtäviä tietosuojavaltuutetulle on annettu yksityisyyden suojasta työelämässä annetussa laissa sekä sähköisen viestinnän tietosuojalaissa, jonka 32 §:ssä (125/2009) on lueteltu tietosuojavaltuutetulle kuuluvat, kyseisen lain säännöksiin liittyvät valvontatehtävät: tietosuojavaltuutettu valvoo 1) yhteisötilaajan tunnistamistietojen käsittelyä,[91] 2) paikkatietojen käsittelyä, 3) puhelinluetteloita, muita tilaajaluetteloita ja numerotiedotusta koskevien säännösten noudattamista, 4) suoramarkkinointia koskevien säännösten noudattamista sekä 5) lakiin sisältyviä erityisiä tiedonsaantioikeuksia ja vaitiolovelvollisuutta koskevien säännösten noudattamista paikkatietojen osalta. Myös muussa erityislainsäädännössä on tietosuojavaltuutetulle annettu tehtäviä, jotka eivät ilmene tietosuojalautakunnasta ja tietosuojavaltuutetusta annetusta laista. Tietosuojavaltuutetun tehtäviä määrittää kaikkiaan yli kolmekymmentä lakia tai asetusta.

On kuitenkin syytä huomata, että mainittujen tietosuojan erityislakien valvonta on annettu osin muille viranomaisille kuin tietosuojavaltuutetulle. Sähköisen viestinnän tietosuojalain valvontatehtävät kuuluvat osin Viestintävirastolle (SävTSL 31 §),[92] ja yksityisyyden suojasta työelämässä annetun lain noudattamista valvovat yhdessä tietosuojavaltuutetun kanssa työsuojeluviranomaiset (TYksL 22 §). Lisäksi Ahvenanmaalla on oma maakunnallinen tietosuojalakinsa (*landskapslag om behandling av personuppgifter inom landskaps– och*

[91] Niin kutsutun *Lex Nokian* valvonta on siis tietosuojavaltuutetun vastuulla. Lain 13 i §:ssä säädetään myös yhteisötilaajan velvollisuudesta tehdä tietosuojavaltuutetulle ennakkoilmoitus *Lex Nokia* –säännösten mukaisen tunnistamistietojen käsittelyn aloittamisesta sekä antaa tälle jälkikäteen vuosittain selvitys tunnistamistietojen manuaalisesta käsittelystä.

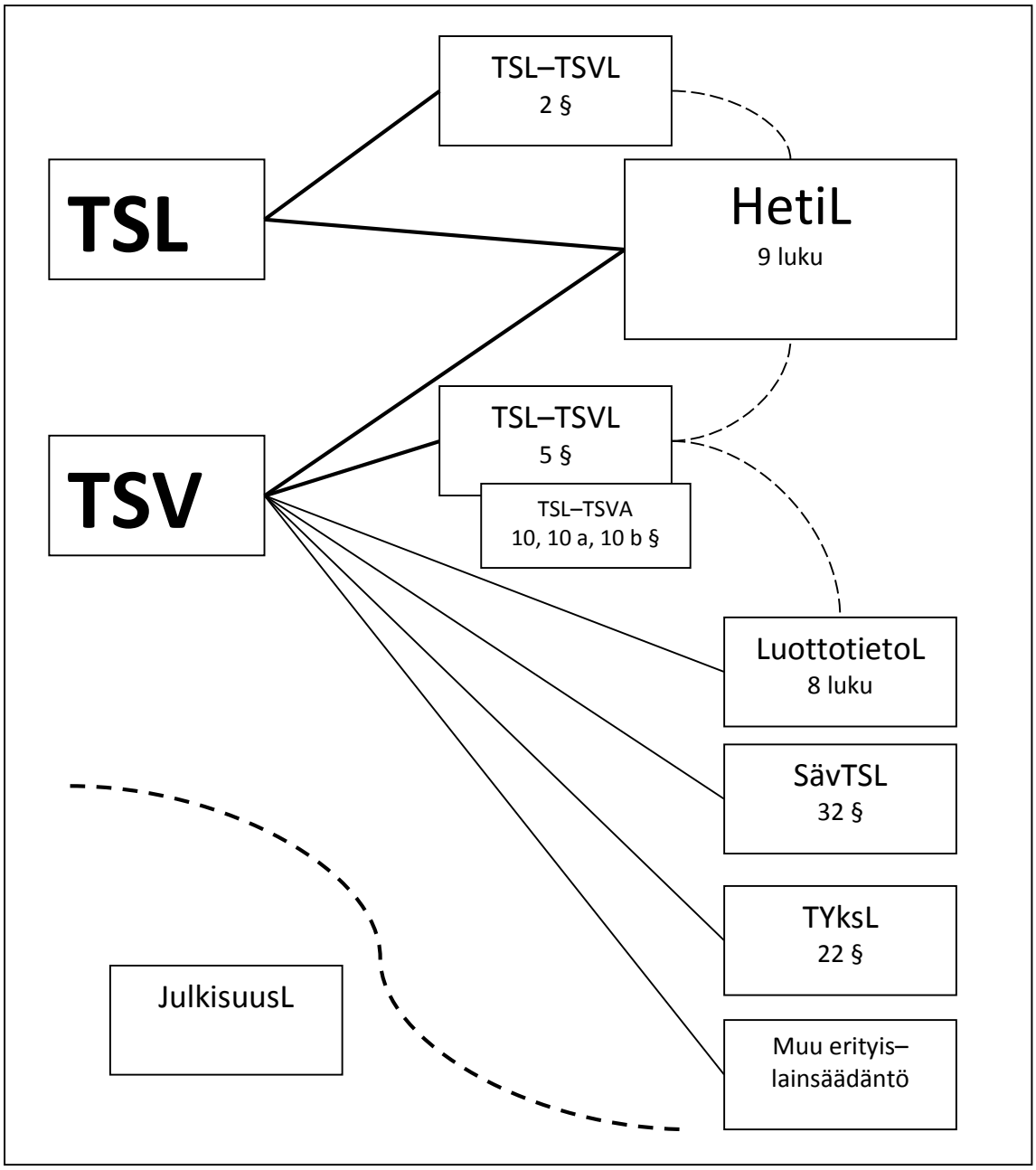
[92] Yleinen ohjaus ja kehittäminen sähköisen viestinnän tietosuojalain tarkoituksen toteutumiseksi kuuluu kuitenkin lain 30 §:n mukaan liikenne– ja viestintäministeriölle. – Sähköisen viestinnän tietosuojalaki on tarkoitus kumota valiokuntakäsittelyssä tätä kirjoitettaessa olevalla tietoyhteiskuntakaarella. Esitys ei muuttaisi viranomaisten työnjakoa, vaan esitetty 305 § vastaisi SävTSL 32 §:ää. Ks. HE 221/2013 vp s. 1, 219–220. Tietoyhteiskuntakaaren on tarkoitus tulla voimaan vuoden 2015 alusta, mutta asiaa saattaa mutkistaa EUT:n tuore tuomio 8.4.2014, C–293/12 ja C–594/12, jolla EUT totesi tunnistamistietojen tallentamista ja säilyttämistä koskevan direktiivin (2006/24/EY) pätemättömäksi. Direktiivi on meillä implementoitu sähköisen viestinnän tietosuojalain muutoksella (343/2008, voimaan 1.6.2008), ja tämä sääntely on ollut tarkoituksena siirtää käytännössä sellaisenaan tietoyhteiskuntakaareen. Kesäkuussa 2014 antamassaan lausunnossa perustuslakivaliokunta katsoi, ettei tuomioista johdu suoranaista estettä tietojen tallentamista, säilyttämistä ja käyttöä koskevalle sääntelylle. Perustuslakivaliokunta kuitenkin edellytti, että tietyistä seikoista, esimerkiksi tietojen säilytysajasta ja käyttötarkoituksesta, määrätään laissa tarkemmin kuin kumotussa direktiivissä ja hallituksen esityksessä. Ks. PeVL 18/2014 vp s. 4–9.

kommunalförvaltningen) ja sen noudattamista valvova tietosuojaviranomaisensa (*Datainspektionen*[93]). Tässä tutkimuksessa ei kuitenkaan käsitellä näiden viranomaisten toimintaa.

Tietosuojavaltuutetulla tai tietosuojalautakunnalla ei ole suoranaista toimivaltaa tulkita asiakirjajulkisuutta koskevaa lainsäädäntöä tai valvoa sen noudattamista. Tietosuojavaltuutettu tai tietosuojalautakunta ei siis päätä, onko jokin tieto julkinen vai salassa pidettävä, vaan julkisuuslain salassapitosäännösten soveltaminen kuuluu kullekin tietopyynnön kohteena olevalle, asiakirjaa hallussaan pitävälle viranomaiselle itselleen (julkisuuslain 14–15 §) ja viime kädessä tuomioistuimille (julkisuuslain 33 §). Eräissä maissa tietosuojasta vastaavalle viranomaiselle on annettu myös julkisuuteen, viranomaistoiminnan avoimuuteen ja informaation vapauteen ja saatavuuteen liittyviä tehtäviä. Tällaisia yhdistettyjä tietosuoja– ja julkisuusviranomaisia toimii mm. Saksassa[94], Sloveniassa[95], Iso–Britanniassa[96] ja Australiassa[97].[98]

Suomen tietosuojaviranomaisten tehtäviä määrittävää lainsäädännöllistä verkkoa havainnollistaa seuraava kuvaaja. Kuvaajassa on mukana vain kansallinen lainsäädäntö.

[93] Ahvenanmaan tietosuojaviranomaiset verkkosivut löytyvät osoitteesta http://www.di.ax, viitattu 20.3.2014.
[94] http://www.bfdi.bund.de/IFG/Dienststelle/Aufgaben/Aufgaben_node.html, viitattu 20.3.2014.
[95] https://www.ip–rs.si/index.php?id=338, viitattu 20.3.2014.
[96] http://ico.org.uk/what_we_cover, viitattu 20.3.2014.
[97] http://www.privacy.gov.au/about–us/what–we–do/what–we–do, viitattu 20.3.2014.
[98] Euroopan unionin tasolla henkilötietojen suojan ja asiakirjajulkisuuden välistä suhdetta määrittää henkilötietodirektiivin resitaali 72, joka otettiin direktiiviin mukaan Ruotsin ja Suomen vaatimuksesta. Kyseisen resitaalin mukaan julkisuusperiaate voidaan ottaa huomioon direktiivin säännöksiä täytäntöön pantaessa.



Kuvaaja 1: Tietosuojaviranomaisten tehtävät lainsäädännössä.

Euroopan unionin oikeudesta johtuvat viranomaistehtäviin liittyvät vaatimukset ilmenevät implementoituina kansallisen lainsäädännön kautta.[99] EU–oikeuden tasolla tietosuojaviranomaisten tehtäviä koskevalle lainsäädännölle vaatimuksia asettaa etenkin henkilötietodirektiivin 28 artikla, jossa käsitellään mm. kenen tahansa oikeutta esittää valvontaviranomaisille tiettyjä vaateita sekä kansainvälistä virka–apua ja yhteistyötä. Artiklassa myös edellytetään, että valvontaviranomaiset laativat säännöllisin väliajoin kertomuksen toiminnastaan. Siinä myös velvoitetaan jäsenvaltiot säätämään siitä, että

[99] Myös kansainvälisistä sopimuksista, esimerkiksi Euroopan neuvoston tietosuojasopimuksesta, aiheutuvat vaatimukset on huomioitu ensisijaisesti kansallisen lainsäädännön välityksellä.

valvontaviranomaisia kuullaan lainsäädännöllisten ja hallinnollisten toimenpiteitä suunniteltaessa, ja siitä että valvontaviranomaisilla on oltava tutkintavaltuudet, tehokkaat toimintavaltuudet ja valtuudet olla osallisena oikeudenkäynnissä tai saattaa direktiivin rikkomukset lainkäyttöviranomaisten tietoon. Lisäksi direktiivin 29 ja 30 artiklassa säädetään tietosuojatyöryhmästä, mikä välillisesti vaikuttaa tietosuojatyöryhmän toimintaan osallistuvien kansallisten tietosuojaviranomaisten tehtäviin.[100] Myös direktiivin eräistä muista artikloista aiheutuu tehtäviä kansallisille valvontaviranomaisille.[101]

Euroopan unionin uusi tietosuoja–asetus tulee muuttamaan tilannetta, sillä siinä asetetaan kansallisille valvontaviranomaisille tehtäviä suoraan ilman tarvetta implementoinnille. Näiden tehtävien lopullinen sisältö, jakautuminen ja se, minkälainen rooli kansallisella lainsäädännöllä on jatkossa, ei ole vielä täysin selvillä. Tietosuoja–asetus ei kuitenkaan sisällä säännöksiä kaikista niistä tehtävistä, joista Suomen tietosuojaviranomaiset nykyisin vastaavat.

2.2.3 Riippumattomuus

Vaikka nykyinen EU–oikeus ei suoraan määritä Suomen tietosuojaviranomaisten tehtäviä, asettaa se kaikelle niiden toiminnalle – ja samalla niitä koskevalle kansalliselle lainsäädännölle – erään keskeisen reunaehdon. Henkilötietodirektiivissä ei ole määräyksiä kansallisten tietosuojaviranomaisten rakenteesta ja organisaatiomallista, mutta direktiivin 28 artiklan 1 kohdan mukaan viranomaisten tulee olla toiminnassaan täysin itsenäisiä.[102] Henkilötietojen suojaa valvovien viranomaisten riippumattomuutta vaaditaan myös Euroopan unionin perusoikeuskirjan (2007/C 303/01) 8 artiklan 3 kohdassa ja Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklan 2 kohdassa. Näiden vaatimusten kannalta jossakin määrin ongelmallista on se, että tietosuojavaltuutetun virka ja toimisto ovat oikeusministeriön yhteydessä ja myös sen tulosohjauksessa, ja toimistossa käytetään esimerkiksi yhteisiä tietojärjestelmiä ministeriön kanssa.[103] Myös tietosuojalautakunnalla on ollut tiiviit käytännölliset ja henkilölliset siteet ministeriöön.[104] Suora hallinnollinen yhteys ministeriöstä tietosuojaviranomaisiin on kuitenkin katkaistu.

Suomalaisen organisaation on kuitenkin katsottu täyttävän EU–lainsäädännön kriteerit, joita Euroopan unionin tuomioistuin on tarkemmin määrittänyt Itävallan *Datenschutzkommission*–viranomaista ja eräitä saksalaisia tietosuojaviranomaisia koskevissa tuomioissaan (16.10.2012, C–614/10 ja 9.3.2010, C–518/07), joissa se totesi Itävallan ja Saksan rikkoneen jäsenyysvelvoitteitaan. Vaikka valvontaviranomaisten rakenne ja organisaatio ovat

[100] Ks. tarkemmin II.5.3.
[101] Ks. ainakin 8 artiklan 4 kohta, 18 artikla, 20 artiklan 2 kohta, 21 artiklan 2 kohta ja 27 artiklan 2 kohta.
[102] Direktiivin suomenkielisessä kieliversiossa ei mainita sanaa *täysin*, joka kuitenkin muista kieliversioista löytyy (englanniksi *complete independence*, saksaksi *völliger Unabhängigkeit)*.
[103] Ulospäin näkyvä, tähän liittyvä seikka on mm. se, että tietosuojavaltuutettu ja toimiston työntekijät käyttävät oikeusministeriön @om.fi –päätteistä sähköpostia.
[104] Ks. myös III.1.2.

jäsenvaltioiden itse päätettävissä, EU–tuomioistuin on korostanut, että toiminnallinen itsenäisyys – se, ettei valvontaviranomaisten jäseniä sido mikään ohje heidän hoitaessaan tointansa – ei yksinään riitä suojaamaan valvontaviranomaisia kaikelta ulkopuoliselta vaikuttamiselta. Itsenäisyysvaatimus sulkee pois myös välillisen ulkoisen vaikuttamisen mahdollisuuden, ja valvontaviranomaisten ja niiden päätösten tulee olla kaiken puolueellisuutta koskevan epäilyn yläpuolella. Tuoreimmassa 28 artiklan 1 kohtaa koskevassa tuomiossaan (8.4.2014, C–288/12) EU–tuomioistuin totesi Unkarin rikkoneen jäsenyysvelvoitteitaan, kun se oli päättänyt tietosuojavaltuutetun toimikauden ennenaikaisesti toimielinrakenteen muutostilanteessa, jossa tietosuojavaltuutettu korvattiin uudella tietosuojavirastolla.

EU:n uudessa tietosuoja–asetuksessa riippumattomuus ja tietosuojaviranomaisten asema määritellään tarkemmin kuin direktiivissä. Asetusehdotuksen 47 artiklassa säädetään mm. jäsenvaltioiden velvollisuudesta varmistaa valvontaviranomaisille riittävät resurssit ja se, ettei valvontaviranomaiseen sovellettava varainhoidon valvonta vaikuta sen riippumattomuuteen. Riippumattomuutta pyritään ylläpitämään myös valvontaviranomaisen jäsenien sivutoimia koskevalla rajoituksella ja määräyksellä, jonka mukaan ”[v]alvontaviranomaisen jäsenten on toimikautensa päättymisen jälkeen osoitettava kunniallisuutta ja arvostelukykyä nimitysten ja etujen vastaanottamisessa”. Eräänlaisena vähimmäisvaatimuksena ja peruslähtökohtana on edelleen valvontaviranomaisten täysi toiminnallinen riippumattomuus tehtäviensä hoidossa, ja se etteivät valvontaviranomaiset tehtäviään hoitaessaan sen enempää pyydä kuin ota ohjeita miltään taholta. Uutena asiana asetuksessa on myös säännökset valvontaviranomaisten jäsenten nimittämisestä, kelpoisuudesta ja tehtävien päättymisestä (48 artikla) sekä valvontaviranomaisten perustamista koskevista säännöistä (49 artikla).[105]

Riippumattomuuden korostamisesta huolimatta on syytä huomauttaa, ettei se tarkoita eikä se voi tarkoittaa eristäytymistä sen enempää nykyisen kuin tulevankaan EU–oikeuden vaatimusten valossa. Sidosryhmien kanssa tehtävällä yhteistyöllä on merkittävä rooli tietosuojaviranomaisten toiminnassa, ja tietosuojavaltuutetun toimiston strategiaan kuuluu nimenomaisesti liittoutuminen. Verkottuminen yhteiskuntaan on nähty keinona vahvistaa voimavaroja ja tehostaa toimintaa. Liittoutumalla on mahdollista kiertää resurssien niukkuudesta aiheutuvia ongelmia.[106]

[105] Itsenäisyyden merkityksestä ks. myös *Saarenpää*, Data protection in the network society – the exceptional becomes the natural, teoksessa *Galindo* (ed.), El derecho de la sociedad en red (2013) s. 108–113.
[106] Esim. KT 2012 s. 18.

II Tietosuojavaltuutettu

1. Yleistä tietosuojavaltuutetusta ja tietosuojavaltuutetun toimistosta

Tietosuojavaltuutettu on valtioneuvoston enintään viiden vuoden määräajaksi nimittämä virkamies (TSL–TSVL 1.1 ja 6.1 §).[107] Tietosuojavaltuutetun virassa on tähän mennessä toiminut kolme eri henkilöä neljännesvuosisadan aikana. Ensimmäiseksi tietosuojavaltuutetuksi vuonna 1987 nimitettiin *Anna–Riitta Wallin*. Wallinin seuraajaksi tämän viisivuotisen toimikauden jälkeen valittiin *Jorma Kuopus*. Marraskuussa 1997 Kuopusta seurasi *Reijo Aarnio*, joka on toiminut tästä lähtien tietosuojavaltuutettuna. Aarnion nykyinen viisivuotiskausi alkoi 1.11.2012. Aarnio on siis toiminut virassa koko henkilötietolain voimassaoloajan.[108]

TSL–TSVL 1.2 §:n mukaan tietosuojavaltuutetulla on toimisto, jossa on esittelijöinä toimivia virkamiehiä ja muuta henkilökuntaa. Toimistossa ei ole vara– tai apulaistietosuojavaltuutetun virkaa. Tietosuojavaltuutettua avustaa ja tarpeen vaatiessa hänen sijaisenaan on tietosuojavaltuutetun toimiston toimistopäällikkö, joka voi tietosuojavaltuutetun määräyksestä käyttää tietosuojavaltuutetun puhevaltaa. Ennen vuotta 1994 vastaava säännös oli TSL–TSVL–1987 8.1 §. Tuon säännöksen sanamuodon mukaan toimistossa saattoi olla esittelijöitä ja muuta henkilökuntaa *tulo– ja menoarvion rajoissa*. Nuo rajat osoittautuivatkin käytännössä varsin ahtaiksi.

Tietosuojavaltuutetun toimiston ensimmäisen täyden toimintavuoden (1988) loppuun mennessä toimistoon oli perustettu seitsemän virkaa ja lisäksi toimistossa työskenteli työsuhteinen tarkastaja, mikä oli vähemmän kuin lakia säädettäessä oli edellytetty. Vuonna 1988 tietosuojaviranomaisten, siis tietosuojalautakunnan menot mukaan lukien, budjetin loppusumma oli 2 349 000 mk, mikä vuoden 2012 rahan arvoon suhteutettuna vastaa noin 670 000 euroa.[109] Tästä summasta henkilöstömenojen osuus oli noin 40 prosenttia.[110]

1990–luvulla toimisto sai asteittain käyttöönsä jonkin verran enemmän työvoimaa ja resursseja. Vuosikymmenen puolivälissä toimiston vuosibudjetti oli 3 900 000 markkaa (noin 880 000 euroa)[111] ja siellä työskenteli 14 henkilöä.[112] Henkilötietolain tultua voimaan vuonna 2000 tietosuojavaltuutetun toimistolla oli käytettävissään 18 henkilötyövuotta ja

[107] Ennen vuotta 2000 nimittäjänä toimi tasavallan presidentti.
[108] Kun tietosuojalautakunnan puheenjohtajana taas on toiminut alusta alkaen Pekka Nurmi, vaihtuvuus tietosuojan ylimmissä viranomaistehtävissä on siis ollut lopulta varsin vähäistä, vaikka kaksi ensimmäistä tietosuojavaltuutettua toimivatkin tehtävässä vain yhden kauden. Myös tietosuojalautakunnan jäsenet ovat usein toimineet tehtävässään useamman kuin yhden kolmivuotiskauden. Vrt. *Kleemola*, Katsaus tietosuojavaltuutetun toimiston 15 vuoteen, Tietosuoja 1/2003 s. 5.
[109] Suomen virallinen tilasto (SVT): Kuluttajahintaindeksi [verkkojulkaisu]. Rahanarvokerroin 1860 – 2012. Saatavilla http://www.stat.fi/til/khi/2012/khi_2012_2013–01–15_tau_001.html, viitattu 10.9.2013.
[110] TK 1987–1988 s. 12.
[111] Luku ei sisällä tietosuojalautakunnan menojen osuutta, joka oli n. 500 000 mk.
[112] TK 1995 s. 6.

toimintamenot olivat 6 300 000 mk (runsaat 1 300 000 euroa)[113]. Palkkamenojen osuus oli n. 67 prosenttia.[114] 2000–luvun alkupuolella toimiston työntekijämäärä vakiintui 20 henkilön paikkeille. Tässä suuruusluokassa se on tämänkin jälkeen pysynyt, joskin pientä kasvua on edelleen tapahtunut. Kasvu ei kuitenkaan ole kohdistunut vakituisten työntekijöiden määrään, vaan määräaikaisiin työntekijöihin ja harjoittelijoihin.[115]

Tietosuojavaltuutetun toimiston vuoden 2013 vuosikertomuksen mukaan toimiston henkilötyövuosien lukumäärä oli 24. Toimiston viroista täytettynä oli vakituisesti 16 ja määräaikaisesti viisi. Lisäksi toimistossa työskenteli yksi oikeusministeriön virassa oleva henkilö sekä kaksi harjoittelijaa.[116] Vuoden lopussa vakituiseen henkilökuntaan kuului tietosuojavaltuutetun ja toimistopäällikön lisäksi kymmenen ylitarkastajaa, yksi tarkastaja, yksi IT–erityisasiantuntija ja kaksi sihteeriä.[117] Toiminnan kokonaiskustannukset vuoden aikana olivat 1 752 005 euroa.[118]

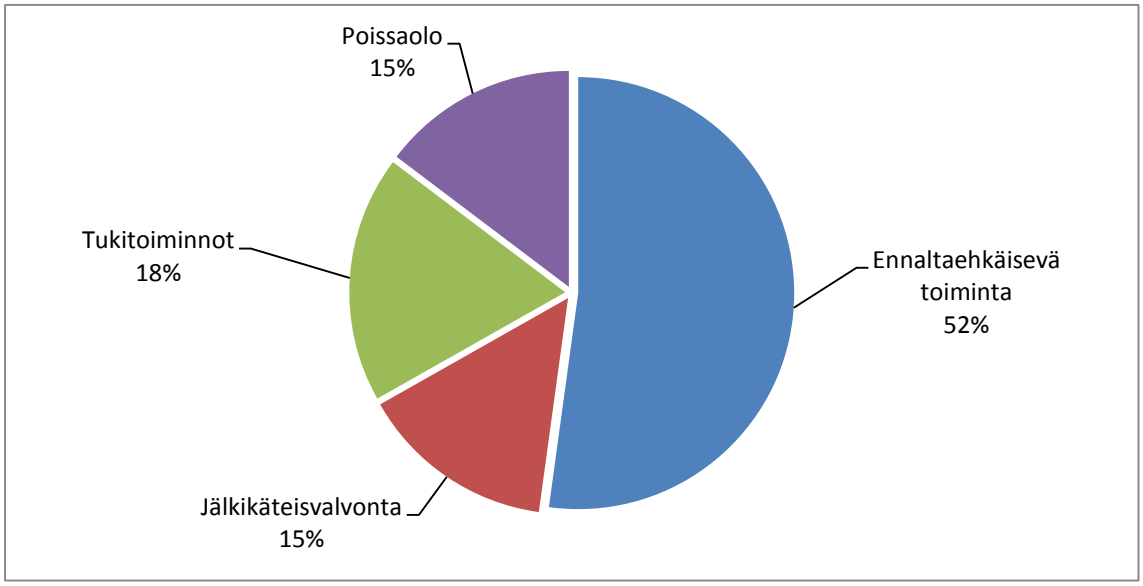
Neljännesvuosisadassa tietosuojavaltuutetun toimiston resurssien määrä on siis kasvanut noin 2,5–kertaiseksi. Toimiston tehtävät ovat kuitenkin moninkertaistuneet. Kun ajanjaksolla 1.10.1987 – 31.12.1988 toimistossa käsiteltiin 314 ja vireille tuli 743 asiaa, jo vuonna 2000 vastaavat luvut olivat 1 139 ja 1 256. Vuonna 2013 tietosuojavaltuutetun toimisto käsitteli 3 426 kirjallisesti vireille tullutta (diarioitua) asiaa, ja vireille tuli 3 852 asiaa.[119]

Varansa toimisto saa eduskunnan päättämästä talousarviosta. Käytännössä resursoinnista päätetään oikeusministeriön kanssa vuosittain loppuvuodesta käytävissä tulosneuvotteluissa, joissa myös asetetaan toimiston toiminnalliset tulostavoitteet seuraavalle vuodelle. Tulostavoitteiden toteutumista seurataan toimintakertomuksissa, joista oikeusministeriö antaa kannanoton.[120]

Tietosuojavaltuutetun toimiston toimintaa voidaan jaotella erilaisiin operatiivisiin toimintalohkoihin. Nykyisessä, vuodesta 2008 lähtien käytössä olleessa jaottelussa pääkategorioita ovat ennaltaehkäisevä toiminta ja jälkikäteisvalvonta, jotka jakautuvat

[113] Luku ei sisällä tietosuojalautakunnan menojen osuutta, joka oli 480 609 mk.
[114] TK 2000 s. 8.
[115] Ruotsin, Norjan ja Tanskan tietosuojaviranomaisiin verrattuna tietosuojavaltuutetun toimiston henkilömäärä on kuitenkin edelleen puolet pienempi. Ks. esim. Ruotsin Datainspektionen, Årsredovisning 2012 s. 47, Norjan Datatilsynet, Årsmelding for 2013 s. 69 ja Tanskan Datatilsynet, Datatilsynets årsberetning 2012 s. 15. Eri viranomaisten välillä on kuitenkin myös huomattavia eroja organisaatiorakenteessa ja tehtävissä, joten resurssitilanne ei ole täysin vertailukelpoinen.
[116] Vielä vuonna 2012 harjoittelijoiden työpanoksen osuus oli huomattavasti merkittävämpi, 4,24 htv. Oikeusministeriö toi tietosuojavaltuutetun toimiston vuosien 2011 ja 2012 toimintaa ja taloutta koskevissa kannanotoissaan esille huolensa harjoittelijoiden käyttämisestä lakisääteisten tehtävien suorittamiseen.
[117] Lisäksi kaksi henkilöä oli virkavapaalla.
[118] TK 2013 s. 7 ja KT 2013 s. 17. Vuodesta 2003 lähtien tietosuojavaltuutetun toimisto on saanut myös hieman tuloja järjestämästään maksullisesta koulutustoiminnasta. Tulot ovat olleet muutaman kymmenen tuhannen euron luokkaa, eivätkä ne ole yleensä kattaneet koko koulutustoiminnan kustannusosuutta. Ks. tarkemmin II.6.5.
[119] Asiamääristä tarkemmin ks. II.2.
[120] Tulosohjausasiakirjoja on julkaistu tietosuojavaltuutetun toimiston verkkosivuilla, ks. http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/tulosohjaussuunnitteluja–seurantauusin.html, viitattu 9.5.2014.

yhteensä kahdeksaksi toiminnaksi. Ennaltaehkäisevä toiminta on jaoteltu tietosuojavaltuutetun toimintaan tarkastajana, konsulttina, valistajana, poliittisena neuvonantajana, neuvottelijana ja kansainvälisenä lähettiläänä. Jälkikäteisvalvonta jakautuu toimintaan valtuutettuna ja täytäntöönpanijana. Näistä toiminta painottuu ennaltaehkäisevään toimintaan, johon toimisto käyttää noin puolet resursseistaan.[121] Ennaltaehkäisevää toimintaa on painotettu myös tulosneuvotteluissa sovituissa tavoitteissa.[122] Jälkikäteisvalvonnan osuus on ollut noin 15 prosenttia. Loput resursseista kuluvat tukitoimintoihin ja poissaoloihin. Vuonna 2013 kustannukset jakautuivat seuraavan kuvaajan alemman osan osoittamalla tavalla.



Kuvaaja 2: Kustannusten jakautuminen eri toimintojen kesken tietosuojavaltuutetun toimistossa 2013.

Käytännössä ennaltaehkäisevään toimintaan sisältyvät sidosryhmäyhteistyö, yleisohjaus– ja tiedoteaineiston tuottaminen, tiedottaminen, lausuntojen antaminen lainsäädännöllisistä ja hallinnollisista uudistuksista, käytännesäännöistä sekä tutkimuslupa–asioissa, rekisteripitäjäkohtainen neuvonta, ohjaus ja konsultointi, ennakkovalvonta ja osa tarkastuksista, tietosuojan yleinen seuranta, tietopalvelu, koulutusten järjestäminen ulkopuolisille ja kansainvälinen toiminta. Jälkikäteisvalvontaan sisältyvät oikeudenloukkauksia koskeva osa ratkaisutoiminnasta, osa tarkastustoiminnasta ja asioiden saattaminen tietosuojalautakunnan käsiteltäväksi tai poliisin tutkittavaksi.

[121] Vanhan jaottelun mukaan varsinaiseen ennaltaehkäisevään toimintaan käytettiin vain noin neljännes resursseista.

[122] Tavoitteisiin on viime vuosina säännönmukaisesti kirjattu laskeva trendi oikeudenloukkauksia koskevien lausuntopyyntöjen määrässä suhteessa kaikkiin lausuntopyyntöihin ja kantelujen määrässä suhteessa kaikkiin asioihin. Lisäksi tavoitteeksi on asetettu nouseva trendi ohjauspyyntöjen määrässä suhteessa kaikkiin asioihin, oma–aloitteisten vireillepanojen määrässä suhteessa kaikkiin ohjaus– ja toimenpidepyyntöihin sekä annettujen lausuntojen määrässä. Tavoitteiden mukaisia trendejä ei suinkaan ole joka vuosi saavutettu.

2. Asiamäärät ja ratkaisutoiminta

2.1 Yleistä

Tässä luvussa tarkastelen tietosuojavaltuutetun toimistossa diarioitujen asioiden lukumäärää eri näkökannoilta ja eri ryhmittelyjä käyttäen. Seuraavassa alaluvussa 2.2 tarkastelun kohteena ovat kaikkien asioiden määrä ja rakenne sekä toimialakohtaiset ryhmittelyt. Alaluvussa 2.3 taas tarkastelen tiettyjä keskeisiä asiaryhmiä, jotka muodostavat periaatteellisesti tai lukumäärällisesti tärkeän osan tietosuojavaltuutetun toimiston toimintaa. Alaluvussa 2.4 tarkastelen ratkaisutoimintaan käytettyjä resursseja sekä käsittelyaikoja.

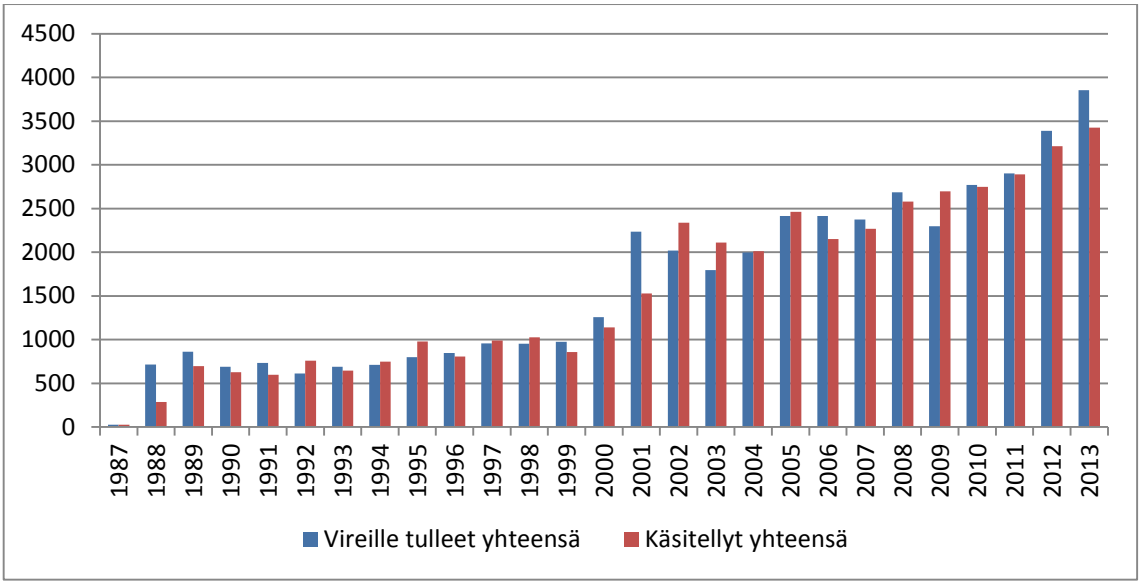
Tämän luvun päähuomio on niin sanotussa ratkaisutoiminnassa, joka kohdistuu kirjallisesti vireille tulleisiin yksittäisasioihin. Ratkaisutoiminnasta puhuessani en tarkoita rajata tarkastelua suppeasti vain niihin asioihin, joissa tietosuojavaltuutettu voi antaa *oikeudellisesti sitovia päätöksiä*. Nämä rekisteröidyn tarkastusoikeuden toteuttamista (HetiL 28 §) tai tiedon korjaamista (HetiL 29 §) koskevat asiat, joita kylläkin käsittelen alaluvussa 2.3, muodostavat lukumäärällisesti vain pienen osan tietosuojavaltuutetun ratkaisutoiminnasta, joka koostuu suurelta osin tietosuojavaltuutetun *neuvontaa* ja *ohjausta* koskevista kannanotoista.

Kaikki tämän luvun kuvaajat perustuvat tietosuojaviranomaisten toiminta– ja vuosikertomuksista saatuihin tilastotietoihin, jollei toisin ole ilmoitettu. Jos eri vuosien julkaisuissa samaa vuotta koskevat luvut ovat eronneet toisistaan, kuvaajissa on käytetty uusinta tietoa, paitsi milloin kyseessä on ollut selkeä virhe. Tilastokategorioita on tarpeen mukaan yhdistelty lukujen vertailukelpoisuuden säilyttämiseksi. Tarkastelu kattaa eräissä tapauksissa koko tietosuojaviranomaisten toiminta–ajan, mutta pääpaino on 2000–luvun eli henkilötietolain voimassaoloajan tiedoilla. Henkilörekisterilain aikaisia tietoja on mukana siinä määrin, kun niitä on saatavilla.[123]

2.2 Kaikkien asioiden määrien ja rakenteen kehitys

Kirjallisesti vireille tulleiden asioiden määrä tietosuojavaltuutetun toimistossa on kasvanut käytännössä koko toimiston toiminta–ajan. Seuraava kuvaaja esittää kaikkien vireille tulleiden ja käsiteltyjen diarioitujen asioiden määrän kehityksen tietosuojavaltuutetun toimiston toiminnan alusta alkaen.

[123] Vesa Muttilainen on vuonna 2006 julkaistussa tutkimuksessaan tarkastellut tilastotietoja 1990–luvulta 2000–luvun puoliväliin. Ks. *Muttilainen*, Suomalaiset ja henkilötietojen suoja (2006) s. 45–56.



Kuvaaja 3: Kaikki tietosuojavaltuutetun toimistossa vireille tulleet ja käsitellyt asiat 1987–2013.

Kuten kuvaajasta ilmenee, on asiamäärä kolminkertaistunut 1990–luvun lopun tasosta. Kasvu on muutamaa poikkeusta lukuun ottamatta ollut melko tasaista. Henkilötietolain voimaantulo nosti selvästi asioiden määrää ja toi myös mukanaan suuren määrän kertaluonteisia asioita, mikä on havaittavissa etenkin lain siirtymäajan päättymisvuonna 2001 vireille tulleissa asioissa.[124] Pienen tasaantumisvaiheen jälkeen asiamäärän kasvu on jatkunut, vuodesta 2006 saakka käsiteltyjä asioita tarkasteltaessa yhtäjaksoisesti. Vireille tulleiden asioiden määrän kehitys on ollut aavistuksen epätasaisempaa, ja esimerkiksi vuonna 2009 vireille tuli lähes 400 asiaa vähemmän kuin vuotta aiemmin.

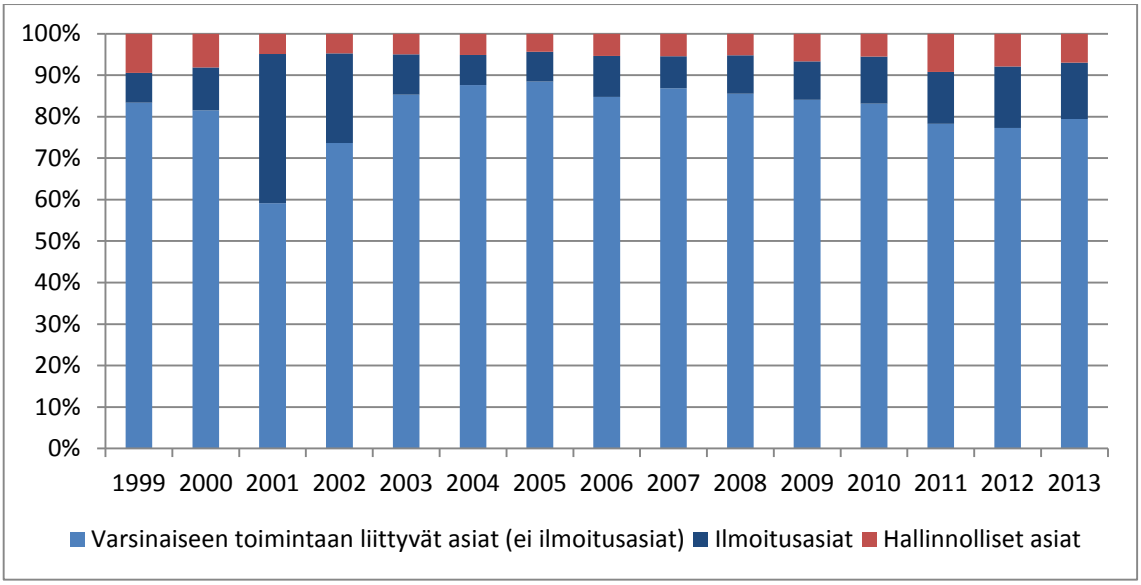
Vireille tulleiden ja käsiteltyjen asioiden määrän erotus on pysynyt yleensä pienenä. Mainittuna poikkeusvuonna 2009 käsiteltyjä asioita oli selvästi enemmän kuin vireille tulleita, eli toimistossa onnistuttiin purkamaan vuosina 2006–2008 kertyneitä asioita. Tilanne oli samankaltainen vuosina 2002–2003, jolloin purettiin vuoden 2001 vireille tulleiden asioiden määrän äkillisen nousun seurauksena syntynyttä siirtyneiden asioiden joukkoa. Vielä vuosina 2004–2005 käsiteltyjen asioiden määrät ylittivät niukasti vireille tulleiden asioiden lukemat. Seuraavalle vuodelle siirrettyjen asioiden määrä on vaihdellut viime vuosina noin kuudestasadasta hieman yli tuhanteen. Tässä suhteessa ei ole tapahtunut suurta muutosta, sillä jo 1990–luvun alkupuolen vuosina asioita jouduttiin siirtämään noin saman verran. Tuolloin siirtyneiden asioiden osuus oli suhteellisesti paljon suurempi kuin nykyään, joinakin vuosina jopa yli 100 prosenttia samana vuonna vireille tulleista asioista. 2000–luvulla eniten asioita on jouduttu siirtämään vuosina 2006–2008, jolloin vastaavat osuudet olivat keskimäärin vajaat 40 prosenttia. Vuoden 2012 lopussa vireille jäi 888 asiaa eli 26,2 prosenttia saman vuonna vireille

[124] HetiL 51.1 §:n mukaan henkilötietojen käsittely, johon oli ryhdytty ennen HetiL:n voimaantuloa, oli saatettava lain vaatimuksia vastaavaksi viimeistään 24.10.2001.

tulleiden asioiden määrästä. Vuoden 2013 nämä luvut olivat asiamäärien nopeana jatkuneen kasvun myötä suuremmat, 1314 asiaa ja 34,1 prosenttia. Vaikka jutturuuhkia on osittain menestyksekkäästi ehkäisty toiminnan tehostamisella, nykyisellä resurssitasolla jutturuuhkien purkaminen on haasteellista, ellei vireille tulevien asioiden määrä ei tasoitu tai käänny laskuun. Vaarana on siis käsittelyjonojen pidentyminen.

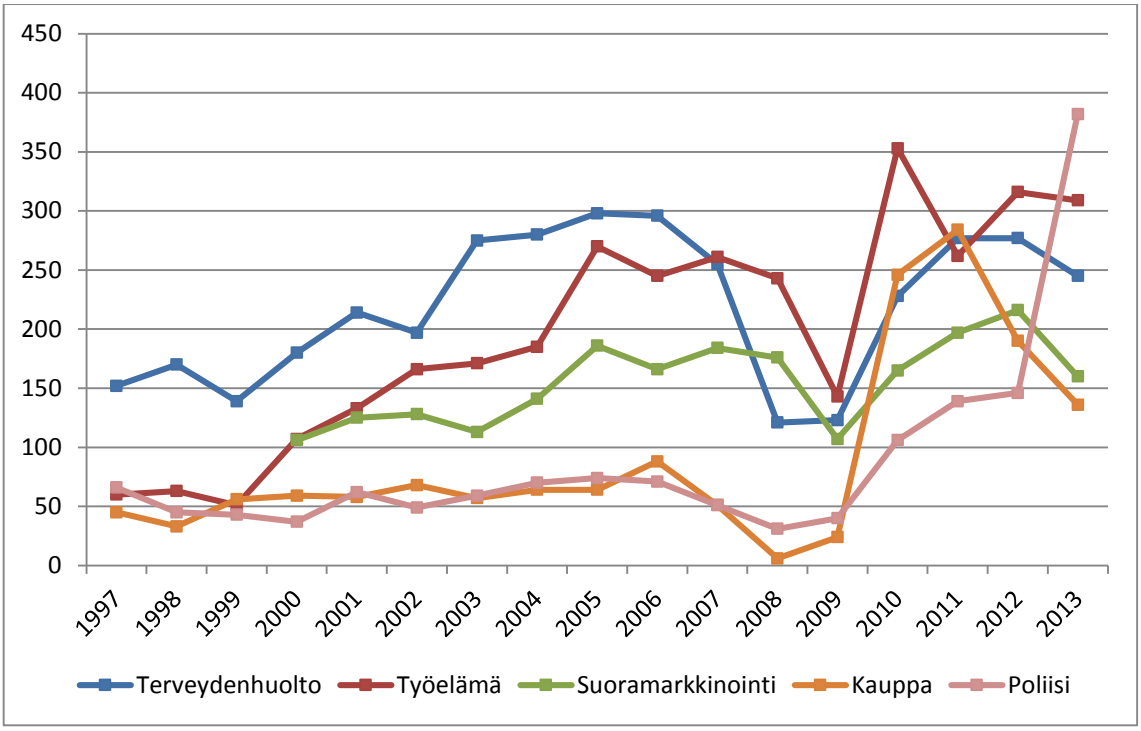
Edellinen kuvaaja esittää kaikkien asioiden lukumäärien kehityksen, sisältäen sekä varsinaiseen toimintaan liittyvät että hallinnolliset asiat. Jälkimmäisten osuus on 2000–luvulla ollut noin 5–10 prosentin luokkaa kaikista asioista. Varsinaiseen toimintaan luettavien, henkilötietolain 36 ja 37 §:n mukaisten ilmoitusasioiden[125] osuus oli suuri etenkin 2000–luvun alussa eli henkilötietolain voimassaolon alkuvuosina – enimmillään 36,0 prosenttia kaikista vireille tulleista asioista vuonna 2001, ja tämän seurauksena 31,3 prosenttia kaikista käsitellyistä asioista vuonna 2002 – mutta laski vuosikymmenen puoliväliin mennessä. Viime vuosina ilmoitusasioiden määrä on jälleen kasvanut. Muiden varsinaiseen toimintaan liittyvien asioiden osuus on ollut 2000–luvun alkuvuosia lukuun ottamatta yli 80 prosentin luokkaa, mutta viime vuosina sekä hallinnollisten asioiden että varsinkin ilmoitusasioiden määrän kasvu on painanut sen alle 80 prosentin rajaviivan. Kaikkien varsinaiseen toimintaan liittyvien asioiden osuus on kuitenkin pysynyt vielä yli 90 prosentin vireille tulleista asioista, mitä voidaan pitää hyvänä asiana. Hallinnolliset asiat eivät siis ole kohtuuttomasti rasittaneet toimistoa vaan pääasiassa se on voinut keskittyä varsinaiseen toimintaansa. Seuraava kuvaaja esittää vireille tulleiden asioiden jakautumisen ilmoitusasioihin, muihin varsinaiseen toimintaan liittyviin asioihin ja hallinnollisiin asioihin.

[125] Ilmoitusasioiden sisällä suurimman ryhmän ovat viime vuosina muodostaneet tietojenkäsittelypalvelujen ostamista koskevat ilmoitukset. Vuonna 2012 36 prosenttia kaikista vireille tulleista ilmoitusasioista koski tietojenkäsittelypalvelujen ostamista. Ilmoitusasioista tarkemmin ks. II.6.1.



Kuvaaja 4: Tietosuojavaltuutetun toimistossa vireille tulleiden asioiden jakautuminen varsinaiseen toimintaan liittyviin ei–ilmoitusasioihin, ilmoitusasioihin ja hallinnollisiin asioihin 1999–2013.

Tietosuojavaltuutetun toimistossa asioita on 2000–luvulla ja osittain jo 1990–luvulla tilastoitu myös toimialoittain. Asiamääriltään merkittävimmät toimialat ovat pitkään olleet terveydenhuolto, työelämä ja suoramarkkinointi. Myös kaupan ala on vuodesta 2010 lähtien noussut suurimpien joukkoon. Eri vuosien välillä on niin mainituilla toimialoilla kuin muillakin ollut prosentuaalisesti suuria ja melko äkillisiä vaihteluita. Seuraavat kaksi kuvaajaa esittävät asiamäärät toimialakohtaisesti. Ensimmäisessä kuvaajassa ovat mukana suurimmat toimialakohtaiset asiaryhmät. Jokaisella näistä toimialoista asioiden lukumäärä on kolmena viime vuotena ylittänyt sadan asian rajan.

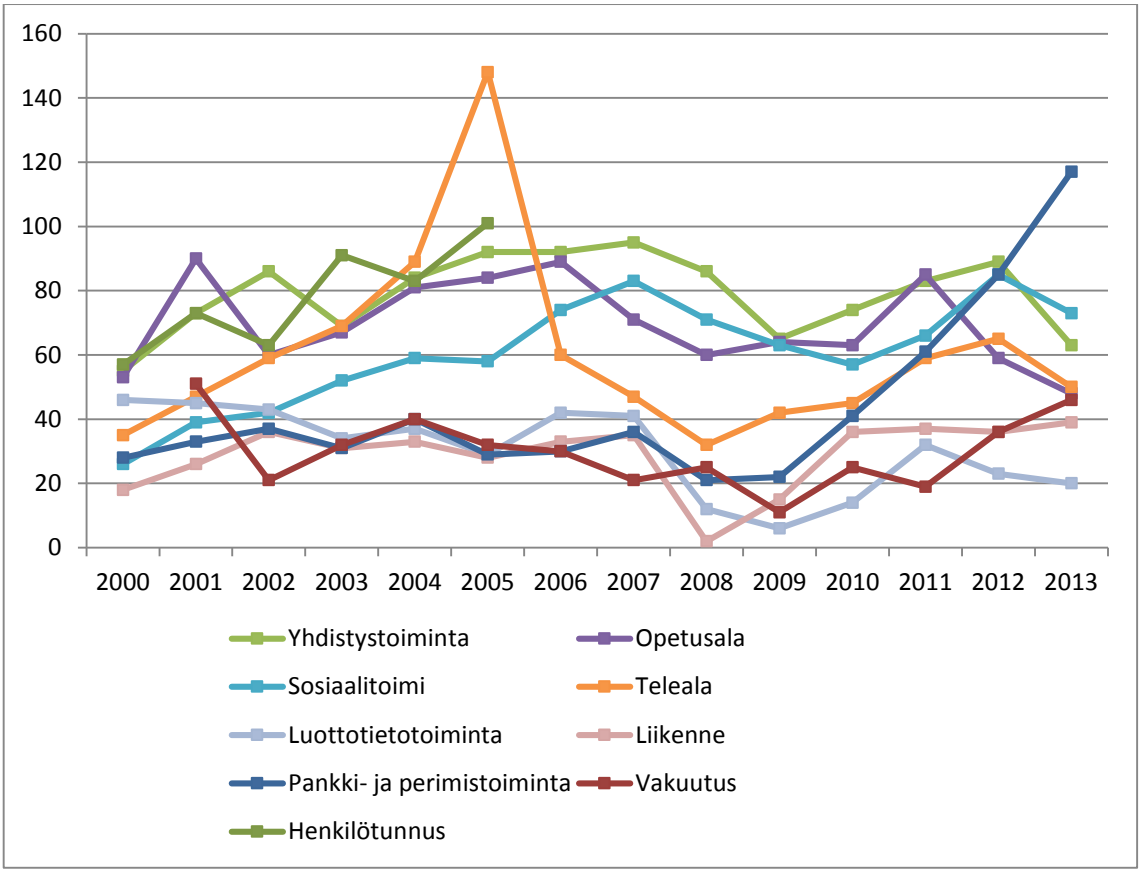


Kuvaaja 5: Tietosuojavaltuutetun toimistossa vireille tulleet asiat toimialoittain 1997–2013 (asiamääräisesti suurimmat toimialat).[126]

Pitkään suurimman asiaryhmän muodostivat terveydenhuoltoa koskevat asiat, joiden määrä on kuitenkin saavuttanut tähänastisen huippunsa jo vuonna 2005. Muutaman selvästi hiljaisemman vuoden jälkeen lukumäärä on palannut kuitenkin edellisen vuosikymmenen puolivälin tasolle. Samaan aikaan työelämää koskevien asioiden määrässä on havaittavissa edelleen jatkuva nouseva trendi, jonka johdosta asioiden määrä on lähes kolminkertaistunut vuodesta 2000. Myös suoramarkkinointiasioiden määrä on yli kasvanut merkittävästi 2000–luvulla. Kaupan alan asioiden määrässä tapahtui suuri hyppäys vuonna 2010, ja vuotta myöhemmin ala nousi jopa asiamäärältään suurimmaksi toimialaksi, mutta kahtena viime vuonna määrä on taas laskenut. Myös poliisin rekisterinpitoa koskevat asiat ovat yleistyneet selvästi viime vuosina, ja niiden määrä on moninkertaistunut vain muutamassa vuodessa. Vuoden 2013 hyppäykseen ovat epäilemättä vaikuttaneet julkisuudessa esillä olleet poliisin rekisterinpidon epäselvyyksiin liittyneet tapaukset.

Toisesta toimialakohtaista jakaumaa koskevasta kuvaajasta ilmenee muiden toimialojen asiamäärien kehitys. Mukana ovat myös henkilötunnusta koskeneet asiat, joita tilastoitiin erikseen vuoteen 2005 saakka, vaikka kyse ei olekaan toimialasta.

[126] Suoramarkkinointiasioita koskevaa tilastotietoa on saatavilla vasta vuodesta 2000 lähtien.



Kuvaaja 6: Tietosuojavaltuutetun toimistossa vireille tulleet asiat toimialoittain 2000–2013 (muut toimialat ja henkilötunnusta koskevat asiat).

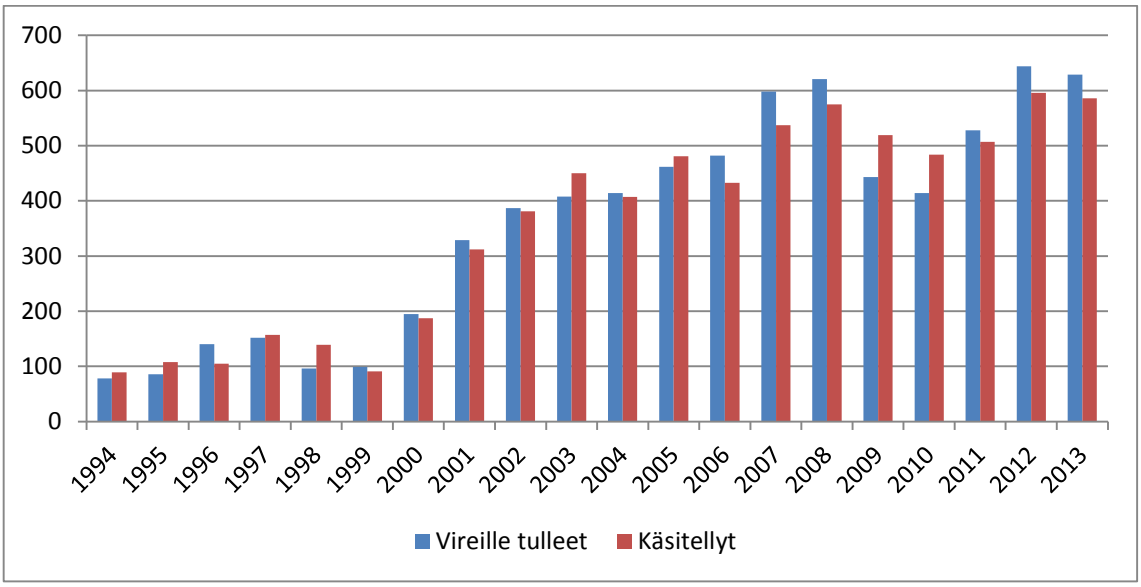
Tässä joukossa selvä nouseva trendi on havaittavissa sosiaalitoimea koskevissa asioissa, joiden määrä on noussut tarkasteluvälillä noin kolminkertaiseksi. Myös telealan asioiden määrä on kasvanut koko tarkasteluvälin aikaväliä tarkasteltaessa, mutta edellisen vuosikymmenen puolenvälin piikistä on tultu selvästi alaspäin. Viimeisen viiden vuoden aikana selvimmin asiamäärä on noussut pankki– ja perimistoiminnassa, minkä voi nähdä olevan kytköksissä yleiseen taloustilanteeseen. Luottotietoasioissa vastaavaa, taloustilanteeseen kytköksissä olevaa kehitystä on mahdollisesti hillinnyt vuonna 2007 säädetty luottotietolaki. Muiden toimialojen asiamäärät ovat pysyneet varsin tasaisina tai jopa laskeneet ainakin vuosiin 2008–2009 saakka, minkä jälkeen asiamäärät ovat jonkin verran kasvaneet. Tämä ei ole yllättävää, sillä kuten edellä havaittiin, myös tietosuojavaltuutetun toimiston käsittelemien asioiden kokonaismäärä on jälleen selvästi kasvanut hiljaisemman vuoden 2009 jälkeen.

2.3 Kehitys asiaryhmittäin

2.3.1 Rekisterinpitäjien neuvonta

Rekisterinpitäjien neuvontaan liittyvät asiat ovat osa tietosuojavaltuutetun toimiston ennaltaehkäisevää toimintaa. Näiden asioiden – kuten ennaltaehkäisevän toiminnan yleensäkin

– merkitys on korostunut henkilötietolain myötä 2000–luvulla. Neuvonta–asioiden lukumäärä onkin moninkertaistunut 1990–luvun lopun tasosta. Kehitystä ilmentää seuraava kuvaaja.



Kuvaaja 7: Rekisterinpitäjien neuvontaa koskevat asiat 1994–2013.

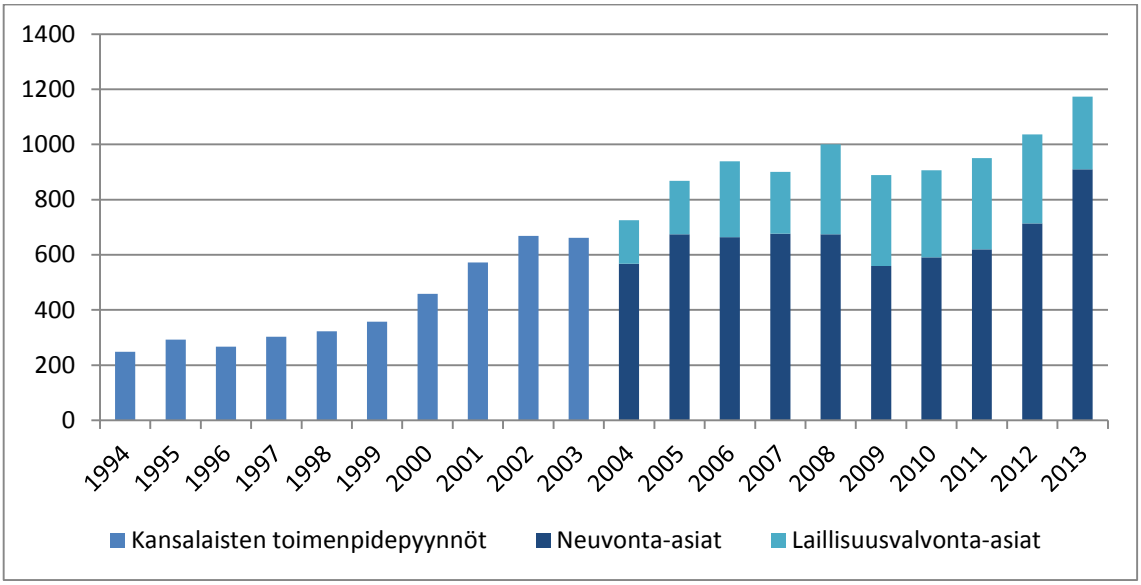
Rekisterinpitäjien neuvontaa koskevat asiat ovat tarkasteluvälillä muodostaneet vähimmillään 10,1 prosentin (1998) ja enimmillään 25,2 prosentin (2007) osuuden kaikista vuoden aikana vireille tulleista asioista. Keskimäärin osuus niin vireille tulleista kuin käsitellyistäkin asioista on ollut koko tarkasteluvälillä noin 17 prosenttia, pelkästään henkilötietolain voimassaoloaikaa tarkasteltaessa pari prosenttiyksikköä enemmän. Myös rekisterinpitäjien neuvonnan suhteellinen osuus kaikista asioista on siis noussut henkilörekisterilain ajoista, joskaan ei yhtä jyrkästi kuin puhtaat asiamäärät. Vuonna 2012 vireille tulleista asioista 19,0 prosenttia koski rekisterinpitäjien neuvontaa, vuonna 2013 16,3 prosenttia.

Henkilötietolain voimaantulo näyttää selvästi ja välittömästi lisänneen neuvonnan tarvetta. Tällaisen nousun voisi kuvitella taittuvan, kunhan uuden lain sisältö on tullut rekisterinpitäjille tutuksi. Näin ei kuitenkaan näytä käyneen, vaan rekisterinpitäjien neuvontaa koskevien asioiden määrän kasvu jatkui yhtäjaksoisesti aina vuoteen 2007 ja muutaman hiljaisemman vuoden jälkeen nousi jälleen uuteen ennätyslukemaan vuonna 2012. Tilastoista ei käy ilmi, minkälaisia kysymyksiä neuvonta–asiat ovat koskeneet. Mahdollinen selitys saattaa löytyä alati kasvavasta erityislainsäädännön määrästä taikka teknologisen kehityksen tai rekisterinpitäjien toiminnan kansainvälistymisen esille nostamista uusista kysymyksistä. Näiden seikkojen ja EU:n uuden tietosuojalainsäädännön voidaan ennakoida pitävän neuvonnan tarvetta yllä myös jatkossa.

2.3.2 Kansalaisten toimenpidepyynnöt

Kansalaisten toimenpidepyynnöt muodostavat ratkaisutoiminnan keskeisimmän ja asiamääriltään merkittävimmän osa–alueen. Toimenpidepyynnöt voidaan jaotella laillisuusvalvonta– ja neuvonta–asioihin. Laillisuusvalvonta–asioista merkittävän alaryhmän muodostavat rekisteröidyn kielto–oikeuden käyttöä koskevat asiat. Kielto–oikeudesta säädetään henkilötietolain 30 §:ssä. Pykälän mukaan rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinointia sekä markkina– ja mielipidetutkimusta samoin kuin henkilömatrikkeleita ja sukututkimusta varten.

Seuraava kuvaaja esittää kansalaisten toimenpidepyyntöjen määrän kehityksen 1990–luvun lopulta lähtien. Vuosien 1994–2003 luvuista on vähennetty niihin sisältyneet tarkastusoikeus– ja virheenoikaisuasiat, joita käsitellään jäljempänä erikseen. Vuodesta 2004 eteenpäin toimenpidepyynnöt on jaoteltu neuvonta– ja laillisuusvalvonta–asioihin.



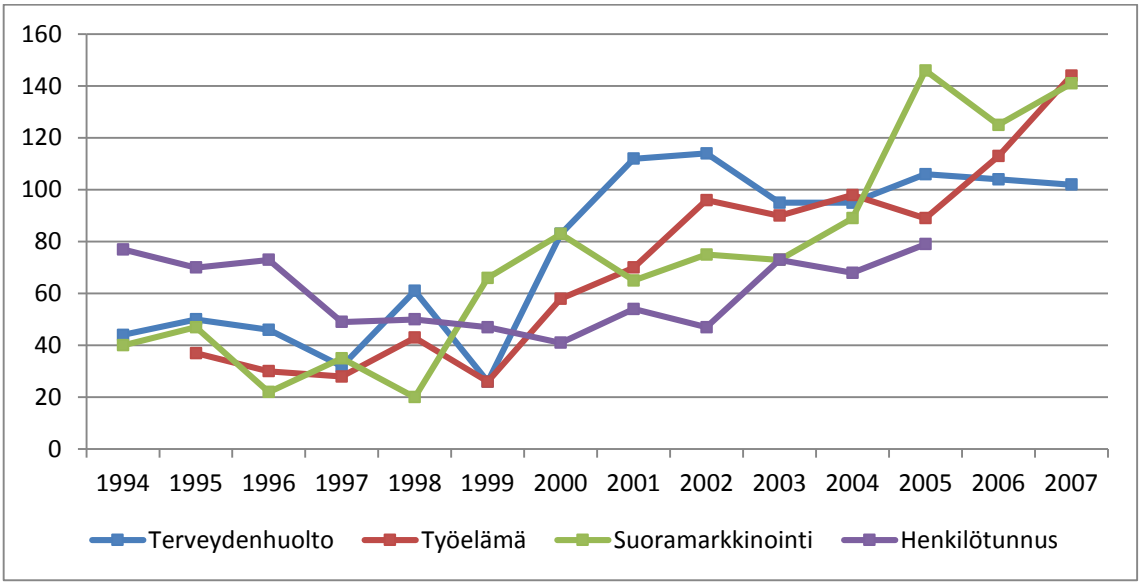
Kuvaaja 8: Vireille tulleiden kansalaisten toimenpidepyyntöjen lukumäärä 1994–2013 ja jakautuminen neuvonta– ja laillisuusvalvonta–asioihin 2004–2013.

Tarkasteluvälillä toimenpidepyyntöjen määrä on kasvanut noin 250:stä lähes 1200 asiaan per vuosi, mutta kasvutahti on hidastunut 2000–luvun ensimmäisen vuosikymmenen lopulla. Kansalaisten toimenpidepyyntöjen osuus kaikista tietosuojavaltuutetun toimiston diarioiduista asioista on merkittävä. Keskimäärin osuus on ollut tarkasteluvälillä vajaat 35 prosenttia. 2010–luvulla vajaa kolmannes tietosuojavaltuutetun toimiston kaikista diarioiduista asioista on koskenut kansalaisten toimenpidepyyntöjä.

Kuvaajassa laillisuusvalvonta–asioista ei ole eroteltu kielto–oikeusasioita. Toimintatilastoista kuitenkin ilmenee, että laillisuusvalvonta–asioiden sisällä kielto–oikeusasioiden suhteellinen määrä on 2010–luvulle tultaessa kasvanut. Vuonna 2009 kielto–oikeusasioita tuli vireille 43

kpl,[127] vuonna 2010 112 kpl, vuonna 2011 160 kpl, vuonna 2012 185 kpl ja vuonna 2013 211 kpl. Näin ollen kielto–oikeusasiat muodostavat jo selvän enemmistön kaikista laillisuusvalvonta–asioista. Kun laillisuusvalvonta–asioiden kokonaismäärä on pysynyt mainittuina vuosina – vuotta 2013 lukuunottamatta – reilussa kolmessasadassa, muiden laillisuusvalvonta–asioiden määrä on siis itse asiassa laskenut viime vuosina. Vuonna 2013 muita laillisuusvalvonta–asioita tilastoitiin enää vain 52.

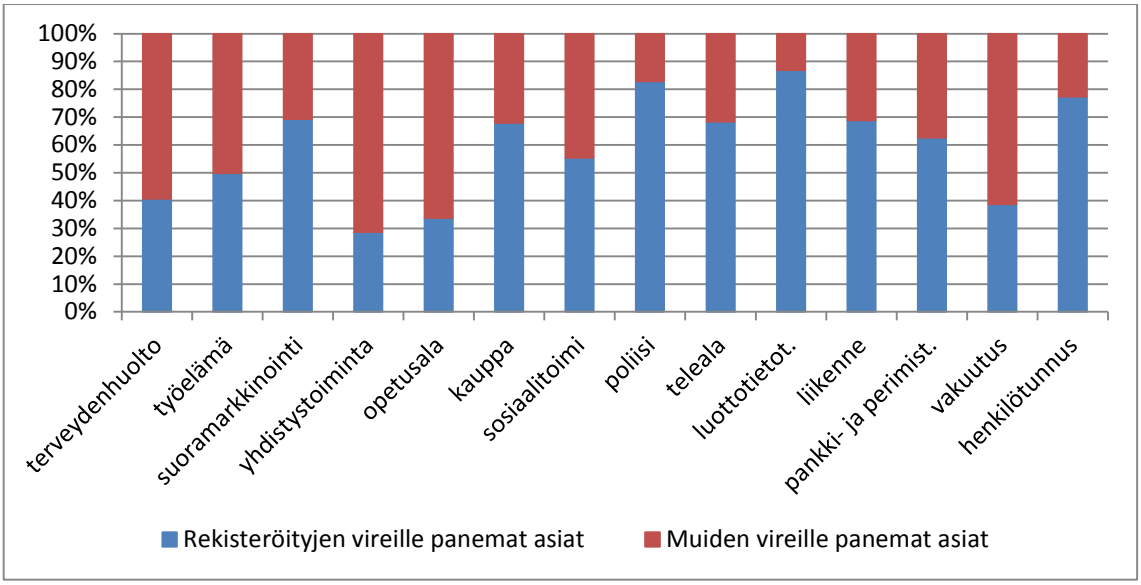
Kansalaisten vireille panemien asioiden määriä tilastoitiin toimialoittain 1990–luvulta aina vuoteen 2007 saakka. Merkittävimmät kansalaisia askarruttaneet asiaryhmät liittyivät terveydenhuoltoon, työelämään ja suoramarkkinointiin. Myös henkilötunnukseen liittyvät asiat kiinnostivat kansalaisia.



Kuvaaja 9: Rekisteröityjen vireille panemien asioiden jakautuminen 1994–2007.[128]

Yllä mainittujen asiaryhmien lisäksi kansalaisten vireille panemissa asioissa edustettuina olivat monet muutkin toimialat. Seuraava kuvaaja kuvaa kansalaisten vireille panemien asioiden toimialakohtaisia prosenttiosuuksia kaikista kutakin toimialaa koskevista asioista.

[127] Luku on otettu vuoden 2010 toimintakertomuksesta (s. 18). Vuosien 2008 ja 2009 toimintakertomuksissa kansalaisten toimenpidepyyntöjen jaottelussa alakategorioihin on epäselvyyksiä. Ennen vuotta 2007 kielto–oikeusasioita ei tilastoitu omana kategorianaan.
[128] Henkilötunnuksia koskevien asioiden määrästä ei ole tietoa vuoden 2005 jälkeen.



Kuvaaja 10: Rekisteröityjen vireille panemien asioiden osuudet kaikista vuosina 2000–2007 vireille tulleista asioista toimialoittain ja henkilötunnusta koskevista, vuosina 2000–2005 vireille tulleista asioista.

Kuten kuvaajasta näkyy, kansalaisten vireille panemien asioiden osuus on ollut erityisen suuri luottotietotoimintaa, poliisia ja henkilötunnusta koskevissa asioissa. Myös suoramarkkinointia, kauppaa, telealaa ja pankki– ja perimistoimintaa koskevista asioista reilusti yli puolet tuli vireille rekisteröidyn toimesta. Sen sijaan yhdistystoiminnassa sekä opetus– että vakuutusalalla selvä enemmistö asioista tulee vireille jonkun muun, yleensä siis rekisterinpitäjän aloitteesta. Näyttääkin siltä, että toimialoilla, joilla kansalaisen yleinen asema suhteessa toiminnan harjoittajaan (joka on samalla rekisterinpitäjä) on heikko tai alisteinen taikka joilla kansalainen on omasta tahdostaan riippumatta lähinnä toiminnan kohde, yhteydenoton tietosuojavaltuutettuun tekee useammin kansalainen. Aloilla, joilla kansalaiset toimivat ennemminkin vapaaehtoisluonteisessa yhteistyössä toiminnan harjoittajien kanssa, kansalaisten osuus yhteydenotoista on pienempi.

2.3.3 Tarkastusoikeus– ja virheenoikaisuasiat

2.3.3.1 Tietosuojavaltuutetun toimistossa

Eräänlaisista kansalaisten toimenpidepyynnöistä on kyse myös tarkastusoikeus– ja virheenoikaisuasioissa, joita kuitenkin käsitellään tässä erikseen. Rekisteröidyn tarkastusoikeudesta säädetään henkilötietolain 26 §:ssä, jonka 1 momentin mukaan jokaisella on salassapitosäännösten estämättä oikeus tiedon etsimiseksi tarpeelliset seikat ilmoitettuaan saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on talletettu tai, ettei rekisterissä ole häntä koskevia tietoja. Henkilötietolain 27 §:ssä säädetään tarkastusoikeuden rajoituksista ja 28 §:ssä tarkastusoikeuden toteuttamisesta, missä pääsääntönä on pyynnön esittäminen ensin rekisterinpitäjälle, jonka kieltäytyessä rekisteröity voi saattaa asian tietosuojavaltuutetun

käsiteltäväksi. Myös erityislainsäädännössä on tarkastusoikeuden sisältöä rajaavaa ja toteuttamista koskevaa sääntelyä, ja eräiden, erityisesti poliisitoiminnassa käytettävien rekistereiden tarkastaminen on mahdollista vain välillisesti tietosuojavaltuutetun toimesta.[129] Rekisterinpitäjän velvollisuudesta oikaista, poistaa tai täydentää rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto on säädetty henkilötietolain 29 §:ssä. Myös tiedon korjaamiseen liittyy erityissäännöksiä.[130] EU–tasolla tarkastusoikeus ja oikeus saada tiedot oikaistuksi perustuvat henkilötietodirektiivin 12 ja 13 artikloihin.[131]

Henkilötietolain 40.2 §:n mukaan tietosuojavaltuutetun on ratkaistava asia, jonka rekisteröity on saattanut lain 28 ja 29 §:n nojalla hänen käsiteltäväkseen, ja hän voi antaa rekisterinpitäjälle määräyksen rekisteröidyn tarkastusoikeuden toteuttamisesta tai tiedon korjaamisesta. Henkilötietolain 45.1 §:stä johtuu, että tietosuojavaltuutetun päätökset tarkastusoikeus– ja virheenoikaisuasioissa ovat sitovia ja niistä voidaan valittaa suoraan hallinto–oikeuteen. Lisäksi henkilötietolain 46 §:ssä säädetään, että tietosuojavaltuutettu voi tehostaa määräystään tarpeen mukaan uhkasakkolain (1113/1990) mukaisella uhkasakolla.

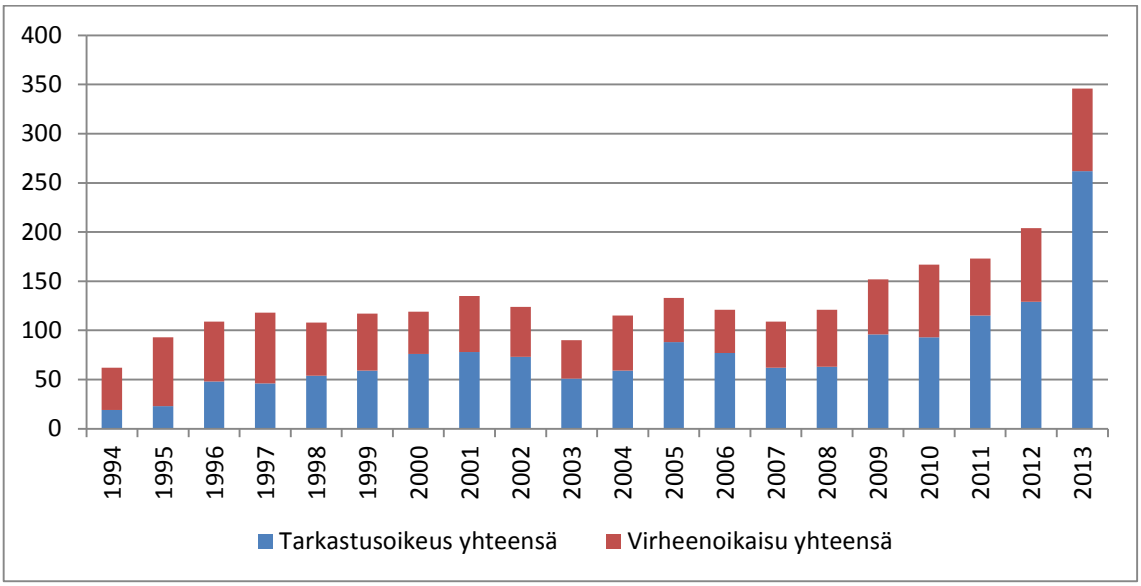
Vanhan henkilörekisterilain 35.1 §:n mukaan tietosuojavaltuutettu saattoi niin ikään rekisteröidyn hakemuksesta antaa rekisterinpitäjälle määräyksen rekisteröidyn tarkastusoikeuden toteuttamisesta ja rekisterissä olevan virheen oikaisusta. Määräys kuitenkin raukesi, jos rekisterinpitäjä ilmoitti vastustavansa määräyksen antamista asetetussa, tiedoksisaannista lukien vähintään kahdeksan päivän määräajassa. Tämän jälkeen tietosuojavaltuutetulla ja rekisteröidyllä oli mahdollisuus saattaa asia tietosuojalautakunnan käsiteltäväksi (HRek 35.2 §).

Tietosuojavaltuutetun päätösten muuttuminen sitoviksi ja suoraan valituskelpoisiksi henkilötietolain voimaan tullessa ei tuonut välitöntä muutosta asioiden määrään, vaan 1990–luvun lopun ja 2000–luvun alun asiamäärät olivat kutakuinkin samaa tasoa. Aina vuoteen 2008 saakka vireille tulleiden tarkastusoikeus– ja virheenoikaisuasioiden yhteenlaskettu määrä pysyi noin 120 asiassa vuosittain. Asioita myös käsiteltiin vuosittain kutakuinkin sama määrä kuin niitä tuli vireille. Tarkastusoikeusasioiden osuus on ollut 2000–luvulla jatkuvasti suurempi kuin virheenoikaisuasioiden. 1990–luvun lopulla suhde oli vielä tasainen ja 1990–luvun puolivälin tienoilla virheenoikaisuasioita oli jopa moninkertaisesti enemmän kuin tarkastusoikeusasioita.

[129] Ks. esimerkiksi laki henkilötietojen käsittelystä poliisitoimessa (761/2003) 44–45, 47 §, laki henkilötietojen käsittelystä rajavartiolaitoksessa (579/2005) 41–42 § ja TSV:n toimisto, Henkilörekisteriin talletettujen tietojen tarkastaminen (2014). Rekisteröity itse ei voi saada nähtäväkseen välillisen tarkastusoikeuden piirissä oleviin rekistereihin mahdollisesti tallennettuja, itseään koskevia tietoja, mutta tietosuojavaltuutettu voi tämän pyynnöstä tarkastaa tietojen lainmukaisuuden.
[130] Ks. TSV:n toimisto, Henkilörekisteriin tallennetun tiedon korjaaminen (2010).
[131] Oikaisumahdollisuuden ulottamisesta internetin hakukoneisiin ks. EUT 13.5.2014, C–131/12.

Vuoden 2008 jälkeen tarkastusoikeus– ja virheenoikaisuasioiden määrä on kuitenkin noussut selkeästi. Kasvua on ollut sekä myös virheenoikaisuasioiden määrässä, mutta etenkin tarkastusoikeusasioissa, joiden määrä oli vuonna 2013 jo yli nelinkertainen virheenoikaisuasioihin verrattuna. Jo vuotta aiemmin pelkästään tarkastusasioiden määrä ylitti 2000–luvun alun tarkastusoikeus– ja virheenoikaisuasioiden yhteenlasketun määrän, ja vuonna 2013 tarkastusoikeusasioiden määrä yli kaksinkertaistui. Myös virheenoikaisuasioiden lukumäärä kasvoi edellisvuodesta.

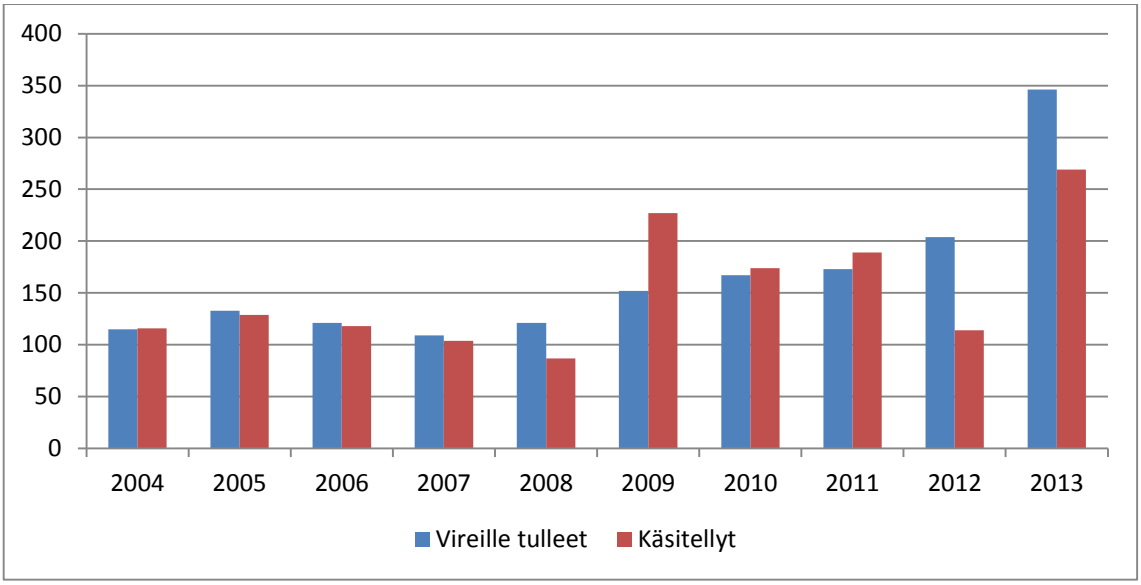
Seuraava kuvaaja esittää tarkastusoikeus– ja virheenoikaisuasioiden kokonaismäärän ja keskinäisen jakauman 1990–luvun puolivälistä vuoteen 2013.



Kuvaaja 11: Vireille tulleet tarkastusoikeus– ja virheenoikaisuasiat 1994–2013.

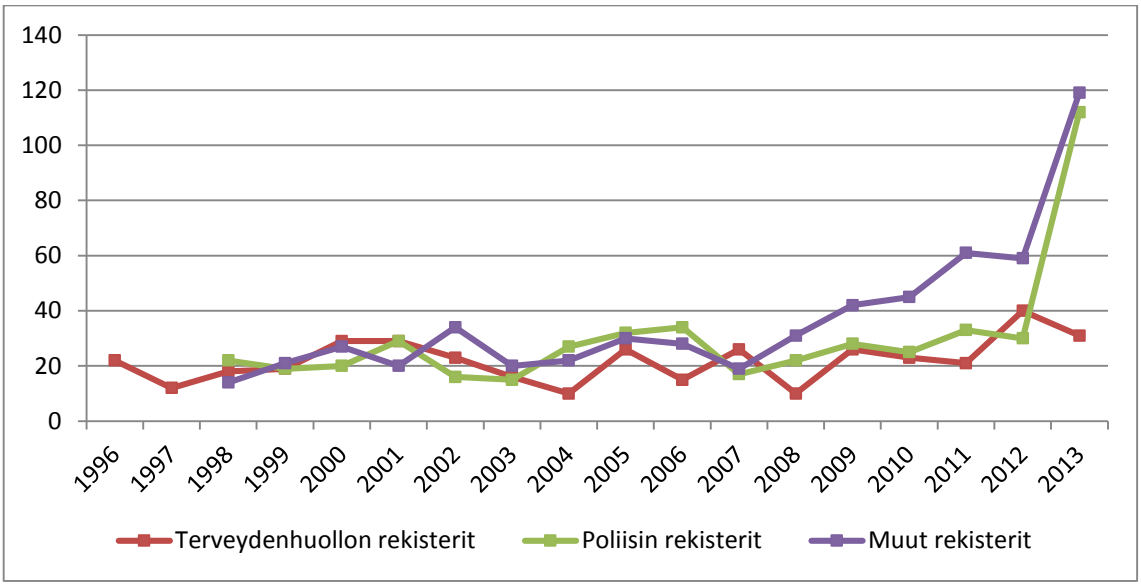
Tarkastusoikeus– ja virheenoikaisuasioiden osuus kaikista tietosuojavaltuutetun toimiston käsittelemistä asioista on pienehkö. 2000–luvun alussa se oli hivenen alle kymmenesosa. Tällä vuosituhannella muiden asioiden osuus on kasvanut suhteessa enemmän kuin tarkastusoikeus– ja virheenoikaisuasioiden, ja 2010–luvulla niiden osuus on ollut vain noin kuudesta seitsemään prosenttia kaikista vireille tulleista asioista. Vähimmillään vuonna 2008 vain neljä ja puoli prosenttia kaikista vireille tulleista asioista oli tarkastusoikeus– ja virheenoikaisuasioita.

Seuraavasta kuvaajasta käy ilmi vireille tulleiden ja käsiteltyjen tarkastusoikeus– ja virheenoikaisuasioiden lukumäärien ero vuodesta 2004 lähtien. Käsiteltyjen asioiden määrässä on ollut huomattavasti suurempaa vuosikohtaista vaihtelua kuin vireille tulleiden asioiden määrässä.



Kuvaaja 12: Tarkastusoikeus– ja virheenoikaisuasiat 2004–2013.

Tarkastusoikeus– ja virheenoikaisuasioita on tilastoitu myös rekisteritoiminnan alan mukaisesti. Henkilötietolain voimassa ollessa tarkastusoikeusasioissa tilastokategorioina ovat olleet terveydenhuollon rekisterit, poliisin rekisterit ja muut rekisterit. Virheenoikaisuasiat on jaettu terveydenhuollon rekistereitä, luottotietorekistereitä ja muita rekistereitä koskeviin.[132] Seuraavat kaksi kuvaajaa esittävät vireille tulleiden tarkastusoikeus– ja virheenoikaisuasioiden jakautumisen näihin kategorioihin.

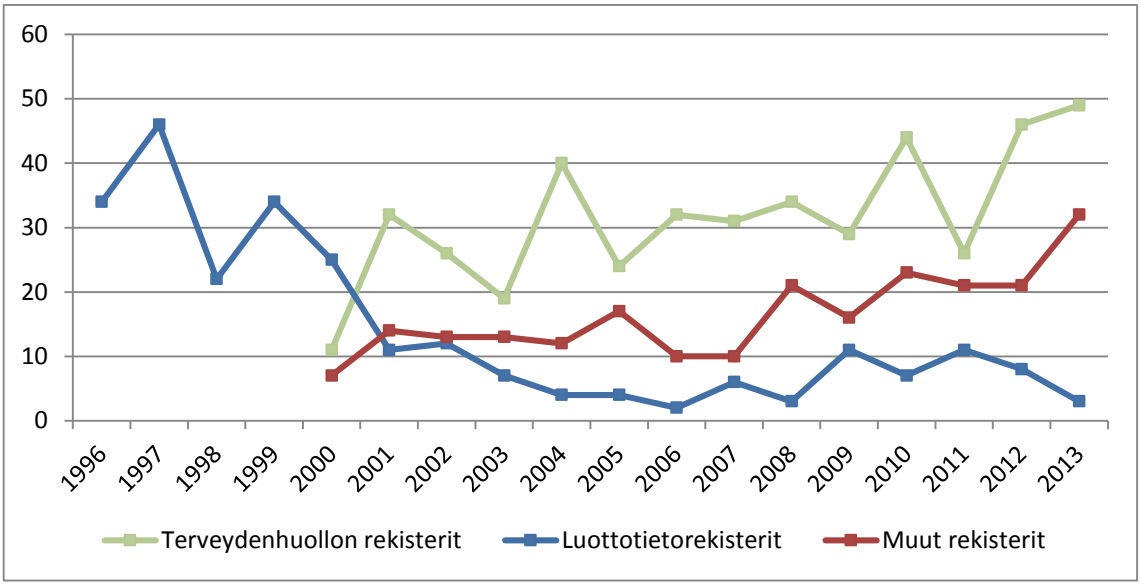


Kuvaaja 13: Vireille tulleiden tarkastusoikeusasioiden rekisterialoittainen jakauma 1998–2013 ja terveydenhuollon rekistereitä koskevien asioiden määrä 1996–2013.

Tarkastusoikeusasioiden määrän kasvu on kohdistunut erityisesti muut rekisterit –kategoriaan, terveydenhuollon ja poliisin rekistereiden suhteen kansalaisten tarkastusinto on säilynyt melko

[132] Tilastoinnissa ei ole eroteltu julkisen ja yksityisen terveydenhuollon rekisterinpitoa.

tasaisena. Vuoteen 2007 asti kolmen tilastokategorian osuudet pysyivät varsin lähellä toisiaan, mutta viime vuosina muiden rekistereiden osuus on noussut lähes tai jopa yli puoleen kaikista tarkastusoikeusasioista. Vuonna 2013 kiinnostus poliisin rekistereitä kohtaan kasvoi julkisuudessa esillä olleiden tapausten myötävaikutuksesta ja asioita tuli vireille tuli 112, mikä oli 42,7 prosenttia kaikista tarkastusoikeusasioista. Eniten uusia asioita tilastoitiin kuitenkin edelleen muut rekisterit –kategoriaan, jossa vireille tuli 119 asiaa (45,4 %). Terveydenhuollon rekistereitä koskevia tarkastusoikeusasioita sen sijaan oli 31 kappaletta (11,8 %), mikä oli edellisvuotta vähemmän.



Kuvaaja 14: Vireille tulleiden virheenoikaisuasioiden rekisterialoittainen jakauma 2000–2013 ja luottotietorekistereitä koskevien asioiden määrä 1996–2013.

1990–luvun lopun ja 2000–luvun lopun kehityslinjana on havaittavissa luottotietorekistereitä koskevien virheenoikaisujen määrän jyrkkä lasku lamavuosien jälkeen. *Vesa Muttilaisen* mukaan tämä johtui luottotietoalan pelisääntöjen selkeytymisestä.[133] Vähimmillään vireille tuli vain kaksi luottotietorekisterissä olevan tiedon korjaamista koskevaa asiaa. Uuden luottotietolain säätämisen jälkeisenä aikana tapauksia on ollut vuosittain muutamasta hieman yli kymmeneen. Tason hienoiseen nousuun on todennäköisesti vaikuttanut yleisen taloustilanteen uusi kiristyminen. 1990–luvun kaltaisia lukemia ei kuitenkaan ole hätyytelty, ja suunta on ollut taas laskussa viimeiset kaksi vuotta.

2000–luvulla on havaittavissa nouseva trendi terveydenhuollon rekistereitä koskevien virheenoikaisuasioiden osalta. Terveydenhuollon rekisterit muodostavatkin selvästi suurimman tapausryhmän vuodesta 2001 lähtien. Muita rekistereitä koskevien virheenoikaisuasioiden määrässä ei ole havaittavissa viime vuosina yhtä selvää nousua kuin tarkastusoikeusasioissa. Muita rekistereitä koskevien asioiden määrä on kuitenkin keskimäärin kasvanut 2000–luvulla. Prosentuaalisesti kaikkien kategorioiden vaihtelut ovat olleet suuria,

[133] *Muttilainen*, Suomalaiset ja henkilötietojen suoja (2006) s. 54. Ks. myös TK 2004 s. 15.

mutta asiamäärissä mitaten melko vähäisiä. Vuoden 2012 84 tarkastusasiasta 49 kpl (58,3 %) koski terveydenhuollon rekistereitä, 3 kpl (3,6 %) luottotietorekistereitä ja 32 kpl 38,1 %) muita rekistereitä.

Tarkastusoikeus– ja virheenoikaisuasioista varsin harva johtaa tietosuojavaltuutetun rekisterinpitäjälle antamaan määräykseen. 2000–luvun puolenvälin tienoilla määräyksiä annettiin vuosittain muutamasta noin kymmeneen. Usein rekisterinpitäjä antaa tiedot tai tekee korjauksen asian tultua vireille ilman, että tietosuojavaltuutetun on tarve antaa määräystä.[134]

2.3.3.2 Muutoksenhaku tietosuojavaltuutetun päätöksistä

Tarkastusoikeus– ja virheenkorjausasiat ovat ainoa asiaryhmä, jossa tietosuojavaltuutettu tekee sitovia, valituskelpoisia päätöksiä. Päätöksistä voi valittaa hallinto–oikeuteen ja korkeimpaan hallinto–oikeuteen hallintolainkäyttölain (586/1996) mukaisesti (HetiL 28, 29, 40.2 ja 45.1 §). Muutamia korkeimman hallinto–oikeuden tarkastusoikeus– ja virheenkorjausasioita koskevia ratkaisuja on julkaistu Finlex–tietokannassa ja Tietosuoja.fi –sivustolla.[135] Nämä tapaukset on esitelty lyhyesti seuraavassa:

> **KHO 23.4.2001 T 926**. Tietosuojavaltuutettu ei ollut antanut rekisterinpitäjälle tarkastusoikeuden toteuttamista koskevaa määräystä, koska hakija oli jo saanut häntä koskevat tiedot, ja tarkastusoikeutta ei ollut hakijalle annetussa jäljennöksessä peitettyihin, muuta henkilöä kuin hakijaa koskeviin tietoihin. Hallinto–oikeus ja korkein hallinto–oikeus hylkäsivät hakijan valitukset.
>
> **KHO 18.8.2006 T 1976**. Korkein hallinto–oikeus päätyi toiseen lopputulokseen kuin tietosuojavaltuutettu, joka oli määrännyt yksityisen eläkelaitoksen asiantuntijalääkärin sisäisen käsittelyn muistioon tekemät merkinnät virheellisinä poistettaviksi. KHO:n mukaan mitään tiedoista ei voitu määrätä poistettavaksi. Hallinto–oikeus oli määrännyt osan tiedoista poistettavaksi.
>
> **KHO 27.2.2007 T 457**. Tietosuojavaltuutettu oli määrännyt pankin antamaan X:lle tiedon kaikista tätä koskevista, rekisterissään olevista henkilötiedoista, myös lainojen tapahtumaerittelyistä korkoprosentteineen. Hallinto–oikeus kumosi määräyksen tarkastusoikeuden ulottamisesta korkoprosenttitietoihin. Korkein hallinto–oikeus hyväksyi tietosuojavaltuutetun valituksen.
>
> **KHO 26.3.2007 T 761**. Asiassa oli kyse siitä, oliko Patentti– ja rekisterihallituksella valitusoikeus päätöksestä, jolla tietosuojavaltuutettu oli rekisteröidyn hakemuksesta henkilötietolain 29 ja 40.2 §:n nojalla velvoittanut PRH:n poistamaan kaupparekisterissä olevan merkinnän. Hallinto–oikeuden mukaan PRH:lla ei ollut sille rekisterinpitäjänä kuuluvien tehtävien perusteella asianosaisen asemaa eikä PRH:lla ollut myöskään valvottavana sellaista julkista etua, jota varten hallintolainkäyttölain 6.2 §:n mukainen

[134] Tietosuojavaltuutetun tarkastusoikeus– ja virheenoikaisuasioissa antamista päätöksistä ks. VK 2005 s. 31–32, VK 2006 s. 56–57, KT 2007 s. 28–30 (TSV Dnro 333/523/2006), KT 2008 s. 29–31, KT 2011 s. 16–19 (TSV 10.5.2011 Dnro 2680/41/2010) ja KT 2012 s. 24–29 (TSV Dnro 1113/523/2012 ja TSV Dnro 1160/533/2012). Ks. myös tarkastusoikeuden toteuttamista internetissä koskeva kannanotto VK 2005 s. 30 (TSV Dnro 1164/41/2005) ja Tietosuoja.fi –sivustolla julkaistut päätökset ja kannanotot TSV 16.8.2000 Dnro 649/41/2000, TSV 18.1.2001 Dnro 36/523/2001, TSV 19.3.2001 Dnro 1196/523/2000, TSV 27.4.2001 Dnro 1119/523/2000, TSV 15.8.2001 Dnro 403/45/2001, TSV 28.9.2001 Dnro 810/45/2001 ja TSV 12.1.2006 Dnro 1950/533/2005

[135] Ks. http://www.tietosuoja.fi/fi/index/ratkaisut/korkeimmanhallinto–oikeudenpaatokset.html, viitattu 9.5.2014.

valitusoikeus olisi tarpeen (Kuopion HAO 1.11.2006 T 06/0645/3). KHO:n mukaan PRH:lla oli valitusoikeus hallintolainkäyttölain 6.1 §:n nojalla, koska PRH:lle oli annettu sitä rekisterinpitäjänä velvoittava määräys rekisterissä olevan merkinnän poistamisesta, ja tietosuojavaltuutetun päätös oli näin ollen kohdistettu PRH:een. KHO palautti asian hallinto–oikeudelle.

KHO 2007:20. Vuosikirjaratkaisussa kyse oli valitustiestä rekisterinpitäjänä toimineen ministeriön ilmoitettua virheenoikaisusta kieltäytymisestä. Ratkaisun otsikko kuuluu seuraavasti: ”Sisäasiainministeriö oli ilmoittanut rekisteröidylle poliisiasiain tietojärjestelmä –nimisen henkilörekisterin rekisterinpitäjänä, että se ei hyväksy tämän tekemää tiedon korjaamista koskevaa vaatimusta. Ministeriön henkilötietolain 29 §:n 2 momentissa tarkoitetun ilmoituksen lainmukaisuus voitiin saattaa henkilötietolain 29 §:n 2 momentin ja 40 §:n 2 momentin mukaan tietosuojavaltuutetun käsiteltäväksi. Ilmoitus ei tähän nähden sisältänyt sellaista hallintopäätöstä, johon voitiin hakea muutosta valittamalla korkeimpaan hallinto–oikeuteen hallintolainkäyttölain 7 §:n mukaan.” KHO siirsi asian tietosuojavaltuutetun käsiteltäväksi.

KHO 13.11.2008 T 2861. Tietosuojavaltuutettu oli A:n pyynnöstä velvoittanut Patentti– ja rekisterihallituksen poistamaan kaupparekisteristä virheellisen merkinnän, jonka mukaan A olisi ollut X Oy:n toimitusjohtajana 26.6.2003–25.3.2004. PRH:n mielestä asiaan olisi tullut soveltaa kaupparekisterilain 22 ja 23 §:n säännöksiä, joiden mukaan virheellisen merkinnän poistamiseen tarvitaan yleisen tuomioistuimen ratkaisu. Hallinto–oikeus hylkäsi PRH:n valituksen eikä KHO muuttanut tätä lopputulosta, vaan katsoi että henkilötietolain 29 ja 40.2 §:n säännöksiä oli voitu soveltaa kaupparekisterilakia täydentävästi.[136]

KHO 2012:51. A oli pyytänyt tietosuojavaltuutettua tarkastamaan keskusrikospoliisin SIRENE–toimiston pitämässä Schengen–rekisterissä hänestä olevien tietojen lainmukaisuuden ja pyytämään keskusrikospoliisia poistamaan häntä koskevat virheelliset tiedot. Tietosuojavaltuutettu oli paitsi todennut, että A:ta koskevat tiedot oli poistettu Schengenin tietojärjestelmästä ja kansallisesta Schengen–tietojärjestelmästä, käsitellyt A:n vaatimuksen hänen virheellisinä pitämiensä merkintöjen korjaamisesta SIRENE–asiankäsittelyjärjestelmän arkistotietokantaan sisältyvien merkintöjen osalta ja hylännyt vaatimuksen. A valitti tietosuojavaltuutetun päätöksestä hallinto–oikeuteen ja edelleen korkeimpaan hallinto–oikeuteen, jotka molemmat hylkäsivät valitukset.[137]

KHO 27.9.2013 T 3084. Tietosuojavaltuutettu oli antanut henkilötietolain 40.2 §:n mukaisen määräyksen tarkastusoikeuden toteuttamisesta potilaan tutkimuksessa käytettävän laitteen tapahtumalokissa olevista tiedoista. KHO ei katsonut tapahtumalokin muodostavan henkilörekisteriä, eikä tietosuojavaltuutettu siten ollut voinut antaa määräystä laitteen teknisten tietojen ja laitteen toimintaan liittyvien tietojen osalta.

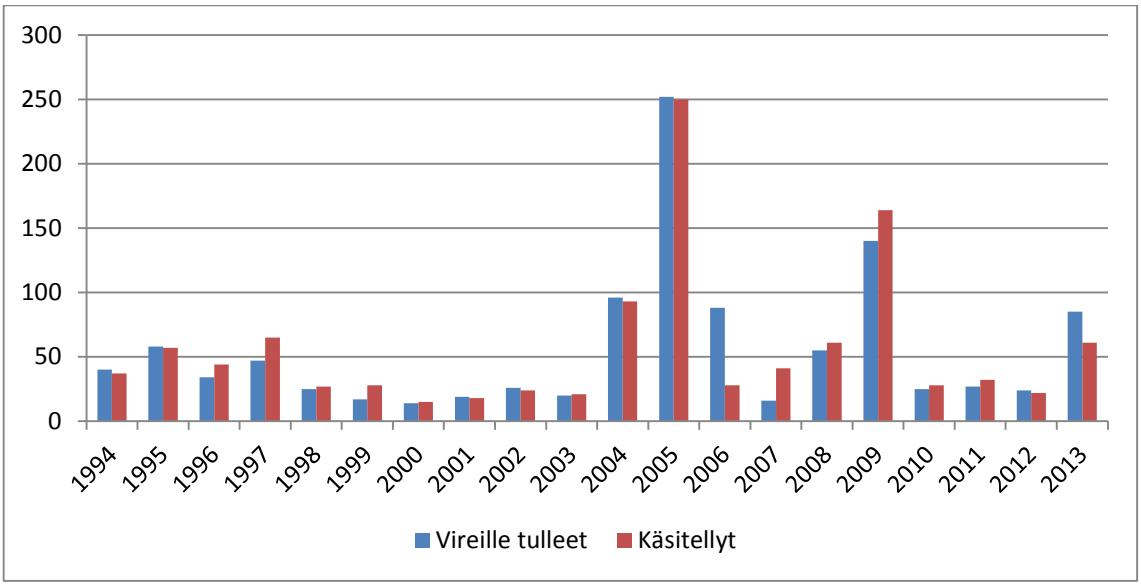
Selostetuista tapauksista neljässä korkein hallinto–oikeus päätyi asiallisesti samaan lopputulokseen kuin tietosuojavaltuutettu. Kahdessa tapauksessa se muutti tietosuojavaltuutetun päätöstä, molemmissa suhtautuen tarkastusoikeuteen tai virheenoikaisuun tietosuojavaltuutettua rajoittavammin. Ratkaisuista kaksi koski menettelyllisiä kysymyksiä – valitustietä ja valitusoikeutta tarkastusoikeus– ja

[136] Finlexissä ks. Kuopion HAO 7.6.2007 T 07/0220/3.
[137] Ks. myös samaa asiaa koskeva välipäätös KHO 2012:3.

virheenoikaisuasioissa. Siten ne eivät sisältäneet sisällöllistä kannanottoa tietosuojavaltuutetun asiassa tekemään päätökseen.[138]

2.3.4 Tietosuojavaltuutetun vireille panemat asiat

Tietosuojavaltuutettu voi laittaa asioita vireille tarpeen mukaan myös oma–aloitteisesti. Lähinnä tämä tulee kysymykseen tarkastustoimintaan liittyen. Seuraava kuvaaja esittää tietosuojavaltuutetun aloitteesta vireille tulleiden asioiden määrät vuosina 1994–2013.



Kuvaaja 15: Tietosuojavaltuutetun oma–aloitteisesti vireille panemat asiat 1994–2013.

Oma–aloitteisten vireillepanojen määrä on vaihdellut eri vuosina melko suurella vaihteluvälillä, alle 20:stä noin 250:een. Kuvaajassa näkyviä piikkejä selittävät eri selvitysprojektit ja toisaalta ilmeisesti myös vaihtelevat tilastointitavat. Vuonna 2005 selvitettiin teleyritysten ja puhelinluettelo–, tilaajaluettelo– ja numerotiedotuspalvelua tarjoavien yritysten ilmoittamis– ja huolehtimisvelvollisuuden hoitamista (143 kohdetta) ja henkilöarviointia suorittavien yritysten tietoisuutta henkilötietojen suojaan liittyvistä velvoitteistaan (89 kohdetta). Vuoden 2009 piikki taas selittyy markkina– ja mielipidetutkimusten tekemistä koskevalla toimialaselvityksellä, jonka yhteydessä lähetettiin kysely sadalle alan yritykselle. Erilaisia etätarkastuksia, selvityksiä ja kyselyitä on toteutettu myös muina vuosina, mutta yleensä jokaista eri rekisterinpitäjälle lähetettyä kyselyä ei ole diarioitu omaksi asiakseen.[139]

---

[138] Menettelyllinen puoli oli myös tapauksessa KHO 2012:51, jossa korkeimman hallinto–oikeuden mukaan tietojen korjaamista tai poistamista koskevan vaatimuksen käsittely ei arkistotietokannan osalta olisi vielä ensi asteessa kuulunut tietosuojavaltuutetun, vaan rekisterinpitäjän toimivaltaan. Tämän vuoksi hallinto–oikeuden ja tietosuojavaltuutetun päätökset olisi tullut osin kumota ja asia siirtää Poliisihallituksen käsiteltäväksi siltä osin kuin A oli vaatinut häntä koskevien virheellisten merkintöjen poistamista arkistotietokannasta. KHO kuitenkin käsitteli asian itse viivytyksen välttämiseksi

[139] TK 2005 s. 16, TK 2009 s. 13 ja tietosuojavaltuutetun toimiston julkiset diaaritiedot. Ks. myös II.6.2.

Tietosuojavaltuutetun omien vireillepanojen osuus on siis ollut yleensä varsin pieni kaikista asioista, keskimäärin muutaman prosentin luokkaa. Vuoden 2005 selvitysprojektit nostivat osuuden poikkeuksellisesti kymmenykseen kaikista asioista. 2010–luvulla osuus on ollut noin prosentti, vuonna 2013 noin kaksi prosenttia.

2.3.5 Lausunnot syyttäjille ja tuomioistuimille rikosasioissa

Henkilörekisterilain vastaista toimintaa on sanktioitu rikosoikeudellisesti sekä rikoslaissa että henkilötietolaissa. Keskeisin henkilötietolain vastaista menettelyä koskeva rikosnimike on henkilörekisteririkos (RL 38:9).[140] Siihen voi syyllistyä ensinnäkin käsittelemällä henkilötietoja vastoin henkilötietolain säännöksiä[141] taikka rikkomalla henkilötietojen käsittelyä koskevia erityissäännöksiä. Toiseksi henkilörikokseen voi syyllistyä siten, että antamalla rekisteröidylle väärän tai harhaanjohtavan tiedon estää tai yrittää estää rekisteröityä käyttämästä hänelle kuuluvaa tarkastusoikeutta. Lisäksi henkilörekisteririkoksena voidaan rangaista henkilötietojen siirtäminen EU/ETA–alueen ulkopuolelle henkilötietolain 5 luvun vastaisesti. Jokaisessa tekotavassa edellytetään törkeää huolimattomuutta tai tahallisuutta ja sitä, että teko loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa. Henkilörekisteririkoksesta voidaan tuomita sakko tai vankeutta enintään yksi vuosi.

Muita henkilötietolain vastaista toimintaa koskevia rikosnimikkeitä ovat tietomurto (RL 38:8) kun se kohdistuu henkilörekisteriin, sekä henkilötietolain 33 §:n säädetyn salassapitovelvollisuuden rikkomisen osalta salassapitorikos ja –rikkomus (RL 38:1–2) sekä virkasalaisuuden rikkominen ja virkasalaisuuden tuottamuksellinen rikkominen (RL 40:5).[142] Henkilötietolain 48.1 § sisältää viittauksen näihin pykäliin.

Lisäksi lain 48.2 §:ssä on säännös henkilörekisteririkkomuksesta.[143] Tähän vain sakolla rangaistavaan, henkilörekisteririkosta lievempään tekoon voi syyllistyä vaarantamalla tahallaan tai törkeästä huolimattomuudesta rekisteröidyn yksityisyyden suojaa tai oikeuksia momentissa mainituilla tavoilla. Näitä ovat eräiden muiden kuin henkilörekisteririkoksen tunnusmerkistössä mainittujen määräysten noudattamisen laiminlyöminen, väärien tai harhaanjohtavien tietojen antaminen tietosuojaviranomaisille ja tietosuojalautakunnan

[140] Henkilörekisteririkosta koskeva säännös oli alun perin HRekL 43 §, joka siirrettiin vuonna 1995 rikoslakiin.
[141] Näitä asioita ovat käyttötarkoitussidonnaisuutta (HetiL 7 §), käsittelyn yleisiä edellytyksiä (HetiL 8 §), henkilötietojen tarpeellisuutta tai virheettömyyttä (HetiL 9 §), arkaluonteisia tietoja (11 §), henkilötunnusta (13 §) ja henkilötietojen käsittelyä erityisiä tarkoituksia varten (14–19 §) koskevat säännökset.
[142] Henkilörekisterilaissa määritettiin ennen vuotta 1995 rangaistukset myös henkilörekisteriin tunkeutumisesta ja henkilörekisteriä koskevan salassapitovelvollisuuden rikkomisesta (HRekL 45 ja 46 §). Vastaavista teoista rangaistaan nyt mainittujen rikoslain säännösten perusteella.
[143] Henkilörekisterilaissa henkilörekisteririkkomusta koski lain 44 §.

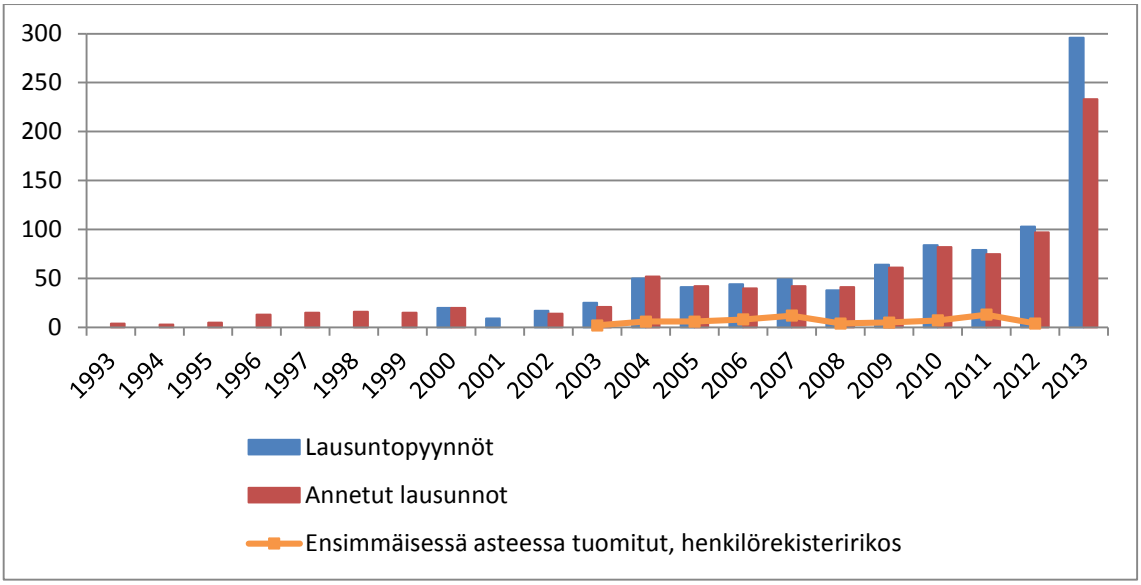
määräysten rikkominen. Henkilörekisteririkkomuksena rangaistaan myös henkilötietojen suojaamisesta tai hävittämisestä annettujen säännösten ja määräysten rikkominen.[144]

Henkilötietolain 41.2 §:n mukaan syyttäjän on ennen henkilötietolain vastaista menettelyä koskevan syytteen nostamista kuultava tietosuojavaltuutettua, ja tuomioistuimen on tällaista asiaa käsitellessään varattava tietosuojavaltuutetulle tilaisuus tulla kuulluksi. Käytännöissä nämä lausuntoasiat koskevat siis edellä mainittuja tekoja ja rikosnimikkeitä. Ennen henkilötietolain voimaantuloa vastaava säännös oli henkilörekisterilain 47 §.

Lausuntopyynnöt syyttäjiltä ja tuomioistuimilta ovat 2000–luvulla yleistyneet selvästi. Muutos ei kuitenkaan ilmennyt välittömästi henkilötietolain voimaan tullessa, mikä on ymmärrettävää, sillä vanha henkilörekisterilain 47 § vastasi sisällöllisesti henkilötietolain 41.2 §:ää. Vuosina 1997–1999 tietosuojavaltuutettu antoi rikosasioissa viitisentoista lausuntoa vuodessa. Vuodesta 2000 vuoteen 2012 lausuntopyyntöjen vuosittainen määrä oli kasvanut yli kahdeksallakymmenellä ja siten viisinkertaistunut. Vuonna 2013 määrä edelleen lähes kolminkertaistui, mihin toimintakertomuksenkin mukaan osasyynä oli eräs julkisuudessa esillä ollut yksittäistapaus.[145] Lausuntopyyntöjen määrän kasvu ei todennäköisesti niinkään kerro henkilötietojen käsittelyä koskevan rikollisuuden määrän kasvusta, vaan ennemminkin tietoisuuden lisääntymisestä ja rikollisuuden kasvavasta esilletulosta. Henkilötietojen käsittelyyn liittyvän piiloon jäävän rikollisuuden määrän (ns. *Dunkelziffer*) voidaan silti edelleen arvella olevan korkea.

Annettujen lausuntojen määrä on kasvanut suurin piirtein samaa tahtia lausuntopyyntöjen kanssa, mutta vuonna 2013 toimisto ei aivan kyennyt vastaamaan lausuntomäärän räjähdysmäiseen kasvuun. Annettujen lausuntojen määrä jäi huomattavasti lausuntopyyntöjen määrästä. Jos lausuntopyyntöjen määrä vakiintuu vuoden 2013 tasolle tai kasvu jopa jatkuu, tulee tällä olemaan huomattava vaikutus toimiston työmäärään.

[144] Lainsäätäjän muutenkin vähäisestä mielenkiinnosta tietoturvaa kohtaan kertonee, että henkilötietolain 32 §:n suojaamisvelvoitteen laiminlyönnin seurauksena on siten vain sakko henkilörekisteririkkomuksesta. – Rangaistussäännöksistä yleisesti ks. myös *Pitkänen – Tiilikka – Warma*, Henkilötietojen suoja (2013) s. 287–307.
[145] TK 2013 s. 16.



Kuvaaja 16: Lausuntopyynnöt syyttäjiltä ja tuomioistuimilta 2000–2013 ja annetut lausunnot 1993–2013 (HRekL 47 § / HetiL 41 §) sekä henkilörekisteririkoksesta ensimmäisessä oikeusasteessa tuomitut 2003–2012.[146]

Viime vuosien kehitys ei vielä näy selvästi rikostilastoissa. Lausuntopyyntöjen määrän kasvu ei ole tuonut mukanaan selvää tasonnousua tilastoitujen tuomioiden määrässä. Henkilörekisteririkoksesta – joka ei siis suinkaan ole ainoa näissä lausuntoasioissa kyseeseen tuleva rikosnimike – on ensimmäisessä oikeusasteessa annettu vuosina 2003–2012 kahdesta 13:een tuomiota vuosittain eikä selvää kehityslinjaa ole havaittavissa. Alin lukema on tosin tarkasteluvälin ensimmäiseltä vuodelta 2003 ja huippulukema toiseksi viimeiseltä vuodelta 2011.[147]

Korkein oikeus on antanut muutaman ennakkoratkaisun henkilötietojen suojaa koskevissa rikosasioissa. Tapauksissa KKO 1998:85 ja KKO 1999:127 oli kyse henkilörekisteririkoksista. Ensimmäisessä tietosuojavaltuutettua kuultiin suullisesti sekä käräjä– että hovioikeudessa ja tietosuojavaltuutetun sijainen antoi korkeimmalle oikeudelle lausunnon. Myös jälkimmäisessä tapauksessa korkein oikeus pyysi ja sai lausunnon. Lisäksi tietomurtoa koskeneessa tapauksessa KKO 2003:36 tietosuojavaltuutetulle oli varattu tilaisuus tulla kuulluksi käräjäoikeudessa.[148]

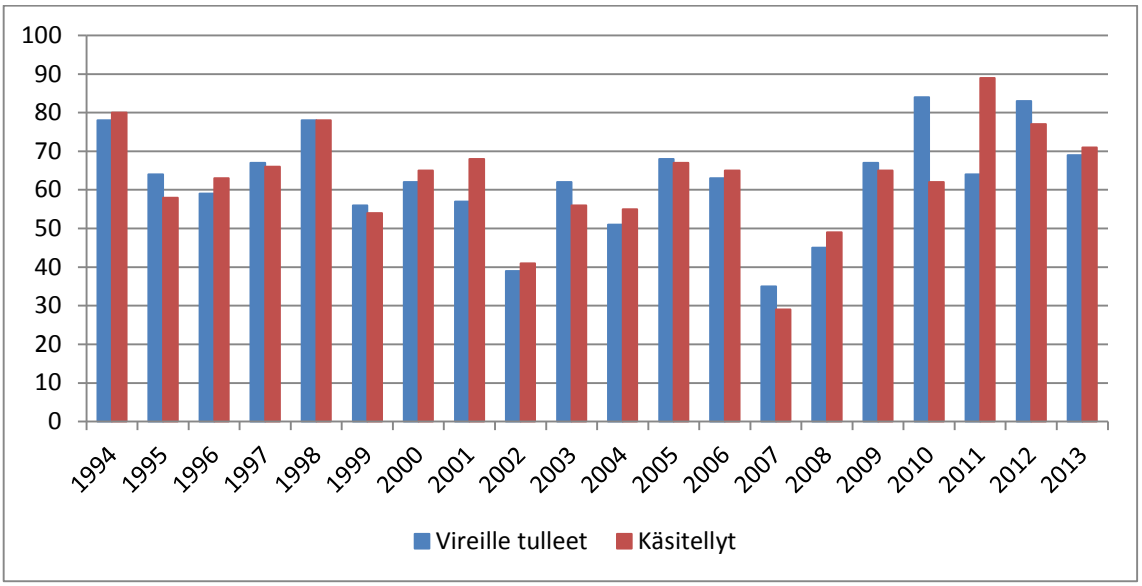
2.3.6 Lausunnot tutkimuslupa–asioissa

Tietosuojavaltuutettu antaa lausuntoja myös tutkimuslupa–asioissa. Terveydenhuollon valtakunnallisista henkilörekistereistä annetun lain 4.1 §:n mukaan kyseisessä laissa

[146] Tiedot annetuista lausunnoista 2001 puuttuvat.
[147] Suomen virallinen tilasto (SVT): Syytetyt, tuomitut ja rangaistukset [verkkojulkaisu]. Saatavilla http://www.stat.fi/til/syyttr/index.html, viitattu 24.1.2014.
[148] Tietosuojavaltuutetun rikosasioissa antamista lausunnoista ks. myös VK 2004, liite 6 s. 11–12, VK 2005 s. 40–44, VK 2006 s. 50–52 ja KT 2007 s. 30–34.

tarkoitettuihin henkilörekistereihin talletetut henkilötiedot on pidettävä salassa. Pykälän mukaan sosiaali– ja terveyshallitus – nykyään Terveyden ja hyvinvoinnin laitos eli THL – ja lääkelaitos voivat kuitenkin osaltaan antaa luvan henkilötietojen luovuttamiseen tietyin edellytyksin. Ennen lupapäätöksen antamista on varattava tietosuojavaltuutetulle tilaisuus tulla kuulluksi.

Pykälän mukaisia lausuntoja koskevien asioiden määrässä ei ole tapahtunut 2000–luvulla selkeää kehitystä, mutta vuosittaiset vaihtelut ovat olleet prosentuaalisesti varsin suuria. Keskimäärin tutkimuslupa–asioita on tullut vuodessa vireille noin 60, vähimmillään 35 (2007) ja enimmillään 84 (2010). Vuonna 2012 vireille tuli 69 ja käsiteltiin 71 tutkimuslupa–asiaa.[149]

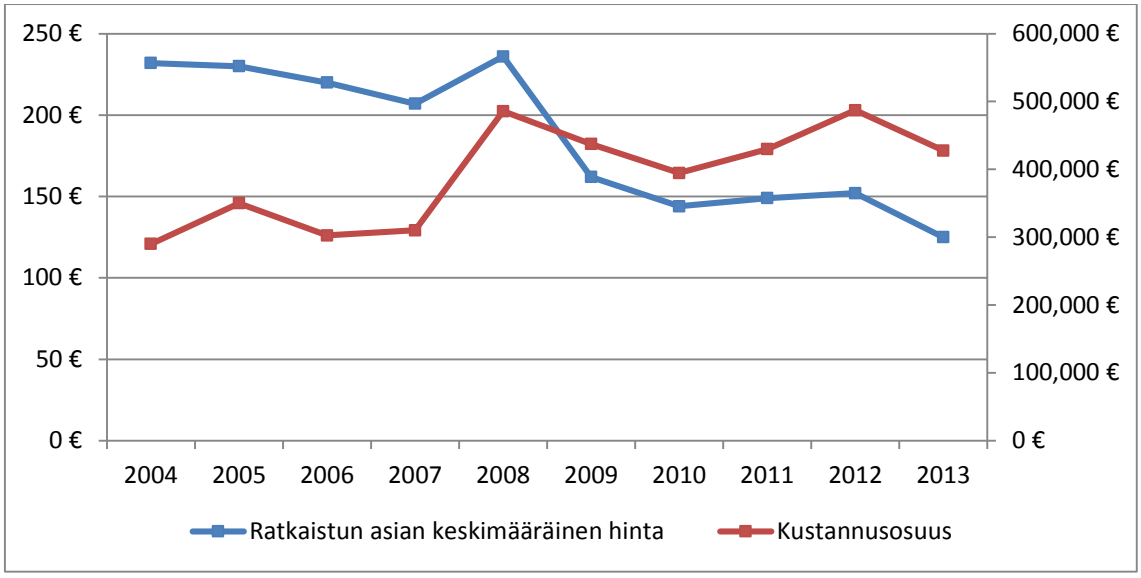


Kuvaaja 17: Terveydenhuollon valtakunnallisista henkilörekistereistä annetun lain 4 §:ssä tarkoitetut lausunnot tutkimuslupa–asioissa 1994–2013.

2.4 Ratkaisutoiminnan resurssit ja käsittelyajat

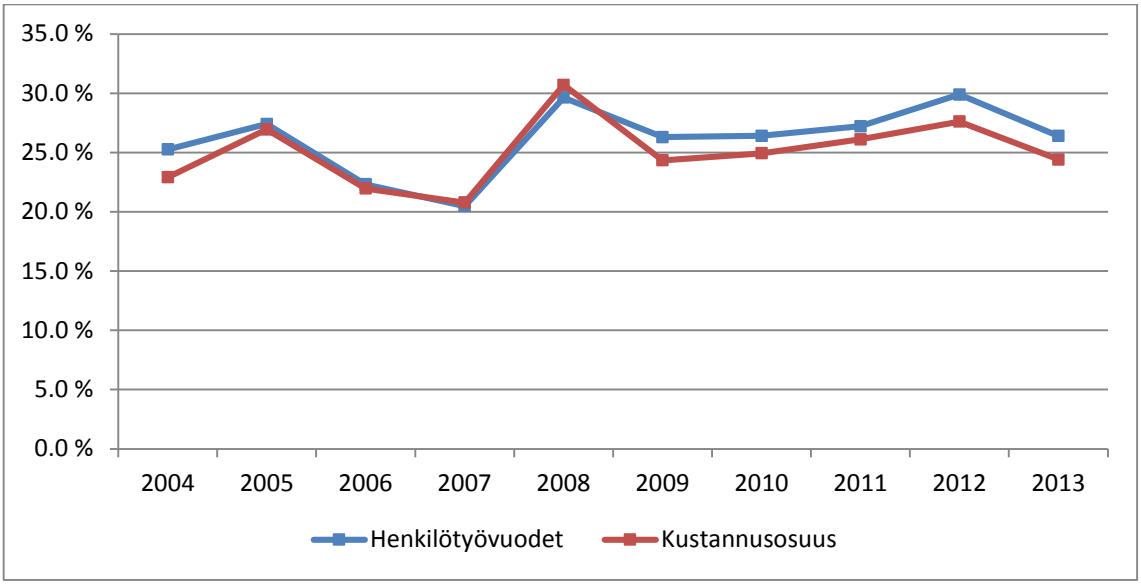
Ratkaisutoiminta vie melko suuren osan tietosuojavaltuutetun toimiston käytettävissä olevista resursseista. Henkilötyövuosissa mitattuna kirjallisesti vireille tulleiden yksittäisasioiden osuus on vuosina 2004–2013 vaihdellut välillä 4,64–7,09 htv. Kustannusosuudessa on tapahtunut euromääräistä nousua. Vuonna 2012 rahaa kului jo lähes puoli miljoonaa euroa, mikä vastaa reilua neljännestä toimiston vuosimenoista. Vuonna 2013 kustannusosuus laski hieman. Ratkaistun asian keskimääräinen hinta on laskenut vuoden 2004 yli 230 eurosta 125 euroon. Kehitys on siten ollut varsin suotuisaa, ja tulosneuvotteluissa asetetut ratkaisujen yksikköhintaa koskevat tavoitteet ovat täyttyneet. Tarkemmin ratkaisutoiminnan resurssien käytön kehitys käy ilmi seuraavista kahdesta kuvaajasta. Tarkastelu keskittyy vuosiin 2004–2013, koska näistä on saatavilla yhtenäistä tilastotietoa.

[149] Ks. KT 2011 s. 23–26 (TSV Dnro 2062/402/2011).



Kuvaaja 18: Ratkaisutoiminnassa ratkaistujen asioiden keskimääräinen hinta ja kustannusosuus 2004–2013.

Kuten ensimmäisestä kuvaajasta näkyy, yksittäisen asian keskimääräisen hinnan trendi on ollut laskeva ja kustannusosuuden samaan aikaan nouseva. Tämä tarkoittaa, että sen lisäksi että ratkaisutoimintaan on panostettu jonkin verran enemmän rahaa, myös tehokkuus on kasvanut. Samalla rahalla on siis ratkaistu entistä enemmän asioita. Tämä onkin ollut välttämätöntä asiamäärien kasvun vuoksi.



Kuvaaja 19: Ratkaisutoimintaan käytetyt osuudet kaikista henkilötyövuosista ja kustannuksista 2004–2013.

Toisen kuvaajan ratkaisutoiminnan osuutta henkilötyövuosista ja kaikista menoista kuvaavat viivat ovat lähes identtisiä. Tämä kertoo siitä, että ratkaisutoiminnan menot ovat erittäin pitkälti henkilöstön palkkamenoja. Kustannusosuus onkin lähinnä laskennallinen: kyse on siitä, miten

suuren osan toimiston työntekijät ovat työajastaan käyttäneet ratkaisutoimintaan. Tämä osuus on siis pysynyt melko vakiona, joskin lievä nouseva trendi on havaittavissa.

Asian keskimääräisen hinnan ohella tulosohjauksessa sovituissa tulostavoitteissa on etenkin 2000–luvun ensimmäisen vuosikymmenen lopulta lähtien kiinnitetty huomiota käsittelyaikojen alentamiseen. Vaikka asetettuja tavoitteita ei ole saavutettu joka vuosi, voidaan pidemmällä aikavälillä havaita kehityksen olleen suotuisaa.[150] Esimerkiksi vuonna 2004 kaikkien asioiden keskimääräinen käsittelyaika oli 4,3 kuukautta, mutta vuonna 2013 vain 42 vuorokautta.[151] Jonkinlainen osuus käsittelyaikojen laskuun on harjoittelijoiden ja muiden väliaikaisten työntekijöiden työpanoksella, joka on hieman nostanut käytettävissä olleiden henkilötyövuosien määrää, vaikkei vakinaisen henkilökunnan määrä olekaan noussut.[152] Toimintakertomuksen tilastoista on havaittavissa, että ratkaisutoiminnan kustannusosuuksien ja siihen käytettyjen henkilötyövuosien määrän ollessa korkeimmillaan käsittelyajat ovat olleet matalimmillaan. Lasku johtuu kuitenkin myös toiminnan tehostamisesta, yksinkertaisemmasta käsittelyprosessista ja asianhallinnan kehittämisestä. Koska suuri osa asioista on samantyyppisiä kuin aikaisemmin käsitellyt asiat, näiden asioiden käsittelemisessä on myös voitu hyödyntää aiemmin tehtyjä ratkaisuja entistä enemmän.

Vaikka yleislinja käsittelyajoissa näyttää selvältä, on käsittelyaikojen tilastoinnissa myös epäselvyyksiä, joten edellä mainittuihin tekijöihin ja eri seikkojen vaikutukseen on suhtauduttava varauksella. Eri vuosien toimintakertomuksiin ja tulossopimusasiakirjoihin sisältyvät, samoja vuosia kuvaavat lukemat käsittelyajoista ovat huomattavan ristiriitaisia, joten selvyyttä yksittäisten vuosien vertailukelpoisista lukemista ei ole. [153]

3. Viestintä, yleisohjaus ja tiedotus

3.1 Yleistä viestinnästä sekä yleisohjaus– ja tiedotustoiminnasta

Tietosuojavaltuutetulla on yleinen ohjaus– ja neuvontavelvollisuus, jonka perustana on henkilötietolain 38.1 §. Lisäksi tietosuojavaltuutetun tehtäviin kuuluu huolehtia toimialaansa kuuluvasta tiedotustoiminnasta (TSV–TSVL 5 §:n 3 kohta). Vastaavat säännökset löytyivät aiemmin TSL–TSVL–1987:n 7 §:stä sekä TSL–TSVA–1987:n 2 §:n 3 ja 5 kohdista. Lisäksi

[150] Eri vuosien toimintakertomuksiin ja tulossopimusasiakirjoihin sisältyvät, samoja vuosia kuvaavat lukemat käsittelyajoista ovat huomattavan ristiriitaisia, joten varmuutta yksittäisten vuosien vertailukelpoisista lukemista ei ole. Suunta on kuitenkin viime vuosina ollut selkeä.
[151] Kansalaisilta tulleiden asioiden käsittelyajat olivat tätä selvästi pidempiä ainakin silloin kun niitä vielä tilastoitiin erikseen (vuonna 2007 9,7 kk).
[152] Ks. edellä II.1.
[153] Esimerkiksi vuoden 2013 toimintakertomuksen tietojen mukaan keskimääräinen käsittelyaika vuonna 2012 oli 60,4 vrk ja vuonna 2011 62,6 vrk. Sen sijaan vuoden 2012 toimintakertomuksen mukaan keskimääräinen käsittelyaika vuonna 2012 oli 36 vrk, vuonna 2011 58,7 vrk ja vuonna 2010 100,3 vrk. Vuoden 2011 toimintakertomuksen mukaan taas keskimääräinen käsittelyaika vuonna 2011 oli 1,26 kk ja vuonna 2010 3 kk. Vuoden 2013 tulossopimuksessa lukemat ovat 32,3 vrk vuonna 2012 (per 6.11.2012), 55,3 vrk vuonna 2011 ja 99,8 vrk vuonna 2011.

tietosuojavaltuutettu saattoi antaa henkilörekisterilain 33 §:n nojalla yleisiä ohjeita lain 19 ja 20 §:iin liittyen sekä rekistereiden suojaamisesta.

Vaikka myös tietosuojavaltuutetun kannanotot yksittäisissä tapauksissa ovat luonteeltaan ohjausta ja neuvontaa, eivät ne kuulu tarkastelun piiriin tässä luvussa. Tapaus– ja rekisterikohtaista ohjausta ja neuvontaa on käsitelty edellisten lukujen puitteissa. Tämän luvun mielenkiinnon kohteena ovat tietosuojavaltuutetun toimiston yleinen informaatiota ja tietoa tuottava toiminta sekä tuotetun informaatiomateriaalin kommunikointi yleisölle. Kyseessä on osa tietosuojavaltuutetun toimiston ennaltaehkäisevää toimintaa.

3.2 Tietosuoja–lehti

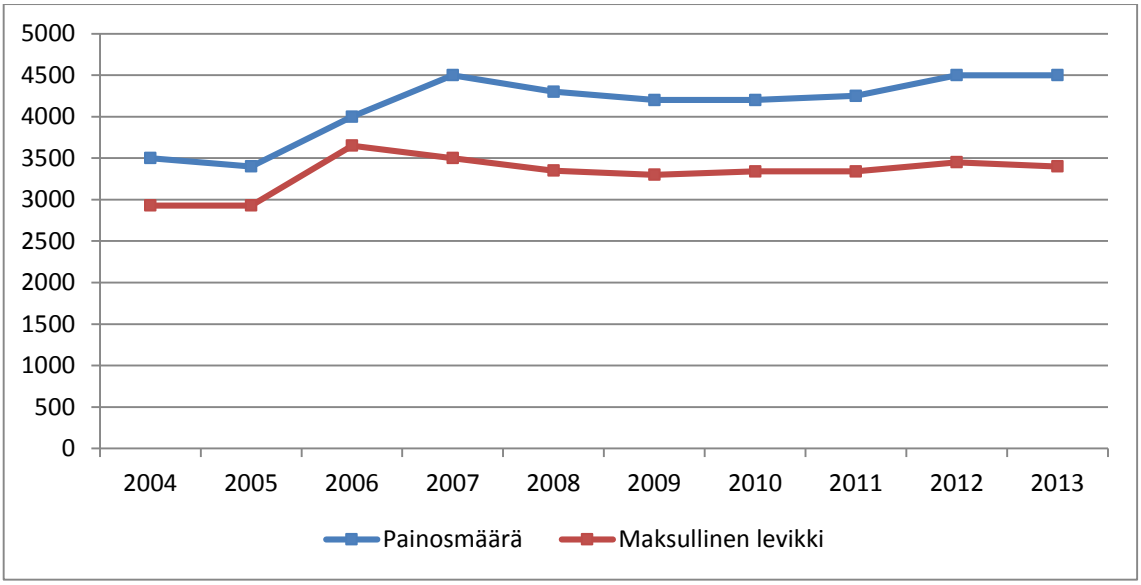
3.2.1 Perustietoa

Tietosuoja–lehden ensimmäinen numero ilmestyi vuonna 1989, tietosuojaviranomaisten toisena täytenä toimintavuotena. Tästä lähtien lehti on ilmestynyt neljä kertaa vuodessa. Alun perin lehteä julkaisi tietosuojavaltuutetun toimisto yksin, pian mukaan tuli myös tietosuojalautakunta. Nykyään julkaisijoina toimivat yhdessä Viestintävirasto, tietosuojavaltuutetun toimisto, tietosuojalautakunta sekä vuoden 2011 lopusta alkaen myös Patentti– ja rekisterihallitus. Lehteä kustantaa Stellatum Oy.

Tietosuoja–lehti oli pitkälle 1990–luvun loppupuolelle saakka tietosuojavaltuutetun toimiston ainoa vakituinen viestintä– ja tiedotuskanava. Lehti oli kuitenkin suunnattu, kuten nykyäänkin, lähinnä rekisterinpitäjille. Rekisteröidyille suunnattu tiedotus oli riittämätöntä ja pääosin epäsäännöllisesti julkaistavien oppaiden ja tiedotteiden varassa.[154]

90–luvulla lehden levikki pysyi pitkään tasaisesti noin 2000 kappaleessa. Vuosituhannen taitteessa lehden maksullinen levikki oli noin 2400. Sittemmin maksullinen levikki on vakiintunut vajaan 3500:n tasolle, ja painosmäärä oli vuonna 2013 4500. Viime vuosina vallinneeseen lehtialan yleiseen negatiiviseen kehitykseen suhteutettuna Tietosuoja–lehti on siis menestynyt verrattain hyvin. Seuraava kuvaaja esittää painosmäärän ja maksullisen levikin kehityksen vuodesta 2004 lähtien.

[154] Ks. TK 1993 s. 8.



Kuvaaja 20: Tietosuoja–lehden painosmäärä ja maksullinen levikki 2004–2013.

Nykyään Tietosuoja–lehti on oman määritelmänsä mukaan tietoturvan ja tietosuojan erikoislehti. Se on suunnattu asiantuntijoille, ”jotka suunnittelevat tai hyödyntävät tietojärjestelmiä, käsittelevät henkilötietoja ja osallistuvat niitä koskevaan päätöksentekoon”.[155] Tilaajakanta jakautuu vuonna 2011 tehdyn haastatteluselvityksen mukaan siten, että suurimmat ryhmät muodostavat yritykset (35 %), sosiaali– ja terveydenhuoltoalan toimijat (20 %) sekä kunnallishallinto ja järjestöt (molemmat 15 %). Yksityishenkilöitä tilaajien joukossa on vain vähän (2 %). Tärkeimmäksi perusteeksi tilata lehteä osoittautuivat suoraan työtehtäviin liittyvät syyt (70 %). Muita keskeisiä syitä olivat ammatillinen kiinnostuneisuus (52 %) ja yleinen mielenkiinto aihetta kohtaan (51 %).[156]

Vuosina 2007–2008 Tietosuoja–lehteä julkaistiin Internetissä näköislehtenä, ja vuoden 2009 alusta lähtien näköislehti korvattiin verkkojulkaisulla. Osoitteesta *http://www.tietosuoja–lehti.fi*[157] löytyvää verkkojulkaisua on viime vuosina pyritty kehittämään, ja tavoitteena on saada yhä useampi organisaatio kokonaisuudessaan sen käyttäjäksi.[158] Nykyisellään se on paperilehden rinnalla julkaistava, sitä täydentävä palvelu, joka sisältyy paperilehden tilauksen hintaan. Osa verkossa julkaistavista artikkeleista on kuitenkin kaikkien luettavissa, ja toisaalta muutamia artikkeleita julkaistaan vain verkossa. Vuonna 2012 kaikkien luettavissa olevia verkkoartikkeleita julkaistiin yhteensä 12 ja vuonna 2013 22 kappaletta.

[155] Esim. TK 2012 s. 10.
[156] TK 2011 s. 11–12.
[157] Myös domain–osoite *tietosuojalehti.fi* ohjaa verkkojulkaisuun.
[158] TK 2011 s. 10.

3.2.2 Lehdessä käsiteltyjä aiheita

Tarkasteltaessa lehden sisältöä eri vuosina voidaan havaita sisällön kehittyneen 2000–luvun jälkipuoliskolla teknisempään ja teknologisempaan suuntaan. Tähän liittyy tietoturvaa ja erilaisia verkkouhkia, –ilmiöitä ja –teknologioita käsittelevien aiheiden korostuminen viime vuosina. Vielä 2000–luvun alussa aiheet olivat pääsääntöisesti oikeudellisia ja tietosuojaan painottuvia. Oikeudellisetkaan aiheet eivät toki ole kokonaan hävinneet lehdestä. Kansainvälisiä asioita on lehdessä käsitelty alusta alkaen, eikä niiden määrä näytä merkittävästi kasvaneen. Myös näissä on nähtävissä EU–asioiden merkityksen korostuminen, erityisesti kun kyse on oikeudellisesta sääntelystä. Teknisemmät aiheet ovat usein luonteeltaan globaalimpia. Aiheiden kehitys käy ilmi myös seuraavasta esimerkinomaisesta taulukosta, jossa on vertailtu lehden kansiotsikoita vuosilta 1989, 2000 ja 2012.

1989	2000	2012
Uhkaako tietosuoja painovapautta?	Sähköinen asiointi hallinnossa	Minne menet, tunnistautuminen?
Rekisterien suojausohjeet	Tietosuoja ja Pankkialan Asiakasneuvontatoimisto	Tietosuoja-asetus (3 kertaa)
Väestötietojen luovutus	Tietosuoja verkossa EU:n säännösten mukaan	Kyberpuolustus
Uudistuspaineita Pohjoismaissa	Väestörekisterikeskuksen sähköiset asiointipalvelut lisäävät tietosuojaa	Etätyö
Euroopan Neuvosto ja tietosuoja	Työntekijän yksityisyydensuoja suhteessa työnantajan velvollisuuksiin	Sosiaalinen media
English Summary	Suomalaisten mielipiteet tietojensa rekisteröinnistä ja yksityisyydestä	Tietovuodot
Tietorikokset ja lainsäädäntö	Potilasrekisterinpitoon liittyvät muutokset	Tietojärjestelmät ja tietojen käsittely – Laadulla vai tuurilla?
Luottotietojen rekisteröinti	Työnantajalla ei oikeutta velvoittaa huumetestiin	Paikantaminen
Tietosuoja ja käyttäjien moraali	Henkilötunnus tietosuojaongelmana	Muistitikut
Henkilötunnuksen käyttö	Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista	Sähköposti
	Mobiilit palvelut ja tietosuoja	Kyberturvallisuus
	Huumetestit kouluissa	Tietosuojaloukkaukset
		IPv6
		Tekijänoikeudet: Surffaaja syynissä
		Kunnat
		Urkinta
		Tietomurrot
		Asuminen
		Poliisi
		Hallitse riskit – Näin suojaat tietosi ja varaudut ongelmiin fiksusti
		Sähköposti
		Suoramarkkinointi
		BYOD
		Biopankit

Taulukko 1: Tietosuoja–lehden kansiotsikot 1989, 2000 ja 2012.

Mainitut kehityslinjat johtuvat luonnollisesti osittain teknologian ja verkkoyhteiskunnan kehityksestä. Esimerkiksi sähköpostin tietosuoja ei vielä 1990–luvun taitteessa ollut kovinkaan keskeinen kysymys, koska sähköposti tai muukaan sähköinen asiointi eivät olleet vielä yleistyneet sen enempää julkishallinnossa kuin yrityskäytössäkään. Nykyisen kaltaisia muistitikkuja tai sosiaalista mediaa ei ollut edes olemassa. Lehden aiheiden kehityslinjat selittyvät kuitenkin osittain myös uusien tahojen liittymisellä lehden julkaisijoihin tietosuojavaltuutetun toimiston ohella.

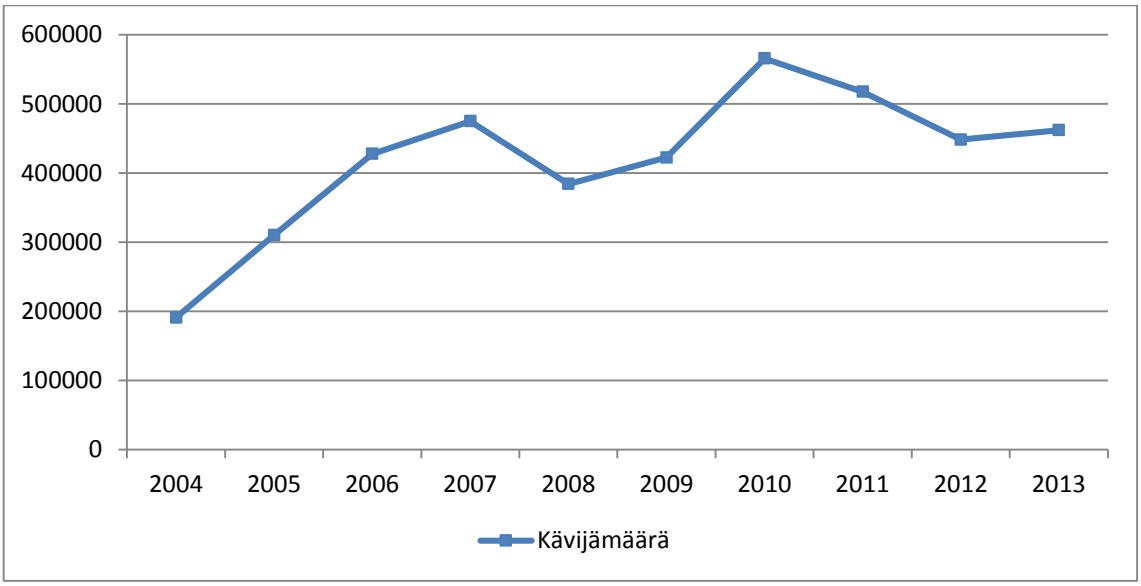
Aiheitakin enemmän näyttää muuttuneen lehden ja kirjoitusten tyyli. Lehti on kehittynyt tietosuojaviranomaisten tekstipainotteisesta tiedotuskanavasta yleiseksi, kaupallisen aikakauslehden kaltaiseksi tietosuoja– ja tietoturva–alan lehdeksi. Tästä voi nähdä viitteitä myös lehden ulkoasun kehityksessä. Vaikutelmaa vahvistaa myös se, että vuonna 2013 lehden kanteen nostettiin näkyvästi henkilöhaastattelujuttuja.

3.3 Tietosuoja.fi

3.3.1 Perustietoa

Toinen tietosuojavaltuutetun toimiston keskeisistä viestintä– ja tiedotuskanavista on keväällä 1997 avattu[159], vuosina 2000, 2004[160] ja viimeksi toukokuussa 2014 uudistettu verkkosivusto, joka sijaitsee internet–osoitteessa *http://www.tietosuoja.fi*. Sivustolla julkaistaan mm. perustietoa tietosuojalainsäädännöstä ja rekisteröidyn oikeuksista, vastauksia usein kysyttyihin kysymyksiin, tietosuojavaltuutetun kannanottoja ja päätöksiä, oppaita, lomakkeita ja malleja sekä tietoa toimiston tehtävistä ja toiminnasta. Suomenkielisen materiaalin lisäksi tarjolla on ruotsin– ja englanninkieliset sivustoversiot, joista varsinkin jälkimmäisen sisältö on varsin niukkaa ja ikääntynyttä.

Tietosuojavaltuutetun toimiston toimintakertomuksissa on julkaistu tietoa sivuston kävijämääristä. Seuraava kuvaaja esittää kävijämäärien kehitystä vuodesta 2004 lähtien.



Kuvaaja 21: Tietosuoja.fi –sivuston kävijämäärät 2004–2013.

Vierailijoiden määrä on yli kaksinkertaistunut tarkasteluvälillä. Toisaalta viimeiset kaksi vuotta kävijämäärässä on ollut pientä laskua. Kaiken kaikkiaan kävijämäärätilastot antavat vain melko karkean kuvan sivuston käytön määrästä ja laadusta. Niistä ei suoraan käy ilmi, kuinka

[159] TK 1997 s. 10.
[160] TK 2000 s. 14, TK 2004 s. 10.

moni yksittäinen ihminen on sivustolla vuoden aikana vieraillut, sillä sama henkilö voi olla laskettuna hyvinkin moneen kertaan. Kävijämäärät eivät myöskään ilmaise, miten pitkään käyttäjät sivustolla viihtyvät, mitä he sieltä etsivät, ja mikä tärkeintä, löytävätkö he etsimänsä.

Lähes puolen miljoonan vuosittaisen kävijän määrää voidaan kuitenkin pitää varsin kohtuullisena osoituksena siitä, että sivusto on laajasti ihmisten tiedossa ja saavutettavissa. Sivusto saavuttaa, mikä nykyisessä verkkoyhteiskunnassa ei ole yllättävää, huomattavasti suuremman ihmisjoukon kuin esimerkiksi toimiston toinen perinteinen kanava, pääosin ammattikäyttöön tarkoitettu Tietosuoja–lehti. Verkkosivusto muodostaa myös välittömämmän ja joustavamman tavan välittää informaatiota kuin neljä kertaa vuodessa ilmestyvä paperijulkaisu. Siten se on tärkeä viestintä– ja tiedotuskanava erityisesti rekisteröityjen eli yksityisten kansalaisten suuntaan.

Verkkosivut tarjoavat myös mahdollisuuden vuorovaikutteiseen viestintään, mikä jo ensimmäisen sivustoversion suunnitteluvaiheessa nimenomaisesti noteerattiin.[161] Tämänhetkinenkin sivusto on kuitenkin nykystandardein varsin yksisuuntainen viestintäkanava, eikä se tarjoa *web 2.0* –mallille ominaisia yhteisöllisyyteen ja käyttäjien aktiivisuuteen tai sivuston käyttäjien ja ylläpitäjän dialogiin perustuvia kommunikaatiomahdollisuuksia taikka verkkopohjaista yhteydenottomahdollisuutta muuten kuin sivulla ilmoitetun sähköpostiosoitteen muodossa.[162] Hivenen lisää vuorovaikutteisuutta ovat tuoneet vuoden 2014 uudistuksessa sivustolle lisätyt tietosuojavaltuutetun ylläpitämä blogi ja gallup–toiminto.[163]

Sivuston päivittäminen on toimintakertomustietojen mukaan ajoittain kärsinyt resurssien vähäisyydestä.[164] Joka tapauksessa sivustolle on lisätty uusia tiedotteita tai muuta materiaalia useita kertoja kuukaudessa, joten ero esimerkiksi tietosuojalautakunnan lähes täysin laiminlyötyyn verkkosivustoon on merkittävä.[165]

3.3.2 Ratkaisujen julkaiseminen

Tietosuoja.fi –sivustolla on julkaistu tietosuojavaltuutetun neuvontaa ja ohjausta koskevia kannanottoja sekä joitakin sitovia päätöksiä. Sivustolla ratkaisut on ryhmitelty varsin erilaisia aiheita käsittävien asiasanojen alle. Eniten ratkaisuja löytyy sosiaalihuoltoon, terveydenhuoltoon, opetukseen ja työelämään liittyen. Internet–hakusanan alta ratkaisuja ei

[161] TK 1996 s. 8, ks. myös TK 1997 s. 10.
[162] Vuoden 2014 Tietosuojapäivän yhteydessä 28.1.2014 toteutettu tietosuojavaltuutetun toimiston kaikille avoin kysymys & vastaus –chat toteutettiin OM:n ylläpitämän Otakantaa.fi –sivuston kautta.
[163] Blogissa ei kuitenkaan ainakaan tätä kirjoitettaessa ole käytössä kommentointimahdollisuutta ja sen päivitystahdiksi ennakoidaan noin kerran kuukaudessa. Kovin suurta vuorovaikutteisuuden lisää se ei siten näytä tuovan.
[164] Esim. TK 2008 s. 12. Johdon sihteeri Erna Laihon haastattelussa (6.5.2014, Helsinki) antaman tiedon mukaan sivuston päivittämisestä on käytännössä vastannut kaksi henkilöä muiden tehtäviensä ohella.
[165] Ks. III.3.

löydy aivan yhtä paljoa, mutta käytännössä henkilötietojen käsittely verkkoympäristössä näkyy lukuisissa ratkaisuissa, jotka on sijoitettu esimerkiksi vain ensin mainittujen hakusanojen alle. Yhteensä ratkaisuja oli toukokuussa 2014 suomenkielisellä sivustoversiolla noin 160, ruotsinkielisellä noin 130.[166] Kun otetaan huomioon tietosuojavaltuutetun vuosittain ratkaisemien asioiden määrät, kyse ei selvästikään ole kovin kattavasta tietopankista. Ratkaisut ovat ilmeisesti valikoitu pitäen silmällä niiden yleistä informaatioarvoa. Pääosin verkkosivuilla julkaistut ratkaisut ovat niitä, joita myös tietosuojavaltuutetun vuosittaisissa katsauksissa toimintaan on julkaistu.

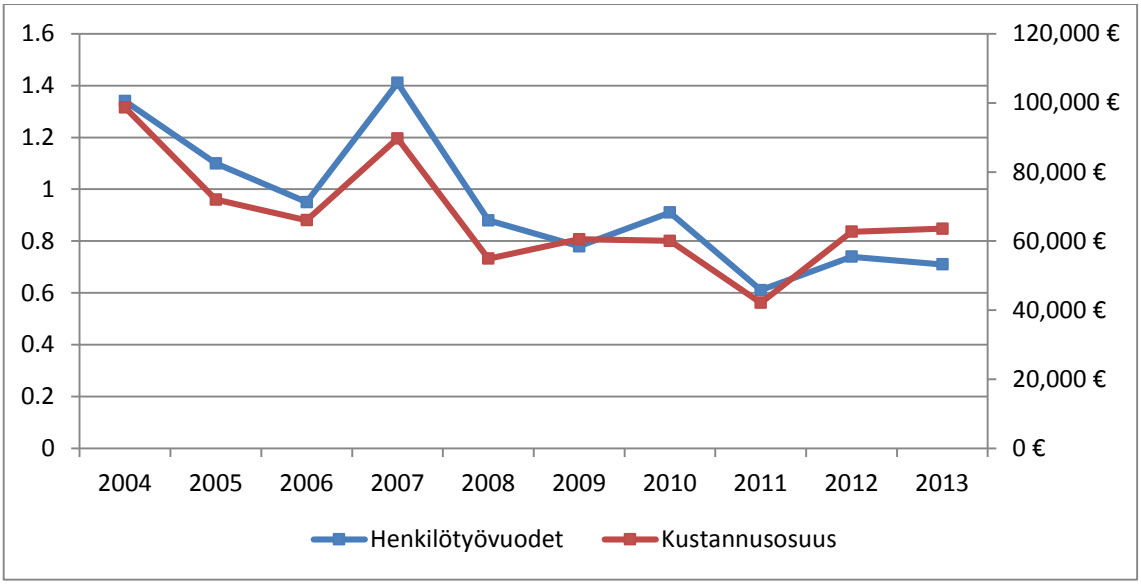
Verkkosivujen Ratkaisut–osiota täydentää Usein kysyttyä –osio[167], johon on koostettu vastauksia tietosuojavaltuutetun toimistolta useimmin tiedustelluista asioista. Osa vastauksista sisältää viittauksen johonkin sivustolla julkaistuun ratkaisuun, oppaaseen tai lomakkeeseen.

3.4 Muuta tiedotustoiminnasta

Tietosuoja–lehden ja Tietosuoja.fi –sivuston kautta tapahtuvan viestinnän lisäksi tiedotustoiminnaksi lasketaan mm. lehdistötiedotteet ja eri medioille annetut haastattelut, joita tietosuojavaltuutettu on toimintakertomusten vakiofraasin mukaan antanut ”lähes päivittäin”. Lehdistötiedotteita on annettu viimeisen viiden vuoden aikana kahdesta kuuteen vuosittain. Tietosuoja–lehden lisäksi toimiston työntekijät ovat kirjoittaneet tekstejä ainakin jossain määrin myös muihin lehtiin.[168]

Tiedotuksen osuus tietosuojavaltuutetun toimiston resurssien käytöstä on viimeisen kymmenen vuoden aikana ollut pienehkö. Käytettyjen henkilötyövuosien osuus on vuosina 2004–2013 vaihdellut 0,61 ja 1,41 htv:n (2010 ja 2007) välillä. Kustannusosuuden vaihteluväli samana aikana on ollut 42 162 – 98 620 euroa (2010 ja 2004). Tarkemmin resurssien käyttö ilmenee seuraavasta kuvaajasta. Tiedotustoimintaan käytettyjen resurssien trendi on laskeva.

[166] http://tietosuoja.fi/fi/index/ratkaisut.html, viitattu 9.5.2014, ja ruotsiksi http://tietosuoja.fi/sv/index/ratkaisut.html, viitattu 9.5.2014.
[167] http://www.tietosuoja.fi/fi/index/useinkysyttya.html, viitattu 9.5.2014. Vastaava osio on tarjolla myös ruotsiksi, http://www.tietosuoja.fi/sv/index/useinkysyttya.html, viitattu 9.5.2014.
[168] TK 2006 s. 14.



Kuvaaja 22: Tiedotustoimintaan käytetyt henkilötyövuodet ja kustannusosuus 2004–2013.

Tiedotuksesta puhuttaessa on syytä muistaa henkilötietolain 24 §, jossa säädetään rekisterinpitäjän informointivelvollisuudesta. Tietyiltä osin vastuu tietojen antamisesta rekisteröidyille on siis annettu laissa rekisterinpitäjille. Tietosuojavaltuutetun toimintaan taas kuuluu – oman tiedottamistoimintansa ohessa – edistää ja valvoa sitä, että rekisterinpitäjät noudattavat tätä velvollisuuttaan. Täten rekisteröityjen tiedonsaantia voidaan välillisesti parantaa rekisterinpitäjille suunnatulla tiedotuksella ja yleisohjauksella, mutta myös esimerkiksi näihin kohdistuvien tarkastusten, neuvonnan ja puhelinneuvonnan kautta.

3.5 Yleisohjaus: oppaat ja mallit

Tietosuojavaltuutetun toimisto on julkaissut merkittävän määrän erilaisia oppaita ja esitteitä, joilla se on pyrkinyt informoimaan ja opastamaan niin rekisteröityjä kuin rekisterinpitäjiäkin ja lisäämään heidän tietoisuuttaan. Näissä julkaisuissa kyse on yleisohjauksesta. Julkaisut oli aiemmin luokiteltu eri sarjoihin. *Asiaa tietosuojasta* –sarjassa julkaistiin ohjemateriaalia erityisesti rekisterinpitäjille. *Tiedotteet rekisteröidyille* –sarjan tavoitteena oli nimensä mukaisesti tiedottaa rekisteröidyille tietosuojalainsäädännön heille antamista oikeuksista. *Hyvä tietää* –sarjassa julkaistiin sekä rekisterinpitäjille että rekisteröidyille suunnattuja henkilötietolain soveltamista koskevia ohjeita ja neuvoja. Lisäksi toimisto julkaisi *Tietosuojavaltuutetun mallit* –sarjaa ja mallilomakkeita.

Tällä hetkellä esitemateriaalia julkaistaan ensisijaisesti Tietosuoja.fi –sivuston Oppaat–osiossa[169], josta löytyi toukokuussa 2014 yli 60 julkaisua. Julkaisut on järjestetty aakkosittain ja aiemmista julkaisusarjoista on suurin osin luovuttu, joskin Asiaa tietosuojasta –sarjaan on edelleen luokiteltu kaksi julkaisua. Käytännössä kaikki oppaat on myös käännetty ruotsiksi ja

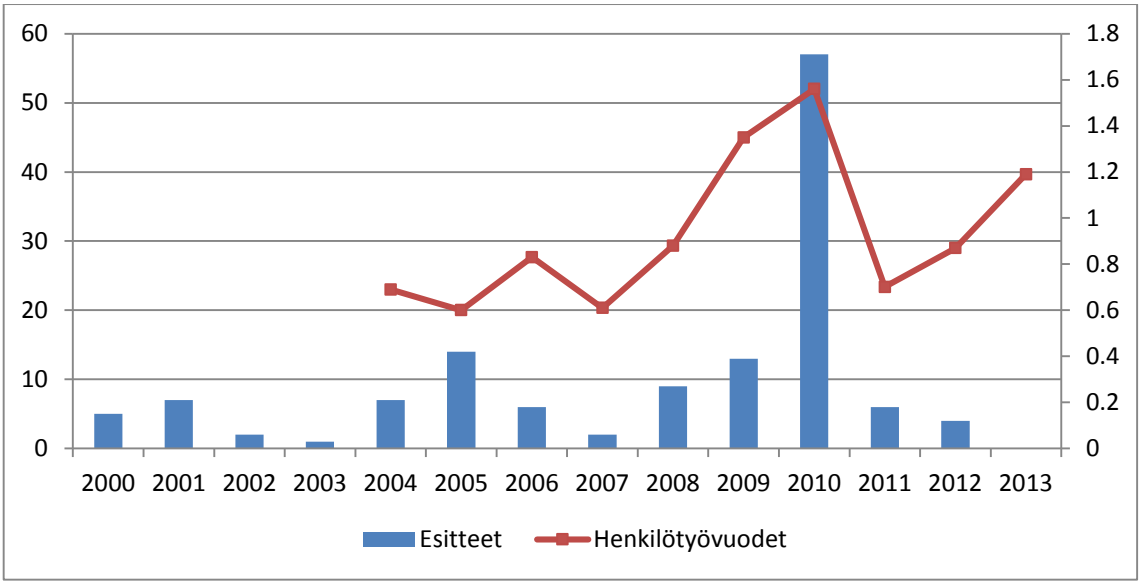
[169] http://www.tietosuoja.fi/fi/index/materiaalia/oppaat.html, viitattu 9.5.2014.

ne ovat saatavilla sivuston ruotsinkielisen version Broschyrer–osiosta[170]. Oppaiden kohderyhmä, taso ja laajuus vaihtelevat. Muutaman sivun mittaiset, aiemmin Hyvä tietää –sarjassa julkaistut normaalille internetin käyttäjälle tarkoitetut ”mikä se on?” –oppaat kertovat sinä–muodossa puhuttelevasti perusasioita sen kaltaisista verkkomaailman käsitteistä kuin blogi, hakupalvelu, huijaussähköposti, identiteettivarkaus ja internetin keskustelupalsta. Osa oppaista on edelleen tarkoitettu viranomaisille ja rekisterinpitäjille, organisaatioiden johdolle ja tietoturvallisuudesta vastaaville. Nämä ovat laajempia ja sisältävät tarkempaa ja oikeudellisempaa tietoa toimijoiden velvoitteista. Oppaat–osioon sisältyy myös muistilistoja ja malleja lainsäädännön eri velvoitteiden noudattamisesta, esimerkiksi tietosuojaselosteen laatimisesta tai informointivelvoitteen toteuttamisesta.

Oppaiden lisäksi Tietosuoja.fi –sivustolta on saatavissa lomakkeita mm. tarkastuspyyntöä, korjaamisvaatimusta, rekisteri– ja tietosuojaselosteita ja henkilötietolain mukaisia ilmoituksia varten. Nämä löytyvät omasta Lomakkeet–osiostaan[171].

Suurin osa tällä hetkellä käytössä olevista oppaista on viimeksi päivitetty vuonna 2010, jolloin hyväksyttiin ennätysmäärä esitejulkaisuja, 57. Myös julkaisujen päivittäminen on ajoittain viivästynyt, mitä on selitetty henkilövoimavarojen riittämättömyydellä.[172] Yleisohjausaineiston tuottamiseen ja päivittämiseen onkin käytetty suhteellisen niukasti resursseja, välillä 2004–2012 keskimäärin noin 0,9 htv ja 60 000 euroa vuodessa. Enimmillään henkilötyövuosien osuus on ollut 1,56 htv (2010) ja kustannusosuus 83 787 euroa (2009). Huippuvuodet selittyvät vuonna 2007 aloitetulla aineiston uudistamishankkeella. Seuraava kuvaaja esittää vuosittain hyväksyttyjen esitteiden (yleisohjaukseen tarkoitettujen julkaisujen) määrän sekä yleisohjaukseen käytetyt henkilötyövuodet vuosina 2000–2012.

[170] http://www.tietosuoja.fi/sv/index/materiaalia/oppaat.html, viitattu 9.5.2014. Sen sijaan englanninkielisen materiaalin määrä on vähäinen eikä useimpia julkaisuja ole päivitetty vuosiin, toisenlaisista tavoitteista huolimatta. Ks. TK 2007 s. 11 ja http://www.tietosuoja.fi/27306.htm, viitattu 20.9.2013.
[171] http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet.html, viitattu 9.5.2014.
[172] Ks. esim. TK 2008 s. 11.



Kuvaaja 23: Yleisohjausta varten hyväksytyt esitteet 2000–2013 ja yleisohjaukseen ja aineiston tuottamiseen käytetyt henkilötyövuodet 2004–2013.

4. Sidosryhmäyhteistyö ja käytännesäännöt

4.1 Yleistä sidosryhmäyhteistyöstä

Tietosuojavaltuutetun toimisto on jatkuvasti osallistunut lukuisiin erilaisiin neuvottelukuntiin, toimikuntiin sekä työ– ja ohjausryhmiin niin valtakunnallisella tasolla kuin hallinnonala– ja toimialakohtaisesti. Viime vuosina näitä ryhmiä on ollut yhteensä noin 80. Näistä eri hallinnonalojen ja toimialojen ohjaus– ja työryhmiä on ollut noin 30. Ryhmien määrä on viime vuodet pysynyt vakaana. Toimisto on myös järjestänyt eri ryhmien kanssa yhteisiä koulutustilaisuuksia ja seminaareja.[173]

Valtakunnallisella tasolla tietosuojavaltuutettu on osallistunut mm. Arjen tietoyhteiskuntaohjelman tietoturvaryhmään sekä valtionhallinnon tietoturvallisuuden johtoryhmään (VAHTI), jonka alaisissa työryhmissä on myös ollut toimiston edustajia. Aiemmin tietosuojavaltuutettu on mm. ollut pysyvänä asiantuntijana vuosina 2003–2007 toimineessa tietoyhteiskuntaneuvostossa[174] ja jäsenenä vuosina 2001–2003 ja 2003–2007 toimineissa tietoturvallisuusasiain neuvottelukunnissa. Valtakunnalliseen sidosryhmätoimintaan kuuluu myös osallistuminen erilaisiin teemapäiviin kuten kansalliseen tietoturvapäivään ja –viikkoon sekä eurooppalaiseen tietoturvapäivään ja tietosuojapäivään.[175] Tietosuojavaltuutetun toimiston säännöllisiä yhteistyötahoja ovat olleet toimintakertomusten

[173] TK 2012 s. 8.
[174] Ks. http://valtioneuvosto.fi/tietoarkisto/aiemmat–hallitukset/vanhanen/tietoyhteiskuntaneuvosto/fi.jsp, viitattu 19.11.2013.
[175] TK 2002:een sisältyvä katsaus s. 2 (saatavilla http://www.tietosuoja.fi/uploads/pm5s162jk.rtf, viitattu 19.11.2013), TK 2005 s. 11 ja TK 2012 s. 8.

mukaan mm. sisäasianministeriö, Viestintävirasto, Kilpailu– ja kuluttajavirasto[176], Valvira, puhelin– ja verkkoauttamisen eettinen neuvottelukunta, lääninlääkärit, potilasasiamiehet, sosiaaliasiamiehet ja arkistolaitos.[177]

Merkittäviä toimialakohtaisesti organisoituneita, pysyviä työ– ja ohjausryhmiä ovat opetustoimen tietosuojan ohjausryhmä OTTO, terveydenhuollon asiantuntijaviranomaisten yhteistyöryhmä TELLU, sosiaalihuollon tietosuojan ohjausryhmä SOHVI, teletoiminnan tietosuojaryhmä TERTTU, markkinoinnin ja asiakkuuden tietosuojan ohjausryhmä MAISA, tieteellisen tutkimuksen sektorilla toimiva tutkimuslupayhteistyöryhmä sekä finanssialan tietosuojafoorumi.

Vuonna 2001 toimintansa aloittanut opetustoimen tietosuojan ohjausryhmä eli OTTO on tietosuojavaltuutetun aloitteesta perustettu, tietosuojavaltuutetun toimistossa säännöllisesti kokoontuva ryhmä. Sen toimintaan osallistuu viranomaisia, järjestöjä ja käytännön toimijoita erilaisista oppilaitoksista.[178] Tietosuoja.fi –sivustolla ryhmän toimintaa kuvataan seuraavasti:

> Ryhmä seuraa tietosuoja–asioiden kehitystä opetusalalla ja toimii jäsentensä keskustelufoorumina. Ryhmän tavoitteena on omalta osaltaan tukea oppilaitoksia moninaisten tietosuojakysymysten ratkaisemisessa. Ohjausryhmä osallistuu koulujen ja oppilaitosten käyttöön suunnattujen materiaalien valmisteluun alan asiantuntemuksellaan. Ajankohtaisiin tietosuojakysymyksiin pyritään tarjoamaan käytännön läheistä ohjausta, josta tiedotetaan opetuksen järjestäjille ja oppilaitoksille.[179]

Käytännössä ryhmässä on käsitelty mm. eri lainsäädäntöhankkeita, sähköisiä reissuvihkoja, sosiaalisen median käyttöä opetuksessa, oppilashuoltoa ja oppilaiden henkilötietojen käsittelyä esim. kouluterveydenhuollossa sekä koulukuraattori– ja koulupsykologipalveluissa, oppilaitosten roolia ns. etsivässä nuorisotyössä ja kameravalvonnan käyttöä oppilaitoksissa. Ryhmässä on valmisteltu ja kommentoitu myös erilaisia ohjausaineistoja. Se on osaltaan vaikuttanut esimerkiksi Opetushallituksen alun perin vuonna 2004 julkaiseman, viimeksi vuonna 2013 päivitetyn yleisoppaan *Julkisuus ja tietosuoja opetustoimessa*[180] sekä tietosuojavaltuutetun toimiston joulukuussa 2012 julkaiseman, peruskouluille suunnatun oppaan *Oppilaiden henkilötietojen käsittely kodin ja koulun yhteistyössä* sisältöön.[181]

Terveydenhuollon asiantuntijaviranomaisten yhteistyöryhmä TELLU on toiminut jo vuodesta 1999.[182] Ryhmän toimintaan osallistuu edustajia erilaisista terveydenhuollon alalla toimivista organisaatioista, mm. sosiaali– ja terveysministeriöstä, Suomen Kuntaliitosta, kunnista,

---

[176] Kuluttajavirasto ja Kilpailuvirasto yhdistettiin vuoden 2013 alussa.
[177] Esim. TK 2012 s. 8.
[178] KT 2007 s. 6, KT 2012 s. 9.
[179] http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/sidosryhmayhteistyo/opetusalantietosuojanohjausryhma.html, viitattu 9.5.2014.
[180] *Pirjo Vehkamäen*, *Matti Lahtisen* ja *Anne Tamminen–Dahlmanin* kirjoittaman oppaan tuorein versio on saatavilla myös ilmaisena verkkojulkaisuna osoitteesta http://www.oph.fi/download/152370_julkisuus_ja_tietosuoja_opetustoimessa.pdf, viitattu 28.10.2013.
[181] KT 2010 s. 8–9, KT 2011 s. 5–6 ja KT 2012 s. 9–10.
[182] TK 1999 s. 10–11.

Terveyden ja hyvinvoinnin laitoksesta, Suomen lääkäriliitosta, Valvirasta, aluehallintovirastoista, Kelasta ja sairaanhoitopiireistä. Kuten OTTO, TELLU toimii alallaan kehitystä seuraavana ja ajankohtaisia lainsäädäntöhankkeita ja muita tietosuojakysymyksiä käsittelevänä keskustelufoorumina, joka myös tuottaa ohjausmateriaalia. Viime vuosina aiheina ovat olleet esimerkiksi hätäkeskukset, käyttöoikeuksien hallintaan ja lokivalvontaan liittyvät ongelmat, tietosuojavastaavan toimenkuva, tehtävien määrittely ja koulutus, ostopalvelut, sosiaali– ja terveydenhuollon yhteiset asiakkaat, valelääkäritoiminta, sähköinen lääkemääräys, ajanvarausjärjestelmät, potilastietojen luvattoman käsittelyn selvittämisprosessi ja seuraamukset sekä tietosuojavaltuutetun tekemät terveydenhuollon tietosuojaa koskevat lakialoitteet. Vuosina 2008–2012 ryhmä kokoontui yhteensä 19 kertaa eli nelisen kertaa vuodessa. Lisäksi TELLU järjestää vuosittaisia seminaareja, joissa käsitellään ajankohtaisia terveydenhuollon tietosuojakysymyksiä, ja osallistuu muiden tapahtumien järjestämiseen.[183]

Tietosuojavaltuutetun johtama sosiaalihuollon tietosuojan ohjausryhmä SOHVI aloitti toimintansa vuonna 2005. Ryhmään kuuluu sosiaali– ja terveysministeriön, kuntien, Suomen Kuntaliiton, Sosiaaliturvan Keskusliiton ja eri viranomaistahojen edustajia. Ryhmässä keskustellaan ajankohtaisista sosiaalihuollon lainsäädäntöhankkeista ja muista tietosuojakysymyksistä, ja se on myös järjestänyt aiheeseen liittyviä seminaareja. Sosiaali– ja terveydenhuollon liittymäkohtien vuoksi osa ryhmän kokouksista ja seminaareista on toteutettu yhteistyössä TELLUn kanssa. Käsiteltäviä asioita ovat olleet esimerkiksi pakolaisten henkilötietojen käsittely, etsivään nuorisotyöhön liittyvä henkilötietojen käsittely ja kameravalvonnan sallittavuus sosiaalihuollossa. Keskeinen, pitkään SOHVIssa esillä ollut asia oli sosiaalialan tietoteknologiahanke (2005–2011)[184] ja sen puitteissa esille nousseet tietosuojakysymykset. Myös tietosuojavaltuutetun toimiston julkaisema ohje *Sähköpostin käytöstä sosiaalihuollossa* (päivitetty 2010) laadittiin SOHVI–ryhmän puitteissa.[185]

Teletoiminnan ohjausryhmä TERTTU on toiminut vuodesta 2003 tietosuojavaltuutetun toimiston ja ICT–alan edunvalvojan ja yhteistyöjärjestö FiCom ry:n johdolla. Ryhmässä käsitellään ajankohtaisia toimialaan liittyviä kysymyksiä ja seurataan tietoyhteiskuntakehitystä. Käsiteltäviä asioita ovat olleet mm. sähköinen tunnistaminen, luettelo– ja numeropalvelut, älykäs liikenne ja mobiilivarmennepalvelu. Kokouksia on ollut vuosittain muutamia, vuosina 2011 ja 2012 kolme ja kaksi. Tietosuojavaltuutettu myös esittelee kokouksissa toimialaa koskevia kannanottojaan ja ohjausaineistoa ja antaa siten ohjausta ja neuvontaa.[186]

[183] VK 2005 s. 12, VK 2006 s. 9–10, KT 2007 s. 6, KT 2008 s. 10–11, KT 2009 s. 6, KT 2010 s. 6–7, KT 2011 s. 7–8 ja KT 2012 s. 11–12.
[184] Sosiaalialan tietoteknologiahankkeesta ks. tarkemmin http://www.thl.fi/fi_FI/web/fi/aiheet/tietopaketit/tiedonhallinta/aineistot/tikesosarkisto, viitattu 28.1.2014.
[185] VK 2006 s. 10, KT 2007 s. 6, KT 2008 s. 12, KT 2009 s. 6–7, KT 2010 s. 7–8, KT 2011 s. 6 ja KT 2012 s. 10.
[186] KT 2007 s. 6, KT 2008 s. 11, KT 2009 s. 7, KT 2010 s. 8

Markkinoinnin ja asiakkuuden tietosuojaryhmä MAISAn perustivat vuonna 2010 tietosuojavaltuutetun toimisto, Asiakkuusmarkkinointiliitto, IAB Finland ja Teleforum. MAISAn tarkoitus on ”edistää hyvien tietosuojakäytäntöjen syntymistä ja tukea kaupallisen sektorin itsesääntelyä sekä parantaa tiedonvaihtoa eri sektoreiden välillä”. Ryhmä on käsitellyt mm. sosiaalista mediaa, sähköistä suoramarkkinointia, paikkatietojen hyödyntämistä, kanta–asiakasjärjestelmiä ja kuluttajakäyttäytymisen seurantaa. MAISA kokoontui vuonna 2011 neljä kertaa ja vuonna 2012 kolmesti.[187]

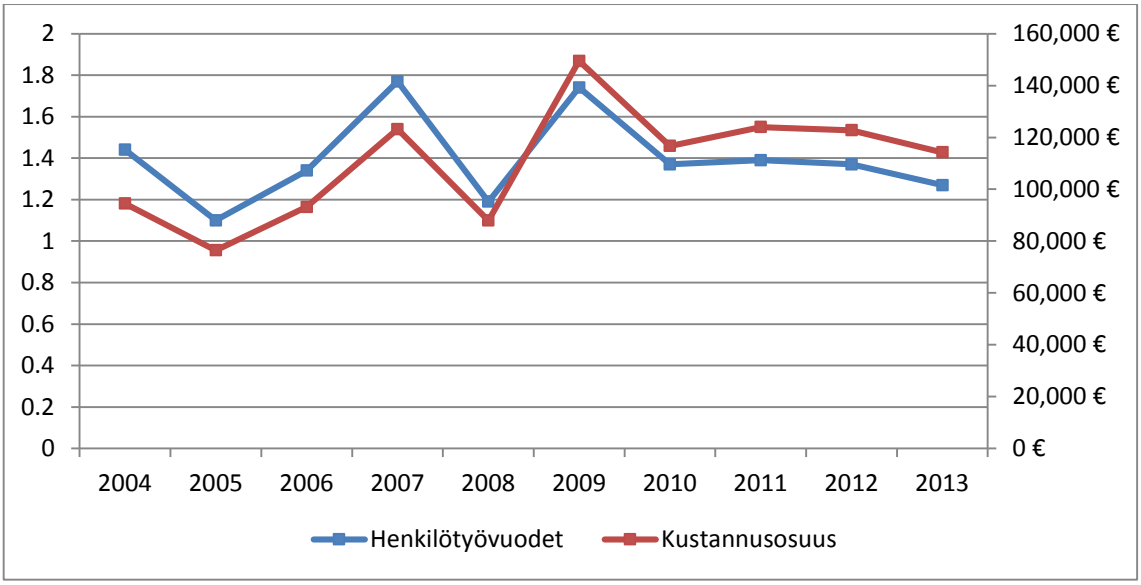
Tieteellisen tutkimuksen sektorilla toimiva tutkimuslupayhteistyöryhmä koostuu THL:n, Kelan, Rekisteritutkimuksen tukikeskuksen sekä sosiaali– ja terveysministeriön edustajista. Ryhmä toimii foorumina tieteelliseen tutkimukseen liittyvistä ajankohtaiskysymyksistä keskustelemiselle. Lisäksi ryhmän tavoitteena on edistää viranomaisten henkilörekisterien käyttöä tieteellisessä tutkimuksessa. Ryhmä on kokoontunut sekä vuonna 2011 että vuonna 2012 neljästi.[188] Tietosuojavaltuutetun toimisto on julkaissut kaksi erityisesti ryhmän käsittelemiin kysymyksiin liittyvää opasta. Julkaisut *Rekisteritutkimuksen tietosuojaopas tutkijoille ja tietopyyntöjä käsitteleville viranomaisille* sekä *Tietosuoja ja tieteellinen tutkimus henkilötietolain kannalta* on päivitetty vuonna 2010.

Vuodesta 2009 lähtien toimineessa Finanssialan tietosuojafoorumissa mukana ovat tietosuojavaltuutetun toimisto, pankki– ja vakuutusalan ja toimijat, Finanssivalvonta sekä kokouksien koolle kutsumisesta vastaava Finanssialan Keskusliitto. Ryhmä käsittelee ajankohtaisia, niin kansallisia kuin kansainvälisiäkin finanssialan tietosuojakysymyksiä. Vuonna 2012 ryhmä kokoontui kolmesti.[189]

4.2 Sidosryhmäyhteistyö tilastoissa

Sidosryhmätyö on ollut varsin laaja–alaista, mikä käy ilmi jo ryhmien suuresta määrästä. Toisaalta useimpien mainittujen ryhmien yhteistyön luonne ei kuitenkaan ole kovinkaan intensiivistä ja päivittäistä, mikä ilmenee mainituista vuosittaisista kokousmääristä. Joka tapauksessa sidosryhmäyhteistyö on vienyt kohtuullisen määrän toimiston resursseista. Siihen on käytetty työaikaa ja rahaa jonkin verran enemmän kuin esimerkiksi edellä käsiteltyihin tiedotukseen ja yleisohjausaineiston tuottamiseen ja päivittämiseen, vuosina 2004–2012 keskimäärin lähes puolitoista henkilötyövuotta ja 110 000 euroa vuodessa. Käytettyjen henkilötyövuosien trendi on ollut vakaa sanotulla aikavälillä, kun taas kustannusten trendi on ollut hienoisesti nouseva, kuten seuraavasta kuvaajasta käy ilmi. Tämä kertonee lähinnä sidosryhmäyhteistyön vakiintuneesta luonteesta ja palkkakustannusten nimellisestä noususta.

[187] KT 2010 s. 9, KT 2011 s. 7 ja KT 2012 s. 10.
[188] KT 2011 s. 8 ja KT 2012 s. 12.
[189] KT 2012 s. 12.



Kuvaaja 24: Sidosryhmäyhteistyöhön käytetyt henkilötyövuodet ja kustannusosuus 2004–2013.

4.3 Käytännesääntötoiminta

4.3.1 Yleistä käytännesäännöistä

Henkilörekisterilaki ei sisältänyt säännöksiä käytännesäännöistä (*codes of conduct, Verhaltensregeln, uppförandekodexar*). Nykyisen tietosuojan käytännesääntötoiminnan perusta on henkilötietolain 42 §, jonka mukaan rekisterinpitäjät tai näitä edustavat yhteisöt voivat laatia toimialakohtaisia käytännesääntöjä henkilötietolain soveltamiseksi ja hyvän tietojenkäsittelytavan edistämiseksi sekä toimittaa laatimansa ehdotukset tietosuojavaltuutetulle. Henkilötietolain 42 §:llä implementoitiin henkilötietodirektiivin 27 artiklan 1 ja 2 kohdat.[190] Uuden tietosuoja–asetusehdotuksen 38 artiklan mukaan kansallisilla valvontaviranomaisilla olisi oikeus antaa lausunto siitä, onko käytännesääntöluonnos asetuksen mukainen. Asetuksessa vaaditaan myös, että valvontaviranomainen pyytää luonnoksista myös rekisteröityjen tai näiden edustajien näkemyksiä, ja listataan käytännesääntöjen laatimisessa erityisesti huomioitavia seikkoja.

Henkilötietolaki sen paremmin kuin muukaan henkilötietoja koskeva lainsäädäntö ei sisällä käytännesäännön määritelmää. Vaikka käytännesäännöt mainitaan lakitekstissä, ei siinä aseteta kenellekään velvollisuutta niiden laatimiseen. Käytännesääntöjen laatiminen on siten vapaaehtoista. Tietosuojavaltuutettu puolestaan voi tarkastaa, että käytännesäännöt ovat henkilötietoja koskevan lainsäädännön mukaisia. Sen sijaan tietosuojavaltuutettu ei varsinaisesti hyväksy tai vahvista käytännesääntöjä. Hänellä ei siis ole sitovaa päätäntävaltaa tässä asiassa. Henkilötietolain käytännesääntöjärjestelmässä kyse onkin eräänlaisesta osittain

[190] HE 96/1998 vp s. 73.

institutionalisoidusta itse– tai myötäsääntelystä, johon tietosuojavaltuutettu viranomaisena vaikuttaa ohjaavasti.[191]

Käytännesäännöt eivät ole vain henkilötietojen käsittelyyn ja tietosuojaan liittyvä ilmiö. Yleisesti käytännesäännöissä määritellään tavallisesti tietyn toimialan pelisäännöt ja yhteiset toimintatavat, mahdollisesti tiettyä toiminnan osaa – kuten henkilötietojen käsittelyä – koskien. Henkilötietojen käsittelyä koskevat käytännesääntömääräykset voivat kuitenkin sisältyä myös laajempaan alan kaikenlaista toimintaa ohjaavaan säännöstöön. Käytännesääntöjä laativat lähinnä kunkin alan yhteistyö– ja etujärjestöt, mutta myös yksittäiset alalla toimijat. Luonteeltaan käytännesäännöt ovat yleensäkin itsesääntelyä, ja niillä voidaan pyrkiä joko tuomaan selvyyttä lain aukkokohtiin tai toisaalta torjumaan lainsäätäjän väliintulo ja alan yksityiskohtainen sääntely laissa.[192] *Ahti Saarenpää* on luonnehtinut käytännesääntöjä *kertomuksiksi lain sisällöstä*. Hänen mukaan niiden avulla välitetään lakitekstiä yksityiskohtaisemmalla tavalla ohjeita ja tietoa hyvästä, yksilön oikeudet huomioon ottavasta henkilötietojen käsittelystä.[193] Käytännesääntöjä on myös kuvattu *soft law* –tyyppiseksi aineistoksi.[194]

Tietosuojavaltuutetun toimisto on julkaissut verkkosivuillaan oppaan *Toimialakohtaisten käytännesääntöjen laatiminen* (päivitetty 2010). Oppaassa ei määritellä käytännesääntöjä, mutta niiden tarkoituksesta todetaan seuraavaa:

> Käytännesääntöjen tarkoituksena on luoda eri toimialoille henkilötietojen käsittelyä koskevaa ohjausta ja suosituksia siitä, millä tavoin alan yritysten, yhteisöjen, laitosten tai viranomaisten toiminnassaan käsittelemien henkilötietojen käsittelyssä henkilöiden yksityisyys ja muut yksityisyyden suojaa turvaavat perusoikeudet tulee ja voidaan ottaa huomioon. Käytännesääntöjä voivat laatia esimerkiksi eri järjestöt jäsenistölleen ja viranomaiset toimivaltansa puitteissa hallinnonalansa viranomaisille ja laitoksille.
>
> Tavoitteena on, että toimialakohtaisessa ohjauksessa voitaisiin ottaa huomioon nimenomaan alan erityiskysymykset. Näin voidaan merkittävästi myös helpottaa ja vähentää toimialan jäsenistöön tai sen piiriin kuuluvien yhteisöjen, yritysten, yhdistysten ja viranomaisten tai laitosten työtä. Toimialojen toteuttamana menettelyt voidaan suunnitella palvelemaan samalla toiminnallisia tavoitteita.[195]

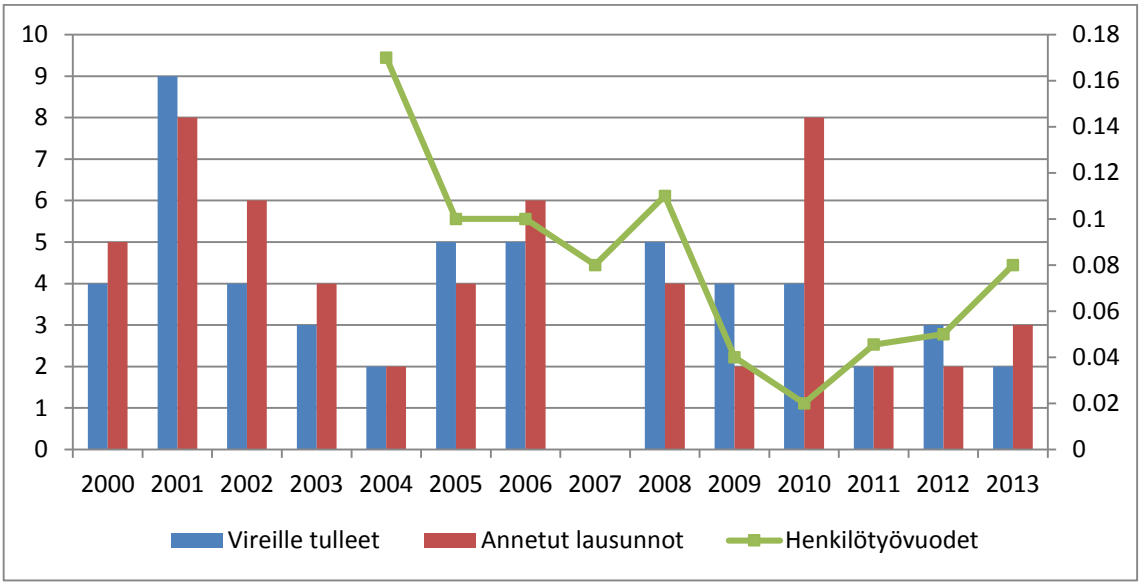
Oppaassa myös todetaan, että käytännössä tietosuojavaltuutetun suorittama tarkastus voi tarkoittaa muun muassa sitä, että tietosuojavaltuutettu toteaa käytännesäännöt asianmukaisiksi, edellyttää niiden tarkastamista tai täydentämistä taikka antaa ohjausta niiden kehittämiseksi. Lisäksi oppaassa todetaan nimenomaisesti, että tietosuojavaltuutettu ohjaa laatijoita myös käytännesääntöjen valmistelun aikana.[196]

---

[191] Ks. HE 96/1998 vp s. 73 ja *Voutilainen*, ICT–oikeus sähköisessä hallinnossa (2009) s. 110, 117.
[192] *Neuvonen*, Tapaoikeus oikeuslähdeopissa, LM 3/2006 s. 416–417, 432. Neuvonen luokittelee käytännesäännöt osaksi *tapaoikeutta*.
[193] *Saarenpää*, Henkilö– ja persoonallisuusoikeus, teoksessa *Tammilehto* (toim.), Oikeusjärjestys. Osa 1 (2012) s. 342.
[194] *Tuori*, Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota, LM 7–8/2004 s. 1213.
[195] TSV:n toimisto, Toimialakohtaisten käytännesääntöjen laatiminen (2010) s. 2.
[196] TSV:n toimisto, Toimialakohtaisten käytännesääntöjen laatiminen (2010) s. 2.

4.3.2 Lausunnot käytännesäännöistä ja käytetyt resurssit

Tietosuojavaltuutetun toimisto on antanut käytännesäännöistä lausuntoja vuosittain nollasta kahdeksaan. Lausuntoja on annettu yhteensä 56 vuosina 2000–2013.



Kuvaaja 25: Vireille tulleet käytännesääntöjä koskevat lausuntopyynnöt ja tietosuojavaltuutetun toimiston niistä antamat lausunnot vuosina 2000–2013 (vasen asteikko) sekä käytännesääntötyöhön käytetyt henkilötyövuodet 2004–2013 (oikea asteikko).

Käytännesääntöjä on laadittu varsin erilaisille aloille, muun muassa suoramarkkinointiin, puhelinmyyntiin, sosiaali– ja terveysalalle, luottolaitosten toimintaan ja sukututkimukseen. Laatijat ovat olleet kunnallisia ja valtiollisia viranomaisia, mutta usein myös erilaisia toimialajärjestöjä tai yhdistyksiä. Joukossa on myös muutama yksittäinen yrityskin. Aktiivisin käytännesääntöjen laatija on ollut väestörekisterikeskus, joka on pyytänyt lausuntoa lukuisista käytännesäännöistä, jotka ovat koskeneet väestötietojärjestelmän tietojen käyttöä eri tarkoituksiin. Kaikista 56:sta (lokakuuhun 2013 mennessä) diarioidusta käytännesääntöasiasta 17 on koskenut väestörekisterikeskuksen laatimia käytännesääntöjä.[197]

Lausuntojen antaminen käytännesäännöistä ei ole muodostunut tietosuojavaltuutetun toimistolle erityisen paljon aikaa tai resursseja vieväksi toiminnaksi. Esimerkiksi vuonna 2013 käytännesääntötyöhön kului vain 0,08 henkilötyövuotta, ja sen kustannusosuus oli 3 694 euroa.[198] Vuonna 2010, kun lausuntoja valmistui kahdeksan, vastaavat luvut olivat vielä pienempiä: 0,02 henkilötyövuotta ja 1059 euroa.[199] Tilastojen mukaan eniten resursseja käytännesääntötoimintaan on kulunut vuonna 2004: 0,17 henkilötyövuotta ja 8 923 euroa.[200] Erot eri vuosien välillä ovat olleet euromääräisesti varsin pieniä eikä merkittävää kehitystä ole

[197] Tieto perustuu tietosuojavaltuutetun toimiston julkisiin diaaritietoihin, joita on seurattu 15.10.2013 saakka.
[198] TK 2012 s. 9.
[199] TK 2010 s. 9.
[200] TK 2004 s. 9. Vuosilta 2000–2003 ei tosin ole saatavilla vastaavia tietoja.

tapahtunut suuntaan tai toiseen. Käytännesääntötoiminta on ollut lukujen valossa erittäin pieni osa tietosuojavaltuutetun toimiston toimintaa. Käytännön merkitykseltään se on saattanut olla hyvinkin kustannustehokas keino edistää henkilötietojen asiamukaista käsittelyä, etenkin koska osa käytännesäännöistä on koskenut kokonaisia toimialoja.

5. Kansainvälinen toiminta

5.1 Yleistä kansainvälisestä toiminnasta

Tietosuojaviranomaiset ovat perustamisestaan lähtien osallistuneet kansainväliseen yhteistyöhön ja toimintaan alallaan. Tietosuojavaltuutetun velvollisuus tällaiseen toimintaan kävi alun perin ilmi tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun asetuksen (477/1987) 2 § 6 kohdasta, jonka mukaan tietosuojavaltuutetun tehtävänä oli huolehtia henkilörekisterien sääntelyyn ja valvontaan liittyvistä kansainvälisistä asioista ja yhteistyöstä. Nykyinen säädösperusta löytyy lain tasolta. Tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain (389/1994) 5 § 4 kohdassa todetaan, että tietosuojavaltuutetun tehtävänä on huolehtia henkilötietojen käsittelyyn liittyvästä kansainvälisestä yhteistyöstä.[201] Tietosuojalautakunnalla ei ole vastaavaa laissa säädettyä tehtävää tai velvollisuutta kansainväliseen toimintaan. Lautakunnan puheenjohtaja ja sihteeri ovat kuitenkin osallistuneet kansainvälisiin kokouksiin mahdollisuuksien ja resurssien puitteissa.[202]

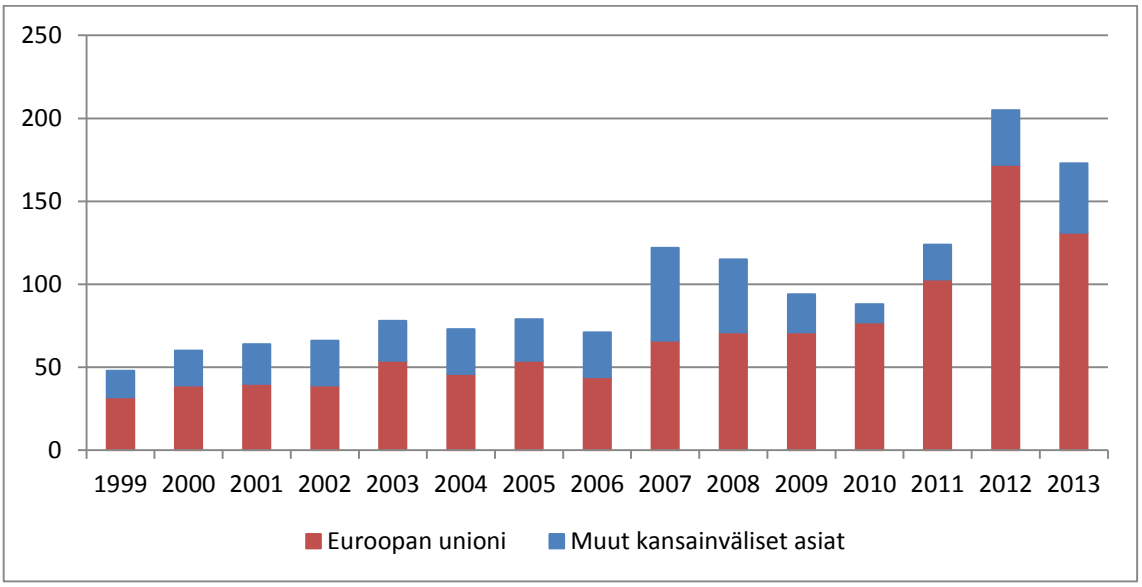
Kansainvälinen toiminta voidaan jaotella nykyään kolmeen osaan sen maantieteellisen suuntautumisen perusteella. Varsinkin 1980–luvulla ja 1990–luvun alkupuolella ydinasemassa oli pohjoismaiden välinen yhteistyö. Tämä yhteistyö on jatkunut nykypäivään saakka, mutta Suomen liityttyä Euroopan unioniin on unionin puitteissa työskentelystä tullut selvästi keskeisin kansainvälisen toiminnan muoto. Tietosuojaviranomaiset ovat lisäksi osallistuneet alusta lähtien kansainväliseen toimintaan myös EU:n ja pohjoismaiden ulkopuolella.

Tässä luvussa esittelen ensin yleisiä tilastotietoja kansainvälisestä toiminnasta, minkä jälkeen esitän tarkempia tietoja kansainvälisen toiminnan osa–alueista kuvattua kolmijakoa noudattaen. Luvun tiedot ovat pääosin peräisin tietosuojavaltuutetun toimiston toiminta– ja vuosikertomuksista sekä Tietosuoja–lehdestä.

Kansainväliseen toimintaan liittyviä diarioituja asioita on tullut vireille ja käsitelty 2000–luvulla vuotta kohden keskimäärin vajaa sata. Lukumäärän trendi on ollut nouseva. Kansainvälisten asioiden osuus kaikista asioista on ollut noin neljä prosenttia, vuonna 2013 viisi prosenttia. Erilaiset EU–asiat muodostavat kansainvälisistä asioista ylivoimaisesti

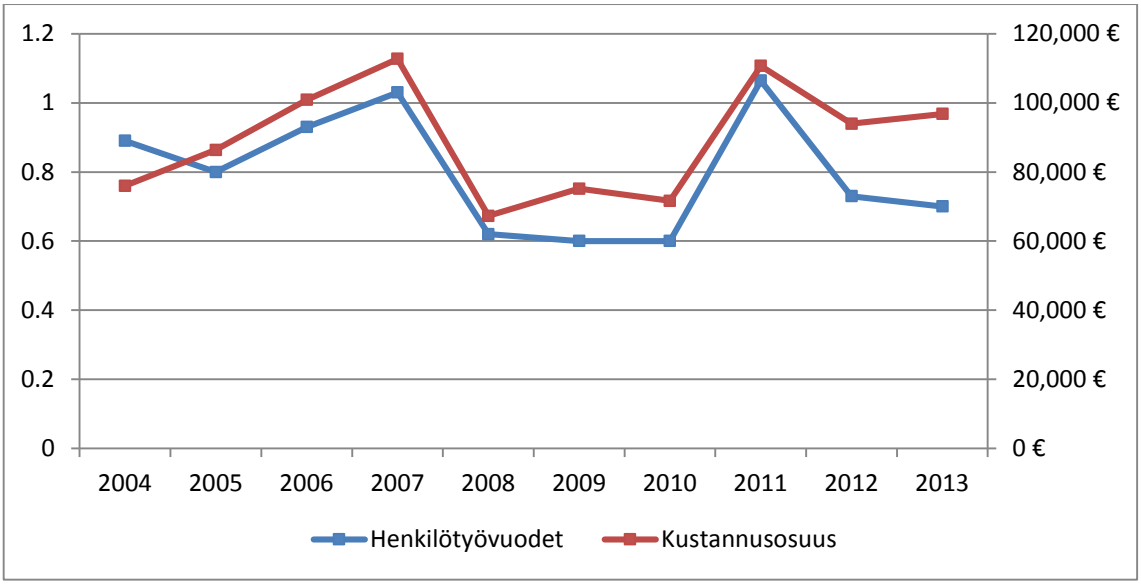
[201] Säännösten sanamuodon ero on lähinnä kielellinen. Säännösten vastaavuus todetaan nykyistä tietosuojalautakunnasta ja tietosuojavaltuutetusta annettua lakia koskevassa hallituksen esityksessä (HE 311/1993 vp s. 19).
[202] Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki.

suurimman ryhmän, sillä niitä on jo yli 80 prosenttia kaikista kansainvälisistä asioista, kun osuus vielä 2000–luvun alkupuoliskolla oli noin kaksi kolmasosaa.



Kuvaaja 26: Vireille tulleiden kansainvälisten asioiden määrä ja EU–asioiden osuus 1999–2013.

Asiamäärät eivät tietystikään kerro koko totuutta kansainvälisten asioiden merkityksestä tai painoarvosta. Kansainvälisen toiminnan ”asia” on luonteeltaan tyypillisesti varsin erilainen kuin kansalaisen esittämä toimenpidepyyntö tai tarkastusoikeuden toteuttamista koskeva hakemus. Kansainvälisessä toiminnassa kysymys on – kuten TSL–TSVL 5 § 4 kohdan sanavalintakin osoittaa – lähinnä *yhteistyöstä*, jota toteutetaan erilaisten kokousten, neuvottelujen, luentojen, seminaarien ja kirjeenvaihdon muodossa. Toiminnan laajuutta kuvaakin huomattavasti paremmin siihen käytetyn työajan määrä, jota ei ole tilastollisesti jaoteltu EU–asioiden ja muiden kansainvälisten asioiden välillä. Toimintakertomus– ja vuosikatsaustietojen valossa on kuitenkin ilmeistä, että EU–asiat vaativat myös valtaosan kansainvälisen toiminnan resursseista, joiden kokonaismäärää kuvaa seuraava kuvaaja.



Kuvaaja 27: Kansainväliseen toimintaan käytetyt henkilötyövuodet ja kustannusosuus 2004–2013.

Keskimäärin kansainväliseen toimintaan on tarkasteluvälillä käytetty vajaa henkilötyövuosi ja noin 90 000 euroa vuodessa. Tämä tarkoittaa hieman yli kolmen ja puolen prosentin osuutta henkilötyövuosista ja lähes kuuden prosentin osuutta kustannuksista. Ero selittyy sillä, että kansainvälisessä toiminnassa palkkamenojen ohella kustannuksia aiheuttaa luonnollisesti matkustaminen. Huomattavaa on, että kansainväliseen toimintaan käytettyjen resurssien määrä ei ole kasvanut diarioitujen kansainvälisten asioiden määrän tahtia. Vuosina 2004–2013 ei ole havaittavissa mainittavaa kasvutrendiä.

5.2 Pohjoismainen yhteistyö

Tietosuojaviranomaiset ovat osallistuneet pohjoismaiseen yhteistyöhön olemassaolonsa alusta alkaen. Heti vuonna 1988 järjestettiin Helsingissä pohjoismaisten tietosuojaviranomaisten kokous, johon osallistuivat mm. tietosuojavaltuutettu, tietosuojavaltuutetun toimiston toimistopäällikkö sekä tietosuojalautakunnan puheenjohtaja.[203] Samana vuonna tietosuojavaltuutettu ja tietosuojalautakunnan puheenjohtaja osallistuivat myös Uumajan ja Vaasan yliopistojen järjestämään seminaariin, jossa tarkasteltiin vertaillen Suomen ja Ruotsin tietosuojalainsäädäntöjä.[204]

Pohjoismaiset tietosuojaviranomaiset ovat kokoutuneet vuosittain aina tämän jälkeen ja käsitelleet kulloinkin ajankohtaisia aiheita. Varsinaisten tietosuojaviranomaisten kokousten lisäksi 1990–luvulta lähtien vuosittain järjestettiin myös pohjoismainen esittelijäkokous sekä

[203] Asialistalla tässä kokouksessa olivat henkilörekistereihin liittyvät teknisen suojauksen ongelmat, terveydenhuollon rekistereiden tietosuoja, hallinnollisten rekistereiden kaupallinen käyttö, telemarkkinointi, henkilötunnuksen käyttö ja luottotietorekisterit.
[204] TK 1987–1988 s. 25.

IT–asiantuntijoiden kokous. Säännöllisiä pohjoismaisia kokouksia oli siis yleensä kolme vuodessa. Viime vuosina erilliset kokoukset on koottu yhteen siten, että esittelijät, IT–asiantuntijat ja virastojen johto ovat kokoontuneet yhtä aikaa, mutta jakautuneet osaksi aikaa alakokouksiin käsittelemään eri asiaryhmiä.[205] Säännöllisten viranomaisten välisten kokousten lisäksi tietosuojavaltuutetun toimisto on osallistunut myös erinäisiin muihinkin pohjoismaisiin tietosuoja–asioita käsitelleisiin konferensseihin.[206] 2000–luvulla pohjoismaiset tietosuojaviranomaiset ovat organisoineet myös yhteistä tarkastustoimintaa.[207]

Koska Suomi, Ruotsi ja Tanska ovat nykyään myös EU:n jäsenvaltioita, limittyy pohjoismainen yhteistyö EU:n tietosuojaa koskevan toiminnan kanssa. Esimerkiksi Oslossa 21.–22.5.2012 järjestetyssä kokouksessa tärkeimpänä aiheena oli keskustelu ehdotetun uuden EU:n tietosuojalainsäädännön vaikutuksista. Kokouksen päätteeksi tietosuojaviranomaiset antoivat aiheesta myös yhteisen julkilausuman.[208]

5.3 Toiminta Euroopan unionissa

Suomi liittyi Euroopan unioniin vuoden 1995 alussa, tietosuojan kannalta varsin mielenkiintoisella hetkellä: jo liittymisvuoden lokakuussa hyväksyttiin EU:n henkilötietodirektiivi (95/46/EY), jonka pohjalta aloitettiin saman tien henkilötietolain säätämiseen johtanut uudistamistyö. Sittemmin EU:n toiminnan tiivistyttyä monella saralla ovat tietosuojakysymykset nousseet esille useissa yhteyksissä, esimerkiksi sähköisen viestinnän tietosuojadirektiivin, mutta myös Schengen– ja poliisiyhteistyön myötä. EU:n myötä henkilötietojen suojasta on tullut myös itsenäinen, EU:n perusoikeuskirjan 8 artiklassa säännelty perusoikeus.[209] EU:n monitasoinen tietosuojasääntely ja sen kehittäminen vaativat luonnollisesti kansallisilta tietosuojaviranomaisilta yhteistyötä ja koordinaatiota.

Säädöstasolla EU:n jäsenvaltioiden tietosuojaviranomaisten keskinäistä yhteistyötä edellyttää ensinnäkin henkilötietodirektiivin 28 artiklan 6 kohta. Tähän perustuvan henkilötietolain 38.3 §:n mukaan tietosuojaviranomaiset toimivat yhteistyössä muiden Euroopan unionin jäsenvaltioiden tietosuojaviranomaisten kanssa ja antavat tarvittaessa virka–apua.

Virka–avun antamisen ja muun kahdenvälisen yhteistyön lisäksi EU:n puitteissa tietosuojavaltuutetun toimisto osallistuu henkilötietodirektiivin 29 artiklan mukaisen

[205] Tietosuojavaltuutettu Reijo Aarnion haastattelu, 5.5.2014, Helsinki.
[206] KT 2011 s. 11.
[207] VK 2004 s. 7 ja tietosuojavaltuutettu Reijo Aarnion haastattelu 5.5.2014, Helsinki. Viimeaikaiset yhteisprojektit ovat liittyneet pankkien henkilötietojen käsittelyyn liittyviin käytäntöihin, Spotify–suoratoistopalveluun ja autojen seurantalaitteisiin (”mustiin laatikoihin”). Ks. myös http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2014/01/pohjoismainenselvityspankeille.html, viitattu 9.5.2014.
[208] KT 2012 s. 15. Kokoukseen osallistuivat Norjan, Suomen, Ruotsin, Islannin, Tanskan, Färsaarten ja Ahvenanmaan tietosuojaviranomaiset.
[209] Lissabonin sopimuksen jälkeen perusoikeuskirjalla on jäsenvaltioita ja siten myös Suomea sitova luonne.

tietosuojatyöryhmän (Article 29 Working Party, WP 29) toimintaan. Itsenäisesti toimiva tietosuojatyöryhmä antaa komissiolle lausuntoja ja suosituksia tietosuojaan liittyvistä asioista. Työryhmässä ovat edustettuina kunkin jäsenvaltion tietosuojaviranomaiset, EU:n tietosuojavaltuutettu ja komissio.[210] Työryhmän tehtävistä on säädetty henkilötietodirektiivin 30 artiklassa ja sähköisen viestinnän tietosuojadirektiivin 15 artiklan 3 kohdassa, ja se on myös hyväksynyt itselleen työjärjestyksen.[211] Työryhmän yhteydessä toimii alatyöryhmiä, joista tietosuojavaltuutetun toimisto on viime vuosina keskittynyt erityisesti Technology Subgroup –ryhmään.[212]

Mainittujen yhteistoimintamuotojen ohella tietosuojavaltuutetun toimisto osallistuu myös muiden työryhmien sekä useiden erilaisten EU–valvontaelinten toimintaan. Näitä valvontaelimiä ovat Europolin yhteinen valvontaelin, Europolin yhteisen valvontaelimen muutoksenhakukomitea, Schengenin tietojärjestelmän yhteinen valvontaelin, Tullitietojärjestelmän yhteinen valvontaelin sekä yhteisen valvonnan koordinaatioryhmä, EURODAC–järjestelmän yhteinen valvonta sekä tuoreimpana syksyllä 2012 toimintansa aloittanut viisumitietojärjestelmän yhteinen valvontaryhmä.[213]

EU:n puitteissa järjestetään myös yleisluontoisempia tietosuojaviranomaisten ja esittelijöiden kokoontumisia, joihin tietosuojavaltuutettu on osallistunut.[214] EU–yhteistyöhön kuuluu myös kansainvälistä koulutuksellista toimintaa. Koulutusta on annettu myös komission rahoittaman, asiantuntija–apua EU:n ns. laajentumis– ja naapurimaille tarjoavan TAIEX–ohjelman myötä. Tässä ohjelmassa tietosuojavaltuutettu on toiminut asiantuntijana, ja toimisto on isännöinyt ulkomaisten delegaatioiden tietosuoja–asioihin liittyviä opintomatkoja. Vaikka TAIEX on EU:n rahoittamaa toimintaa, ovat avun kohdemaat EU:n ulkopuolisia valtioita. TAIEX–toiminta voidaankin nähdä myös osana muuta, Euroopan ulkopuolelle suuntautuvaa kansainvälistä toimintaa.[215]

Toimintakertomusten tilastoista ilmeneviä asiamääriä tarkasteltaessa EU:n piirissä tapahtuva kirjeenvaihto sekä 29 artiklan mukaisen tietosuojatyöryhmän ja muiden EU:n työryhmien toiminta ovat nousseet suurimmiksi kansainvälisen toiminnan asiaryhmiksi. Muutaman viime vuoden suurta EU–asioiden määrää selittää osaltaan ehdotus uudeksi EU:n

[210] Ryhmän puheenjohtajana toimii tätä kirjoitettaessa hollantilainen *Jacob Kohnstamm*.
[211] Työjärjestys ja työryhmän tuottamat asiakirjat ovat saatavilla työryhmän verkkosivuilla, http://ec.europa.eu/justice/data–protection/article–29/index_en.htm, viitattu 28.1.2014.
[212] Esim. VK 2012 s. 13.
[213] KT 2012 s. 12–15. Perustietoa valvontaelimistä on saatavilla esimerkiksi tietosuojavaltuutetun toimiston sivuilta ja Euroopan tietosuojavaltuutetun sivujen kautta, ks. http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/kansainvalinenyhteistyo/valvontaelimet_0.html, viitattu 9.5.2014 ja https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/pid/79, viitattu 16.1.2014.
[214] Esim. KT 2010 s. 13, KT 2011 s. 11–12, KT 2012 s. 15–16.
[215] Esim. VK 2007 s. 20, TK 2011 s. 14 ja http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2014/02/fyromnmacedoniadelegaationopintomatka3.–6.3.tietosuojavaltuutetuntoimistoon.html, viitattu 9.5.2014. TAIEX–ohjelmasta ks. tarkemmin http://ec.europa.eu/enlargement/taiex/index_en.htm, viitattu 1.4.2014 ja http://www.formin.fi/public/default.aspx?contentid=201547&contentlan=1&culture=fi–FI, viitattu 1.4.2014.

tietosuojalainsäädännöksi. EU–asioiden lukumäärien ja jakauman kehitys käy ilmi seuraavasta taulukosta.

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Euroopan unioni	*46*	*54*	*44*	*66*	*71*	*71*	*77*	*103*	*172*	*131*
-Tietosuojaryhmän (Art. 29) kokoukset	7	4	2	4	5	3	3	8	11	7
--ed. kokouksiin liittyvä kirjeenvaihto	17	6	7	6	7	4	4	11	28	24
-EU:n muut työryhmät	3	12	7	18	17	23	10	16	30	28
-Virka-apupyynnöt	0	1	0	1	1	2	4	2	12	2
-Unionin piirissä tapahtuva kirjeenvaihto	1	5	9	12	16	17	33	42	62	52
-Europol-valvontaryhmä	9	8	5	8	9	8	8	8	5	4
-Muut Europol-asiat	0	3	1	4	6	1	2	1	6	1
-Tullijärjestelmään (CIS) liittyvät asiat	2	1	4	4	4	6	6	6	9	7
-Schengen-valvontaryhmä	5	6	4	5	4	6	4	4	2	4
-Muut Schengen-asiat	2	8	4	4	2	1	3	5	7	2
-CNSA	0	0	1	0	0	0	0	0	0	0

Taulukko 2: Vireille tulleet EU–asiat 2004–2013.

Uusi tietosuoja–asetus muuttaa eri jäsenvaltioiden kansallisten viranomaisten roolia ja toimivaltuuksia merkittävästi jo siitä syystä, että se on kaikissa jäsenvaltioissa suoraan sovellettavaa oikeutta. Asetuksessa on myös nimenomaisesti kiinnitetty huomiota yhteistyön järjestämiseen ja yhdenmukaiseen soveltamiseen. Näitä koskevat säännökset on sijoitettu asetuksen VII lukuun. Luvussa säädetään viranomaisten keskinäisestä avunannosta, velvollisuudesta toteuttaa yhteisiä tutkintatehtäviä, täytäntöönpanotoimenpiteitä ja muita operaatioita,[216] uudesta yhdenmukaisuusmekanismista sekä 29 artiklan mukaisen tietosuojatyöryhmän korvaavasta uudesta Euroopan tietosuojaneuvostosta, jonka tehtävä on varmistaa asetuksen yhdenmukainen soveltaminen.[217] Siinä missä 29 artiklan mukainen tietosuojatyöryhmä on ollut luonteeltaan ensisijaisesti suosituksia ja lausuntoja antava keskustelufoorumi, tietosuojaneuvostolla tulee olemaan vahvempia keinoja harmonisoinnin toteuttamiseen, ja päätöksenteolla tulee olemaan sen toiminnassa suurempi rooli.[218] Tietosuojaneuvoston muodostavat yksi valvontaviranomaisen johtaja kustakin jäsenvaltiosta ja Euroopan tietosuojavaltuutettu.[219] Suomea tietosuojaneuvostossa tullee edustamaan

[216] Kuten edeltä käy ilmi, yhteisiä operaatioita on harjoiteltu pienemmässä piirissä eli pohjoismaiden kesken jo ennen asetusta.

[217] 66 artiklan 1 kohdan mukaan Euroopan tietosuojaneuvosto toteuttaa joko omasta aloitteestaan tai komission pyynnöstä erityisesti seuraavia tehtäviä: a) antaa komissiolle neuvoja kaikissa henkilötietojen suojaan unionissa liittyvissä kysymyksissä, myös tämän asetuksen mahdollisessa muuttamisessa; b) tarkastelee omasta aloitteestaan tai jonkin jäsenensä tai komission pyynnöstä kysymyksiä, jotka koskevat tämän asetuksen soveltamista, ja antaa valvontaviranomaisille osoitettuja suuntaviivoja, suosituksia ja parhaita käytänteitä, joiden tarkoituksena on tukea tämän asetuksen johdonmukaista soveltamista; c) tarkastelee b alakohdassa tarkoitettujen suuntaviivojen, suositusten ja parhaiden käytänteiden soveltamista käytäntöön ja raportoi asiasta komissiolle säännöllisesti; d) antaa lausuntoja valvontaviranomaisten päätösluonnoksista 57 artiklassa tarkoitetun mekanismin mukaisesti; e) edistää valvontaviranomaisten välistä yhteistyötä ja tehokasta kahden– ja monenvälistä tietojen ja käytänteiden vaihtamista; f) edistää yhteisiä koulutusohjelmia ja tukee henkilövaihtoa valvontaviranomaisten välillä sekä tarvittaessa kolmansien maiden tai kansainvälisten järjestöjen valvontaviranomaisten kanssa; g) edistää tietosuojalainsäädäntöä ja käytänteitä koskevien tietojen ja asiakirjojen vaihtoa tietosuojaviranomaisten kesken kaikkialla maailmassa.

[218] Ks. *Saarenpää*, Data protection in the network society – the exceptional becomes the natural, teoksessa *Galindo* (ed.), El derecho de la sociedad en red (2013) s. 113.

[219] Lisäksi komissiolla on oikeus osallistua tietosuojaneuvoston toimintaan ja nimetä sinne edustaja.

tietosuojavaltuutettu, ja osallistumisesta Euroopan tietosuojaneuvoston toimintaan näyttääkin olevan tulossa merkittävä osa tietosuojavaltuutetun kansainvälistä toimintaa.

5.4 Muu kansainvälinen toiminta

Tietosuojaviranomaisten toiminnan alkuvuosina oli havaittavissa kahtiajako pohjoismaiseen ja maailmanlaajuiseen yhteistyöhön. Kahtiajaon on sittemmin korvannut edellä selostettu EU:n merkityksen kasvu, mutta maantieteellisesti laajempi kansainvälinen toiminta ei suinkaan ole loppunut tai menettänyt merkitystään.

Maailmanlaajuisen yhteistyön tärkeänä foorumina ovat toimineet jo vuodesta 1979 lähtien vuosittain järjestetyt kansainväliset tietosuojaviranomaisten maailmankokoukset.[220] Maailmankokouksissa mm. keskustellaan ajankohtaisista henkilötietojen suojaan liittyvistä asioista ja annetaan niistä julkilausumia. Tietosuojavaltuutettu on osallistunut kokouksiin säännöllisesti heti 1980–luvun lopulta lähtien. Usein kokouksiin on osallistunut myös muita toimiston henkilöstöön kuuluvia ja tietosuojalautakunnan edustajia.

Maailmankokousten lisäksi tietosuojavaltuutetun toimisto on osallistunut lukuisiin muihinkin tietosuojaan ja henkilötietojen suojaan liittyviä erityisiä aiheita käsitelleisiin maailmanlaajuisiin konferensseihin ja kokouksiin ja pitänyt niissä luentoja.[221] Muuhun kansainväliseen toimintaan on kuulunut myös osallistuminen opiskelijavaihto–ohjelmaan, jonka kautta tietosuojavaltuutetun toimisto on saanut harjoittelijoita Georgetownin yliopistosta Yhdysvalloista.[222]

Kuten aiemmin jo on mainittu, varsinkin varhaisessa tietosuoja–asioiden kansainvälisessä, pääosin hallitustenvälisessä lainsäädäntöyhteistyössä puitteina toimivat Euroopan neuvosto ja maailmanlaajuisemmin Taloudellisen yhteistyön ja kehityksen järjestö (OECD) sekä Kansainvälinen työjärjestö (ILO).[223] Myös suomalaiset tietosuojaviranomaiset osallistuivat ainakin 80– ja 90–luvuilla joihinkin näiden järjestöjen kokouksiin.[224] Vaikka toiminta näissä järjestöissä jatkuu tietosuoja–asioissa edelleen, ei tietosuojavaltuutetun toimisto juuri ole 2000–luvulla osallistunut tähän toimintaan.

[220] Viimeisin, 35. kokous järjestettiin Puolan Varsovassa 23.–26.9.2013. Ks. tapahtuman verkkosivut osoitteessa https://privacyconference2013.org, viitattu 14.11.2013.
[221] Esim. KT 2008 s. 8, KT 2010 s. 13 ja KT 2012 s. 16–17.
[222] VK 2005 s. 7 ja KT 2009 s. 8.
[223] Näiden järjestöjen puitteissa suoritetusta varhaisesta suosituksiin, julkilausumiin ja sopimuksiin johtaneesta yhteistoiminnasta ks. edellä I.2.1.
[224] Esim. TK 1987–1988 s. 26–27, TK 1993 s. 14 ja TK 1995 s. 14.

6. Muu toiminta

6.1 Etukäteisvalvonta

Tietosuojavaltuutettu suorittaa sekä etukäteistä että jälkikäteistä valvontaa. Etukäteisvalvontaa on henkilötietolain 36 §:ssä tarkoitettujen ilmoitusasioiden käsittely.[225] Rekisterinpitäjien on ilmoitettava tietosuojavaltuutetulle henkilötietojen automaattisesta käsittelystä lähettämälle tälle rekisteriseloste (ns. rekisteri–ilmoitus). Tästä säännöstä on kuitenkin lukuisia poikkeuksia, jotka rajoittavat sen käytännön merkitystä. Rekisterinpitäjien on ilmoitettava myös henkilötietojen siirrosta EU/ETA–alueen ulkopuolelle tietyissä tapauksissa ja automatisoidun päätöksentekojärjestelmän käyttöönotosta. Velvollisuus ns. toimintailmoituksen tekemiseen on sillä, joka harjoittaa elinkeinona perimistoimintaa tai markkina– tai mielipidetutkimusta taikka hoitaa toisen lukuun henkilöstön valintaan ja soveltuvuuden arviointiin liittyviä tehtäviä tai tietojenkäsittelytehtäviä ja tässä toiminnassa käyttää tai käsittelee henkilörekistereitä ja niissä olevia tietoja, sekä luottotietolain 38 §:n mukaisesti luottotietotoiminnan harjoittajilla.

Henkilörekisterilaissa ilmoitusvelvollisuudesta säädettiin 22 ja 30 §:ssä. 30 §:n 1 momentti koski rekisteri–ilmoituksia sekä henkilötietojen luovuttamista ulkomaille ja 2 momentti toimintailmoituksia. Täydentävää sääntelyä sisältyi lisäksi henkilörekisteriasetuksen 15–17 §:iin. Erona henkilötietolakiin henkilörekisterilain 22 §:n ilmoitusvelvollisuus ulkomaille luovutuksista ei ollut rajattu tilanteisiin, joissa henkilötietoja luovutettiin EU/ETA–alueen ulkopuolelle. Tässä tilanteessa henkilötietolaki siis supisti ilmoitusvelvollisuutta, mutta muutoin henkilötietolaki laajensi ilmoitusvelvollisuutta lukuisiin uusiin tilanteisiin. Henkilötietolain mukaan ilmoitusvelvollisuus aiemmasta poiketen on olemassa, kun:

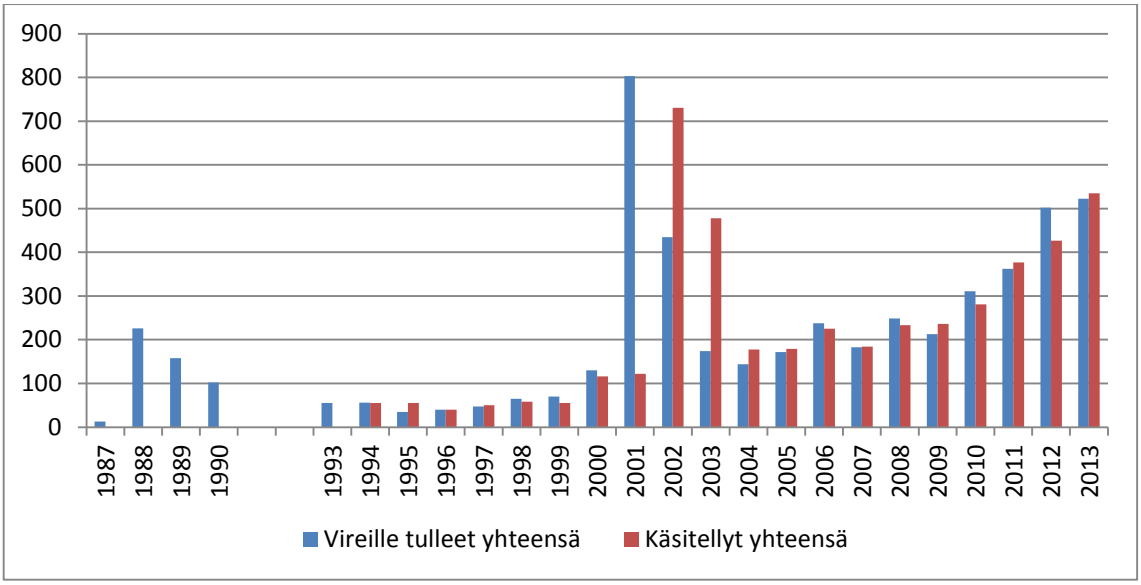
1) otetaan käyttöön HetiL 31 §:ssä tarkoitettu automatisoitu päätöksentekojärjestelmä;
2) käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta (HetiL 8.1 §:n 4 kohdan loppuosa);
3) käsitellään henkilötietoja HetiL 8.1 §:n 5 kohdan nojalla muun kuin asiakas– tai palvelussuhteen tai jäsenyyteen verrattavan suhteen perusteella;
4) arkaluonteisten tietojen käsittely johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä (HetiL 12.1 §:n 5 kohdan loppuosa);
5) käsitellään arkaluonteisia tietoja historiallista tai tieteellistä tutkimusta taikka tilastointia varten, jos tietoja kerätään muualta kuin rekisteröidyltä itseltään (HetiL 12.1 §:n 6 kohta);
6) käsitellään vakuutustoiminnassa arkaluonteisia henkilötietoja (HetiL 12.1 §:n 11 kohta);

[225] Ks. myös II.2.2.

7) henkilötietojen käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä ja muita niihin verrattavia tehtäviä varten (HetiL 8.1 §:n 7 kohta); sekä

8) kun käsitellään henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavia yleisesti saatavilla olevia tietoja (HetiL 8.1 §:n 8 kohta). [226]

Henkilötietolain 37 § sisältää säännökset ilmoituksen tekemisestä ja sisällöstä. Tietosuojavaltuutettu ei tee ilmoituksista päätöksiä, eikä ilmoituksen vastaanottaminen merkitse rekisterinpidon hyväksymistä. Käytännössä tietosuojavaltuutettu käsittelee ilmoitukset lähettämällä ilmoituksen tekijälle viestin ilmoituksen vastaanottamisesta, ilmoittamalla tälle mahdollisista täydennystarpeista ja antamalla tarpeen mukaan ohjeistusta. Ilmoituksista valtuutetulle välittyvät tiedot palvelevat myös yleisemmin valtuutetun toiminnan ja ohjauksen suunnittelua.[227] Vireille tulleiden ja käsiteltyjen ilmoitusten vuosittaisten määrien kehitys käy ilmi seuraavasta kuvaajasta.



Kuvaaja 28: Vireille tulleiden ilmoitusasioiden määrä 1987–1990 ja 1993–2013 sekä käsiteltyjen ilmoitusasioiden määrä 1994–2013.[228]

Kuten kuvaajasta on havaittavissa, sekä henkilörekisterilain että henkilötietolain voimaantulojen myötä ilmoitusmäärä nousi hetkellisesti korkeaksi. Henkilörekisterilakia säädettäessä arvioitiin lain voimaantulon myötä kertaluonteisesti saapuvien ilmoitusasioiden määräksi noin 250, minkä lisäksi odotettiin vuosittain saapuvaksi noin 200 ilmoitusta.[229] Taso kuitenkin vakiintui ennakoitua alemmaksi: vuoden 1988 loppuun mennessä

[226] Rekisterinpitäjille säädetty ilmoitusvelvollisuus laajeni, Tietosuoja 2/1999 s. 25–27, 30. Ks. myös TSV:n toimisto, Henkilötietolain mukainen ilmoitusvelvollisuus (2010).
[227] Rekisterinpitäjille säädetty ilmoitusvelvollisuus laajeni, Tietosuoja 2/1999 s. 29 ja TSV:n toimisto, Henkilötietolain mukainen ilmoitusvelvollisuus (2010) s. 10.
[228] Tiedot perustuvat tietosuojavaltuutetun toimintakertomuksiin. Vuosien 1991 ja 1992 toimintakertomuksia ei ollut käytettävissä tätä tutkimusta varten.
[229] HE 49/1986 vp s. 18.

tietosuojavaltuutetun toimistoon oli saapunut 239 ilmoitusta, ja 90–luvulla vireille tuli vain noin 50 ilmoitusasiaa vuodessa. Vuonna 1988 tuli vireille myöhempiin vuosiin verrattuna suuri määrä perimistoimintaan ja tietojenkäsittelytehtävien hoitamiseen liittyviä ilmoituksia. 90–luvulla suurimman ilmoitusasioiden ryhmän muodostivat henkilötietojen luovuttamista ulkomaille koskeneet ilmoitukset, joita oli vuosina 1993–1997 noin 58 prosenttia kaikista ilmoitusasioista.

Henkilötietolain siirtymävaiheen huippuvuosien jälkeen ilmoitusten kokonaismäärä vakiintui noin 200 ilmoituksen vuositasolle. 2010–luvulla määrä on kuitenkin kasvanut ripeästi, ja vuonna 2013 vireille tuli jo 523 ilmoitusta. Henkilötietolain aikana suurimmiksi ilmoitusten ryhmiksi ovat nousseet ilmoitukset tietojenkäsittelypalveluiden ostamisesta[230] ja hoitamisesta. Näiden ilmoitusten määrä on myös ollut viime vuosina selvässä kasvussa: ostamisesta tehtiin vuonna 2004 31, vuonna 2008 91, vuonna 2012 181 ilmoitusta ja viimeksi vuonna 2013 164 ilmoitusta. Tietojenkäsittelypalveluiden hoitamisesta tehtiin toimintailmoituksia näinä vuosina 11, 18, 97 ja 83. Tietojenkäsittelypalveluita siis ulkoistetaan aiempaa useammin, mikä näkyy loogisesti myös palvelutarjontaa kuvaavien toimintailmoitusten määrän kasvuna. 2010–luvun ilmoitusmäärän kasvu onkin kohdistunut erityisesti näihin asiaryhmiin.

Ilmoitusasioiden käsittelyyn on vuosina 2004–2013 kulunut keskimäärin jonkin verran yli puoli henkilötyövuotta ja yli 42 000 euroa vuodessa. Prosentuaalisen kustannusosuuden vaihteluväli on ollut vajaasta kahdesta jopa viiteen prosenttiin. Vuonna 2013 ilmoitusasioiden käsittelyyn käytettiin 0,88 henkilötyövuotta ja 50 181 euroa. Nämä luvut ovat noin kaksi kertaa suurempia kuin vuonna 2004.[231] Resurssienkin osalta ennakkovalvonnan trendi on siten ollut vahvasti nouseva.

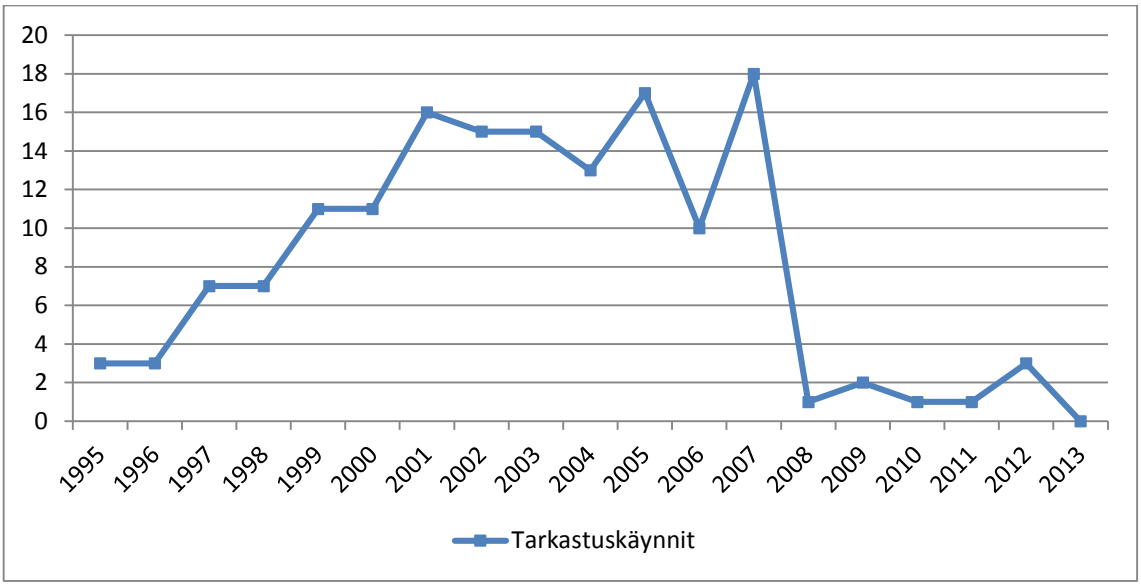
6.2 Tarkastustoiminta

Henkilötietolain aikana myös tietojen käsittelystä historiallista tai tieteellistä tutkimusten varten on tehty runsaasti ilmoituksia, välillä 2004–2012 keskimäärin vajaat 50 vuodessa ja vuonna 2013 huomattavasti tätä enemmän, 141. Seuraavaksi suurin ryhmä ovat olleet suoramarkkinointia koskevat ilmoitukset, joita on ollut noin puolet vähemmän. Samalla aikavälillä tietojen luovuttamisesta ulkomaille on tehty huomattavasti vähemmän ilmoituksia kuin vanhan laajemman velvollisuuden ollessa voimassa, keskimäärin alle kymmenen vuodessa.

Rekisterinpitäjien tiloihin kohdistuvilla tarkastuskäynneillä tietosuojavaltuutettu toteuttaa lähinnä jälkikäteisvalvontaa, joskin tarkastuksilla voidaan myös suunnata rekisterinpitäjien

[230] Toisin sanoen tietojenkäsittelypalvelujen ulkoistamisesta HetiL 8.1 §:n 7 kohtaan perustuen.
[231] Ennakkovalvonnan huippuvuosi resurssien valossa on kuitenkin ollut 2010 (1,1 htv, 79 196 euroa eli 5,0 % kaikista kustannuksista).

huomiota hyvään rekisteritapaan ennakoivasti.[232] Tietosuojavaltuutetun tarkastusoikeutta koskee henkilötietolain 39 §, joka antaa valtuutetulle laajan, salassapitosäännökset ohittavan tiedonsaantioikeuden (1 momentti). Pykälän 2 momentin mukaan tietosuojavaltuutetulla on oikeus tarkastaa henkilörekistereitä ja käyttää tarkastuksessa asiantuntijoita. Valtuutetulla ja tämän käyttämällä asiantuntijalla on oikeus päästä sellaisiin rekisterinpitäjän ja hänen toimeksiannostaan toimivan hallussa oleviin huoneistoihin, joissa henkilötietoja käsitellään tai henkilörekistereitä pidetään, sekä saada käytettäväkseen tarkastuksen toimittamisessa tarvittavat tiedot ja laitteet. Tarkastuksen toimittaminen kotirauhan piiriin kuuluvassa tilassa edellyttää kuitenkin syytä epäillä henkilötietojen käsittelyä koskevien säännösten jo tapahtunutta tai tulevaa rikkomista. Momentissa säädetään lisäksi, että tarkastus on toimitettava niin, että siitä ei aiheudu rekisterinpitäjälle tarpeettomasti haittaa ja kustannuksia.



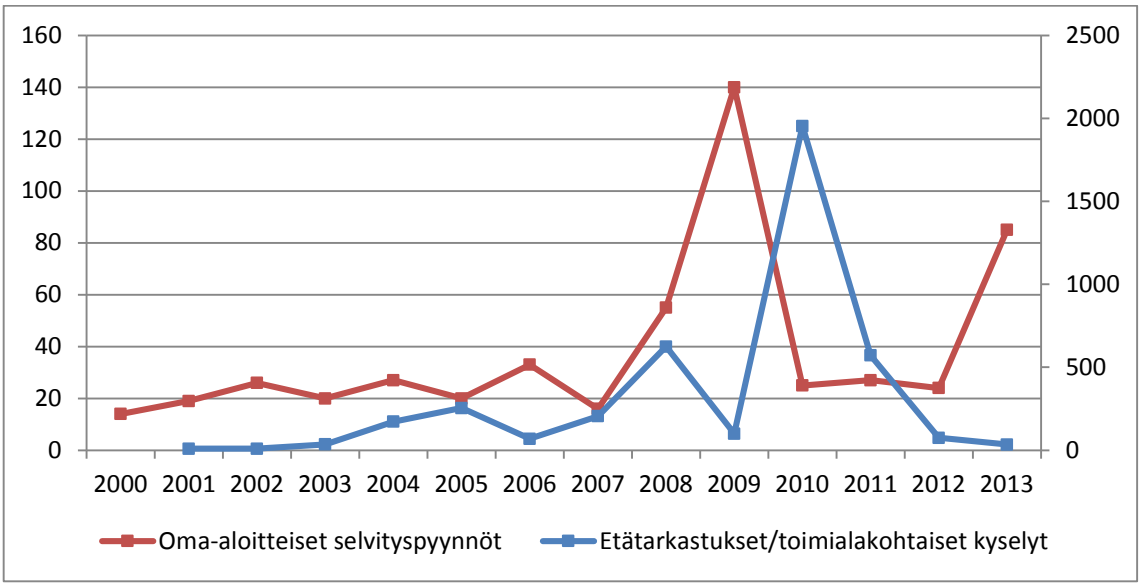
Kuvaaja 29: Rekisterinpitäjien luokse tehdyt tarkastuskäynnit 1995–2013.

Etenkin tarkastustoiminta on kärsinyt resurssien vähäisyydestä, ja se on usein ollut se toiminnan lohko, josta on resurssien puutteessa tingitty.[233] Henkilörekisterilakia säädettäessä ennakoitiin jopa viittäkymmentä vuosittaista tarkastusta, mutta tarkastuskäyntien toteutunut määrä on ollut yleensä pieni, keskimäärin alle kymmenen vuodessa välillä 1995–2013.[234] Tarkastuskäyntien määrän nostaminen oli jo 1990–luvulla pitkään tavoitteena, ja 2000–luvun taitteesta aina vuoteen 2007 saakka tarkastuskäyntejä tehtiinkin jonkin verran enemmän, enimmillään 18 kappaletta vuonna 2007. Vuodesta 2008 lähtien tarkastuksia on tehty vain muutamia, vuonna 2013 ei yhtään.

Varsinaisten tarkastuskäyntien sijaan tietosuojavaltuutetun toimisto on viime vuosina keskittynyt ns. etätarkastuksiin, jotka toteutetaan sähköisesti. Niissä lähetetään tiedustelu

[232] TK 1998 s. 8.
[233] Esim. TK 1989–1990 s. 6, TK 1993 s. 8, TK 1996 s. 6 ja TK 1997 s. 6.
[234] Ks. HE 49/1986 vp s. 18.

tyypillisesti suurelle joukolle tietyn alan rekisterinpitäjiä. Usein kyse on toimialakohtaisista kyselyistä tai muuten suurelle rekisterinpitäjien joukolle lähetettävistä selvityspyynnöistä. Näiden asioiden diariointi on ollut vaihtelevaa. Yleensä kutakin eri taholle lähetettyä kyselyä ei ole kirjattu omaksi erilliseksi asiakseen, mutta tietyissä tapauksissa jokainen lähetetty kysely on kirjattu erilliseksi oma–aloitteiseksi selvityspyynnöksi.[235] Oma–aloitteisilla selvityspyynnöillä taas viitataan yleensä asioihin, joissa lehdistöstä tai muulla vastaavalla tavalla on tullut tietoon selvitystä edellyttävä tapaus, jota tietosuojavaltuutettu on ryhtynyt selvittämään.[236] Etätarkastusasioiden ja oma–aloitteisten selvityspyyntöjen määrien kehitys käy ilmi seuraavasta kuvaajasta.



Kuvaaja 30: Vireille tulleet tietosuojavaltuutetun oma–aloitteiset selvityspyynnöt 2000–2013 (vasen asteikko) ja etätarkastukset/toimialakohtaiset kyselyt 2001–2013 (oikea asteikko).

Erilaisten tarkastusten ja selvitysten vaihteleva diariointi ja tilastointi selittänee myös kuvaajassa ilmenevän oma–aloitteisten selvityspyyntöjen vuoden 2009 piikin.[237] Tilastoista huolimatta selvää on, että tarkastustoiminnan painopistettä on 2000–luvulla ja erityisesti vuoden 2007 jälkeen

[235] Oma–aloitteisista selvityspyynnöistä vrt. II.2.3.4.
[236] Esim. TK 2005 s. 17.
[237] Vuosien 2009–2012 toimintakertomuksissa Tarkastustoiminta–otsikon alla olevissa taulukoissa, joihin yllä oleva kuvaaja perustuu, on ilmoitettu vuoden 2009 oma–aloitteisten selvityspyyntöjen lukumääräksi 140 ja etätarkastusten lukumääräksi 100. Molempiin kategorioihin on ilmeisesti tilastoitu markkina– ja mielipidetutkimusten tekemistä koskenut toimialaselvitys, joka lähetettiin 100 taholle ja kirjattiin erillisinä asioina tietosuojavaltuutetun vireille panemien asioiden diaarikategoriaan (tunnus 44). Toimintakertomuksessa ei mainita vuonna 2009 suoritetun muita etätarkastuksia tai toimialakyselyitä. Diaarikategoriassa 44 vireille tulleiden asioiden kokonaismäärä on toimintatilastojen mukaan 140. Oma–aloitteisten selvityspyyntöjen vertailukelpoinen lukema vuonna 2009 on siis ilmeisesti ollut 40 tai alle, ja etätarkastusten vertailukelpoinen lukema ilmoitettu 100. Tämän puolesta puhuu myös, että vuonna 2005 samaan diaarin kategoriaan 44 kirjatut selvitykset teleyritysten ja puhelinluettelo–, tilaajaluettelo– ja numerotiedotuspalvelua tarjoavien yritysten ilmoittamis– ja huolehtimisvelvollisuuden hoitamisesta (143 kohdetta) ja henkilöarviointia suorittavien yritysten tietoisuutta henkilötietojen suojaan liittyvistä velvoitteista (89 kohdetta) on vuosien 2005–2010 toimintakertomusten Tarkastustoiminta–otsikon alaisissa taulukoissa siirretty etätarkastukset–kategorian lukuihin. Muita vastaavia laajoja toimialaselvityksiä ei ole kirjattu erillisinä asioina diaarikategoriaan 44.

siirretty suurelta osin massaluonteisiin, usein satoihin rekisterinpitäjiin kohdistuviin etätarkastuksiin.[238] Perinteisten tarkastuskäyntien suorittaminen yhtä laajaan rekisterinpitäjien joukkoon kohdistuen ei nykyisellä resurssitasolla – tai edes huomattavalla resurssien lisäyksellä – olisi mahdollista. Perinteisten tarkastuskäyntien lukumäärää ei siten tulisikaan nähdä tarkastustoiminnan kannalta keskeisenä indikaattorina, etenkin kun tarkastuskäyntien tehokkuus yksittäisenkin rekisterinpitäjän osalta riippuu suuresti tarkastuksen toteuttamistavasta. Myös tarkastustoimintaa arvioitaessa huomio tulisi kiinnittää ensisijaisesti siihen, mikä vaikutus toiminnalla käytännössä on rekisterinpitäjiin ja rekisterinpitoon. Tämän tutkimuksen puitteissa perinteisten tarkastuskäyntien ja erilaisten etätarkastusten vaikuttavuutta ei ole ollut mahdollista tarkemmin selvittää ja vertailla. On silti ehdottomasti positiivista, että tietosuojavaltuutetun toimistossa on viime vuosina pyritty löytämään uudenlaisia toimintamalleja tulosten saavuttamiseksi selvästi ongelmalliseksi osoittautuneella toimintalohkolla.

Vaikka tarkastustoiminta eri muodoissaan on 2000–luvulla jonkin verran aktivoitunut 1990–luvun alun ja puolenvälin tasosta, tarkastustoimintaan käytettyjen resurssien määrä on ollut pieni: välillä 2004–2013 keskimäärin alle puoli henkilötyövuotta ja hieman yli 27 000 euroa vuotta kohden. Rahallisesti tarkastustoimintaan panostettiin vuosina 2008–2012 lähes yhtä paljon kuin vuosina 2004–2007, jolloin varsinaisia tarkastuksia tehtiin huomattavasti enemmän. Resursseja siis siirrettiin etätarkastuksiin, ei juurikaan vähennetty. Vuonna 2013 tarkastustoimintaan käytettiin kuitenkin vain 9 682 euroa.

6.3 Lainsäädännön kehittäminen

Henkilötietolain 41.1 §:n mukaan asianomaisen viranomaisen on varattava tietosuojavaltuutetulle tilaisuus tulla kuulluksi valmisteltaessa lainsäädännöllisiä tai hallinnollisia uudistuksia, jotka koskevat henkilöiden oikeuksien ja vapauksien suojaamista henkilötietojen käsittelyssä.[239] Tällaista nimenomaista kuulemisvaatimusta ei sisältynyt henkilörekisterilakiin, vaan se otettiin lakitekstiin henkilötietodirektiivin 28 artiklan 2 kohdan vuoksi. Tietosuojavaltuutettua oli kuitenkin ollut tapana kuulla henkilötietojen suojaan liittyvää lainsäädäntöä valmisteltaessa ilman nimenomaista säännöstäkin.[240] Osallistumalla uudistusten valmisteluun tietosuojavaltuutetulla on mahdollisuus vaikuttaa lainsäädännön

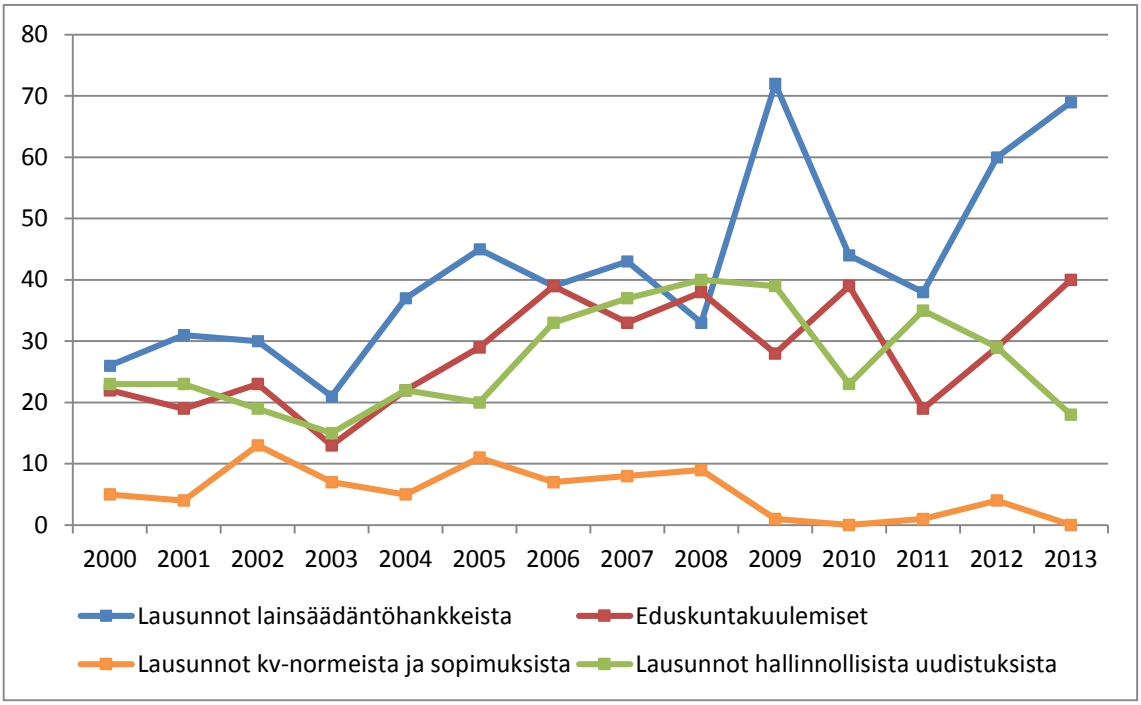
[238] Kohdemäärältään suurin tarkastus on ollut yhteensä noin 1700:lle terveydenhuollon palveluntarjoajalle ja apteekille vuonna 2010 lähetetty, verkossa täytettävän lomakkeen muodossa toteutettu kysely. Kyselyllä selvitettiin, miten kohdeorganisaatiot huolehtivat tietosuoja– ja tietoturva–asioista. Vastaukset saatiin noin 60 prosentilta kohteista. Ks. TK 2010 s. 12.

[239] Säännöksen perusteluiden mukaan hallinnollisilla uudistuksilla tarkoitetaan esimerkiksi sellaisia viranomaisten organisaatiorakenteisiin liittyviä uudelleenjärjestelyjä, joilla on vaikutusta henkilörekisterien pitoon. HE 96/1998 vp s. 73.

[240] HE 96/1998 vp s. 73. Mainitun direktiivin säännöksen mukaan kunkin jäsenvaltion on säädettävä siitä, että valvontaviranomaisia kuullaan henkilöiden oikeuksien ja vapauksien suojaamista henkilötietojen käsittelyssä koskevia lainsäädännöllisiä ja hallinnollisia toimenpiteitä suunniteltaessa.

kehittämiseen henkilötietojen suojaa kunnioittavaan suuntaan. Lainsäädännön kehittäminen voidaankin lukea tietosuojavaltuutetun ennaltaehkäisevään toimintaan.

Tietosuojavaltuutettu antaa vuosittain merkittävän määrän lausuntoja lainsäädännöllisistä ja hallinnollisista uudistuksista. Lisäksi tietosuojavaltuutettu antaa joitakin lausuntoja kansainvälisistä normeista ja sopimuksista. Kirjallisten lausuntojen lisäksi tietosuojavaltuutettua myös kuullaan säännöllisesti eduskunnassa. Seuraava kuvaaja esittää lausunto– ja kuulemisasioiden määrän kehityksen 2000–luvulla.



Kuvaaja 31: Yleisissä asioissa annetut lausunnot ja eduskuntakuulemiset 2000–2013.

Tietosuojavaltuutetun lainsäädäntöhankkeista antamien lausuntojen määrä on ollut jonkin verran nousujohteinen, joskin kehitys on ollut epätasaista. Keskimäärin 2000–luvulla tietosuojavaltuutettu on antanut nelisenkymmentä lausuntoa lainsäädäntöhankkeista vuodessa. Vähimmillään lausuntoja on annettu vuodessa 21 (1993), enimmillään 72 (2009). Vuonna 2013 lausuntoja annettiin 69. Eduskuntakuulemisten ja hallinnollisista uudistuksista annettujen lausuntojen määrä on pysynyt koko 2000–luvun muutaman kymmenen asian tasolla. Keskimäärin molempia asioita on ollut vuodessa vajaat kolmekymmentä. Ehkäpä hieman yllättäen lausuntoja kansainvälisistä normeista ja sopimuksista on annettu viime vuosina hyvin vähän, 2013 ei yhtäkään.[241]

Lainsäädännön kehittämiseen liittyen tietosuojavaltuutetulla on myös mahdollisuus tehdä tarpeellisiksi katsomiaan aloitteita (TSL–TSVL 5 § 2 kohta). Lausuntojen, kuulemisten ja aloitteiden lisäksi tietosuojavaltuutettu vaikuttaa lainsäädännön kehittämiseen osallistumalla

[241] 1990–luvulla yleisistä asioista annettiin vuositasolla vajaat viitisenkymmentä lausuntoa. Lausunnot koskivat toimintakertomusten mukaan lähinnä lainsäädäntöhankkeita.

erilaisiin uutta lainsäädäntöä käsitteleviin työryhmiin, jotka toimivat eri hallinnonaloilla. Tällaisia virallisluontoisia työryhmiä, joissa tietosuojavaltuutetun toimistolla on ollut edustaja, on ollut toiminnassa vuosittain noin kaksikymmentä. Lisäksi tietosuojavaltuutettu ja toimiston edustajat ovat osallistuneet erilaisten epävirallisempien ryhmien toimintaan.[242]

Vuosina 2004–2013 lainsäädännön kehittämistyöhön sen eri muodoissa on käytetty vähimmillään alle puoli henkilötyövuotta, enimmillään noin yksi henkilötyövuosi. Rahaa toimintaan on käytetty keskimäärin noin 50 000 euroa eli jonkin verran yli kolme prosenttia toimiston kaikista menoista. Resurssien käytön trendi on ollut laskeva vuoden 2006 jälkeen.

6.4 Tietopalvelu

Kuten tietosuojavaltuutetun toimintakertomuksissa toistuvasti on todettu, edustavat kirjallisesti vireille tulleet asiat vain osaa tietosuojavaltuutetun toimiston tehtävistä. Toimisto antaa ohjausta ja neuvontaa myös puhelimitse, mikä muodostaa ns. tietopalvelun keskeisimmän osan. Myös puhelimitse annettava neuvonta voidaan lukea tietosuojavaltuutetun toimiston ennaltaehkäisevään toimintaan.

Puhelimitse tietosuojavaltuutetun toimistoon tulleiden yhteydenottojen määrän kuvattiin toiminnan alkuvuosina olleen moninkertainen kirjallisesti vireille tulleiden asioiden määrään verrattuna. 2000–luvun toimintakertomusten vakiofraasien mukaan puheluiden vuosittaiseksi lukumääräksi on arvioitu noin 7 500, ja puhelinneuvontaan on osallistunut kerralla kaksi työntekijää. Valitettavasti puhelujen todellista määrää ja laatua ei ole tilastoitu. Toimintakertomusten lukemassa on kyse vastatuista puheluista, joten arvioidun määrän pysyminen vakiona kertoo vain puhelinneuvonnan tarjonnan säilyneen samana, eikä se näin ollen kerro mitään puhelinneuvonnan kysynnän kehityksestä. Myös tietopalvelun resursseja koskevien tilastojen perusteella voidaan havaita, ettei suuria muutoksia puhelinneuvonnan määrässä ole tapahtunut. Keskimäärin tietopalveluun on käytetty vajaat puolitoista henkilötyövuotta ja hieman yli 75 000 euroa vuodessa. Kaikista toimiston menoista tämä on vastannut kolmesta kuuteen prosenttia.

Sen enempää puhelumäärät kuin resurssitilastot eivät kerro mitään puhelinpalvelun tehokkuuden kehityksestä. Puhelinneuvonnan yhtenä tavoitteena on ollut ehkäistä tarpeettomia asioiden vireillepanoja. Ajatuksena on ollut, että puhelinneuvoja voi antaa soittajalle välittömästi informaatiota selvissä asioissa esimerkiksi aiemmin ratkaistujen samantyyppisten tapausten perusteella. Tämä asettaa vaatimuksia sekä puhelinneuvontaa antavan työntekijän asiantuntemukselle että toisaalta toimistossa käytettäville asian– ja tiedonhallintajärjestelmille. Ihanteellisessa tilanteessa puhelinneuvontaa antaa juuri soittajan ongelmaan tai tämän edustaman alan tietosuojakysymyksiin hyvin perehtynyt, kokenut asiantuntija, joka pystyy

[242] Esim. TK 2006 s. 14, TK 2010 s. 11 ja TK 2012 s. 11.

tunnistamaan olennaisen soveltamisongelman ja antamaan soittajan tarvitsemat tiedot välittömästi. Vähintäänkin neuvojan on kyettävä tunnistamaan ongelma ja selvittämään, onko vastaava kysymys jo joskus ratkaistu. Tällöin tiedon aiemmista ratkaisuista tulisi olla helposti etsittävissä ja nopeasti saatavilla, jotta tämä tieto voidaan välittää soittajalle.

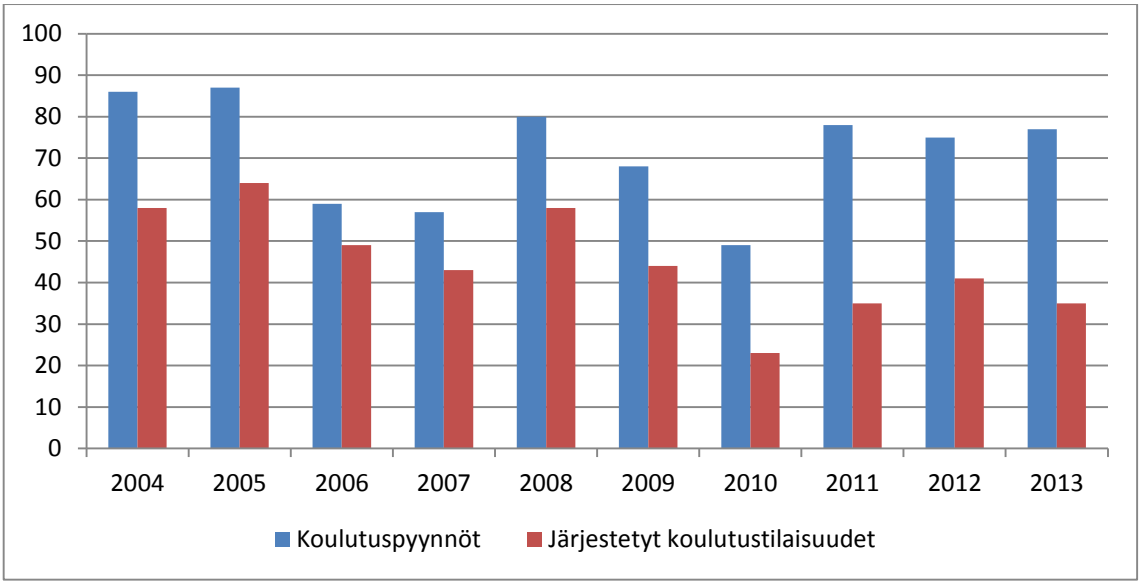
Kun puhelinneuvonnassa on käytetty esimerkiksi paljon harjoittelijoita ja toimiston tiedonhallintajärjestelmien kehittäminen on ajoittain laiminlyöty,[243] voidaan puhelinneuvonnan tehokkuudessa epäillä olleen tässä suhteessa toivomisen varaa. Sillä lienee silti ollut jonkin suuruinen vireillepanojen määrää alentava vaikutus. Puhelinneuvontaa seuraavien vireillepanojen määrää ei kuitenkaan ole mitenkään tilastoitu, eikä mitään varmaa tietoa puhelinneuvonnan vaikutuksesta kirjallisten vireillepanojen määrään muutenkaan ole. Tietopalvelun ja siihen liittyen puhelinneuvonnan merkitykseen ja järjestämiseen on kuitenkin toimistossa viime aikoina kiinnitetty huomiota, ja toimistoon on hiljattain perustettu uusi nimenomainen tietopalveluyksikkö, jonka toimintaa pyritään edelleen kehittämään.[244]

6.5 Koulutustoiminta

Tietosuojavaltuutetun toimiston ennaltaehkäisevään toimintaan kuuluu myös koulutustoiminta. Kouluttamalla rekisteritoiminnan parissa työskenteleviä tietosuojavaltuutetun toimisto toteuttaa neuvonta– ja ohjausvelvollisuuttaan. Toisaalta koulutustoiminta on läheisessä kytköksessä sidosryhmien kanssa tehtävän yhteistyön kanssa. Toimisto järjestää koulutus– ja luentotilaisuuksia ja osallistuu sidosryhmien seminaareihin. Osa koulutuksesta järjestetään maksutta, mutta vuodesta 2003 lähtien toimisto on järjestänyt myös maksullista koulutusta. Tietosuojavaltuutetun toimisto on pyrkinyt toteuttamaan koulutusta kysynnän mukaan, mutta myös vaikuttavuuden huomioiden.[245] Koulutusta on järjestetty resurssien puitteissa, ja koulutuspyyntöjä onkin saapunut enemmän kuin koulutustilaisuuksia on pystytty järjestämään.

Keskimäärin välillä 2004–2013 koulutustilaisuuksia on järjestetty vuodessa noin 45 kappaletta. Pyyntöjä on saapunut keskimäärin noin 70, eli yli 50 prosenttia enemmän kuin tilaisuuksia on kyetty järjestämään. Vireille tulleiden koulutuspyyntöjen määrä ilmenee seuraavasta kuvaajasta.

[243] Omien järjestelmien kehittämisen laiminlyöntiin yhtenä syynä oli valtion dokumentinhallintaa yhtenäistämään pyrkinyt, epäonnistunut VALDA–hanke (2006–2012), jonka valtiovarainministeriö päätti lopettaa pitkän ja kalliiksi käyneen kehitystyön jälkeen.
[244] Tietosuojavaltuutettu Reijo Aarnion haastattelu, 5.5.2014, Helsinki.
[245] Esim. TK 2012 s. 9.



Kuvaaja 32: Vireille tullet koulutuspyynnöt ja järjestetyt koulutustilaisuudet 2004–2013.

Maksulliseen ja maksuttomaan koulutustoimintaan yhteensä on kulunut keskimäärin noin puoli henkilötyövuotta, ja kustannuksia toiminta on aiheuttanut noin 38 000 euroa vuotta kohden. Maksullisista koulutustilaisuuksista tietosuojavaltuutetun toimisto on saanut tuloja keskimäärin noin 26 000 euroa vuodessa[246], eli nämä tulot eivät ole riittäneet kattamaan koulutustoiminnan kustannuksia. Varsin maltillisiksi asetetut koulutustoiminnan tulostavoitteet on kuitenkin yleensä ylitetty.[247]

III Tietosuojalautakunta

1. Yleistä tietosuojalautakunnasta

1.1 Kokoonpano ja päätöksenteko

Tietosuojalautakunnan kokoonpanona on ollut alusta alkaen puheenjohtaja, varapuheenjohtaja ja viisi jäsentä. Heillä kaikilla on henkilökohtaiset varajäsenet. Valtioneuvosto määrää jäsenet kolmeksi vuodeksi kerrallaan ja he toimivat tehtävissään sivutoimisesti. Kaikilta jäseniltä edellytetään rekisteritoiminnan tuntemusta. Puheenjohtajalta, varapuheenjohtajalta ja yhdeltä jäseneltä sekä tämän varajäseneltä edellytetään oikeustieteen kandidaatin (tai maisterin) tutkintoa. Vuoden 1987 laissa kahdelta jäseneltä ja heidän varajäseniltään edellytettiin hyvää tietotekniikan asiantuntemusta (TSL–TSVL–1987 2 §). Vuonna 1994 kokoonpanoa ja kelpoisuusvaatimuksia koskeva sääntely siirrettiin uuden tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun asetuksen 1 §:ään, ja samalla muutettiin tietotekniikan

[246] Luku ei sisällä arvonlisäveron osuutta.
[247] Kansainvälisestä koulutustoiminnasta ks. II.5.3.

asiantuntemusta koskeva vaatimus muotoon, jonka mukaan lautakunnassa on *oltava edustettuna* hyvä tietotekniikan asiantuntemus. Pykälää ei ole tämän jälkeen muutettu.

Sivutoimisten jäsenten lisäksi lautakunnalla voi TSL–TSVA 2 §:n (266/2001) mukaan olla päätoiminen sihteeri ja tarpeellinen määrä sivutoimisia sihteereitä. Saman pykälän mukaan sihteerillä tulee olla oikeustieteen kandidaatin tutkinto.[248] Pykälän aiemman sanamuodon ja pykälää edeltäneen TSL–TSVL–1987 2.3 §:n mukaan lautakunnalla ei pelkästään voinut olla vaan *oli* päätoiminen sihteeri.

Lautakunta kokoontuu tarpeen mukaan puheenjohtajan tai varapuheenjohtajan kutsumana. Päätösvaltainen lautakunta on, kun läsnä on kokouksen puheenjohtaja ja vähintään kolme muuta jäsentä. Päätökset tehdään sihteerin esittelystä yksinkertaisella enemmistöllä. Tasatilanteessa kokouksen puheenjohtajan ääni ratkaisee (TSL–TSVA 3–4 §).[249]

Tietosuojalautakunta voi kuulla asiantuntijoita ja pyytää näiltä lausuntoja (TSL–TSVL 7 §). Alun perin lautakunnan tehtävien ajateltiin edellyttävän oikeudellisen asiantuntemuksen ohella varsin paljon myös teknistä ymmärrystä, mihin pyrittiin varautumaan myös kahdelta jäseneltä edellytetyllä hyvällä tietotekniikan asiantuntemuksella. Lautakunnan päätöksenteko on osoittautunut kuitenkin luonteeltaan valtaosin oikeudelliseksi, ja lautakunta on käyttänyt mahdollisuuttaan asiantuntijoiden kuulemiseen erittäin säästeliäästi. Oikeudellista päätöksenteko on ollut myös siinä mielessä, ettei lautakunta myöskään ole juurikaan selvittänyt tosiasiakysymyksiä asianosaisten suullisten kuulemisten avulla.[250]

1.2 Jäsenet

Tietosuojalautakunnan puheenjohtajana on toiminut alusta alkaen *Pekka Nurmi*, joka työskenteli pitkään myös oikeusministeriön lainsäädäntöosaston osastopäällikkönä.[251] Kahden ensimmäisen kauden ajan (1988–1993) varapuheenjohtajana toiminutta valtiovarainministeriön *Pekka Ojalaa* lukuun ottamatta varapuheenjohtajat ovat tulleet yliopistomaailmasta.[252] Vuosina 1994–2005 varapuheenjohtajana toimi professori *Timo Konstari* Helsingin yliopistosta ja vuodesta 2006 eteenpäin professori *Ahti Saarenpää* Lapin yliopistosta. Puheenjohtajiston ohella myös useat lautakunnan jäsenistä ovat toimineet

[248] Ennen vuoden 2001 muutosta vain päätoimiselta sihteeriltä vaadittiin oikeustieteen kandidaatin tutkintoa (silloinen TSL–TSVA 6.2 §). Alun perin sihteeriltä edellytettiin TSL–TSVA–1987 6.2 §:n mukaan vain ”virkaan soveltuvaa ylempää korkeakoulututkintoa”.
[249] Vuoden 1987 asetuksen 11 §:n mukaan lautakuntaan sovellettiin täydentävästi valtion komiteoista annettuja määräyksiä. Näiden katsottiin soveltuvan huonosti tietosuojalautakunnan kaltaiseen pysyvään elimeen. Vuoden 1994 uudistuksessa tämä säännös poistettiin. *Wallin – Nurmi*, Tietosuojalainsäädäntö (1991) s. 163.
[250] Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki ja *Wallin – Nurmi*, Tietosuojalainsäädäntö (1991) s. 163.
[251] OM:stä Nurmi jäi eläkkeelle 1.11.2013, mutta hän jatkaa tietosuojalautakunnan puheenjohtajana vuoden 2014 loppuun.
[252] Ojala aloitti varapuheenjohtajana vasta 4.2.1988. Ensimmäinen varapuheenjohtaja oli reilun kuukauden ajan (1.1.–3.2.1988) professori Pirkko K. Koskinen, joka siirtyi eduskunnan apulaisoikeusasiamieheksi.

tehtävissään lukuisia toimikausia, mutta yli 25 vuoden toiminnan aikana lautakunnan kokoonpanossa on luonnollisesti ollut myös vaihtuvuutta. Nykyisen lautakunnan (toimikausi 1.1.2012 – 31.12.2014) varsinaisista jäsenistä vain yksi on lautakunnassa ensimmäistä kauttaan, ja hänkin on lautakunnan pitkäaikainen varajäsen.[253]

Lautakunnan puheenjohtaja on siis koko ajan pysynyt samana ja ollut päätoimenaan oikeusministeriön palveluksessa. Lautakunnan muut jäsenet ovat päätoimenaan työskennelleet ministeriöiden, yliopistojen, kaupunkien, sairaanhoitopiirien, työmarkkinajärjestöjen sekä muiden järjestöjen ja yksityisten yritysten palveluksessa. Jäsenet ovat siis tuoneet mukanaan varsin laajaa ja erilaista yhteiskunnallista kokemusta ja osaamista, minkä voi katsoa myös tukevan lautakunnan itsenäisyyttä. Lautakunnan läheistä tosiasiallista kytköstä oikeusministeriöön ei tosin ole syytä kieltää, mutta tämä ei näytä aiheuttaneen ainakaan suuria ongelmia lautakunnan päätöksentekokyvylle tai arvovallalle.

Valtioneuvosto nimittää tietosuojalautakunnan, mutta ehdotukset kokoonpanosta valmistellaan ja tehdään oikeusministeriön hallintoyksikössä. Jäseniä valittaessa hallintoyksikkö on käytännössä tiiviissä yhteistyössä ja keskusteluyhteydessä lautakunnan ja etenkin sen puheenjohtajan sekä tarpeen mukaan muidenkin tahojen kanssa. Huomiota kiinnitetään sekä potentiaalisten jäsenten henkilökohtaisiin ominaisuuksiin ja pätevyyteen että eri taustaorganisaatioiden ja alojen tasapainoon, vaikka jäsenet eivät varsinaisesti edusta taustaorganisaatioitaan tai niiden intressejä lautakunnassa toimiessaan.[254]

Lautakunnan kokoonpanossa ei ole tapahtunut kerralla radikaaleja muutoksia, mutta uusia kokoonpanoesityksiä valmisteltaessa voidaan luonnollisesti tarpeen mukaan huomioida esimerkiksi teknisen kehityksen tuomia uusia painotuksia ja tarpeita. Näin on tehtykin: viimeisimmän lautakunnan kokoonpanossa tämä ilmenee esimerkiksi siten, että toisin kuin aiemmin, lautakunnassa on – joskin varajäsenenä – myös liikenne– ja viestintäministeriössä työskentelevä henkilö. Liikenne– ja viestintäministeriön hallinnonalan merkitys tietosuojakysymyksissä on korostunut viime vuosina, joten lautakuntaan haluttiin näkemystä myös tältä alalta.[255]

1.3 Resurssit

Koska kyse on sivutoimisesta, palkkioperusteisesta ja tarpeen mukaan kokoontuvasta elimestä, lautakunnan toimintamenot riippuvat pitkälti kokous– ja asiamääristä. Lautakunnan asiamäärissä mitattuna vilkkaimpana vuotena eli vuonna 1993 sen menot olivat noin 400 000 mk ja vuonna 1995 vielä enemmän, noin puoli miljoonaa markkaa. Samaa luokkaa menot olivat

[253] Lautakunnan muista rivijäsenistä yksi on mukana toista kauttaan, yksi kolmattaan. Loput kaksi ovat olleet mukana jo henkilörekisterilain voimassaoloajoista saakka. Nykyisistä varajäsenistä ensikertalaisia on kolme, joista yksi on varapuheenjohtajan varajäsen.
[254] Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki.
[255] Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki.

vielä vuosituhannen vaihteessakin, vuonna 1999 408 000 mk ja vuonna 2000 480 609 mk. Sittemmin 2000–luvulla tietosuojalautakunnan vuosimenot ovat olleet noin 15 000 euron luokkaa, vuonna 2013 vain 10 121 euroa. Lautakunnan menot ovat siis laskeneet merkittävästi henkilörekisterilain voimassaoloajasta. Pudotus on rahan arvoon suhteutettuna jopa yli 80 prosenttia. Resurssien tarve on toisaalta pudonnut selvästi, koska myös asiamäärät ovat toimivallan kaventumisen seurauksena vähentyneet jäljempänä luvuissa 2 ja 3 kuvattavalla tavalla. Lautakunta myös kokoontuu aiempaa selvästi harvemmin. Henkilörekisterilain aikaan lautakunta kokoontui vuosittain jopa yli 20 kertaa, mutta vuosina 2004–2013 kokoontumisia on ollut neljästä kahdeksaan. Käsittelyajat ovatkin 2000–luvulla lautakunnassa asiamäärien laskusta huolimatta jonkin verran nousseet.[256]

2. Toimivalta ja sen muutokset

2.1 Lupatoimivalta

Henkilörekisterilain 37 § antoi tietosuojalautakunnalle mahdollisuuden myöntää poikkeuslupia. Pykälä kuului seuraavasti:

> **37 §**
>
> **Poikkeusluvat**
>
> Tietosuojalautakunta voi antaa 5, 7, 19 ja 20§:ssä taikka yleisten asiakirjain julkisuudesta annetun lain 18 a§:ssä tarkoitetun luvan taikka luvan poiketa tämän lain tai sen nojalla annetun asetuksen säännöksistä, jos tähän on painava syy ja rekisteröidyn yksityisyyden sekä hänen etujensa ja oikeuksiensa ja valtion turvallisuuden vaarantuminen voidaan estää.
>
> Lupa voidaan antaa määräajaksi tai toistaiseksi ja siihen on liitettävä rekisteröidyn yksityisyyden suojan sekä hänen etujensa ja oikeuksiensa samoin kuin valtion turvallisuuden suojaamiseksi tarpeelliset määräykset.
>
> Tietosuojalautakunta voi tietosuojavaltuutetun tai luvan saajan hakemuksesta muuttaa tai täydentää 2 momentissa tarkoitettuja määräyksiä, jos se muuttuneiden olosuhteiden vuoksi on tarpeen. Lupa voidaan peruuttaa, milloin syytä siihen harkitaan olevan.

Tietosuojalautakunnan toimivalta antaa poikkeuslupia oli siis erittäin laaja. Lautakunta saattoi antaa hakijalle luvan poiketa mistä tahansa henkilörekisterilain tai henkilörekisteriasetuksen säännöksestä. Se ei kuitenkaan voinut antaa lupaa rekisterinpitoon, joka oli muun lainsäädännön vastaista.[257] Luvananto oli myös sidottu henkilörekisterilain 37 §:ssä määriteltyihin perusteisiin, jotka olivat painavan syyn olemassaolo ja se, että rekisteröidyn yksityisyyden sekä hänen etujensa ja oikeuksiensa ja valtion turvallisuuden vaarantuminen voitiin estää.[258] Joka tapauksessa viranomaiselle annettu laaja, tarkasti määrittelemätön valta ohittaa eduskuntalain tasoisia säädöksiä oli ongelmallista EU:n henkilötietodirektiivin

[256] Tietosuojalautakunnan asiamääristä ja toimivallan muutoksista ks. III.2–3.
[257] *Konstari*, Henkilörekisterilaki (1992) s. 348–349 ja päätökset TSL 3/1990 ja TSL 4/1990.
[258] Näiden merkityksestä ks. *Konstari*, Henkilörekisterilaki (1992) s. 352–368 ja *Wallin – Nurmi*, Tietosuojalainsäädäntö (1991) s. 175–179.

(95/46/EY) ja perusoikeusuudistuksen edellyttämän lainsäädännön täsmällisyysvaatimuksen kannalta.[259]

Vuoden 1994 lainmuutoksella (387/1994, voimaan 1.7.1994) henkilörekisteriin lisättiin säännöksiä sukututkimus– ja henkilömatrikkelitoimintaan liittyvästä rekisterinpidosta ja rekisterien tietosisällöstä. Näitä aloja koskevat useat poikkeuslupahakemukset olivat työllistäneet lautakuntaa.[260] Lainmuutoksella ei supistettu lautakunnan toimivaltaa, mutta sillä poistettiin tarve poikkeusluvan hakemiselle tietyissä tapauksissa. Periaatteellisesti ja käytännössä paljon merkittävämpi muutos lautakunnan toimintaan aiheutui nykyisen henkilötietolain voimaantulon myötä 1.6.1999. Tällöin tietosuojalautakunnan toimivalta supistui merkittävästi, sillä henkilötietolaissa lupatoimivaltaa sääntelee olennaisesti aiempaa pykälää tarkkarajaisempi 43 §.

> **43 §**
>
> **Tietosuojalautakunnan lupatoimivalta**
>
> Tietosuojalautakunta voi antaa 8 §:n 1 momentin 9 kohdassa tarkoitetun luvan henkilötietojen käsittelyyn, jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi muussa kuin yksittäistapauksessa taikka yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai sivulliselle, jolle tiedot luovutetaan. Lupa voidaan myöntää myös rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun edun toteuttamiseksi edellyttäen, ettei tietojen tällainen käsittely vaaranna henkilön yksityisyyden suojaa ja oikeuksia.
>
> Tietosuojalautakunta voi antaa 12 §:n 13 kohdassa tarkoitetun luvan arkaluonteisten henkilötietojen käsittelyyn tärkeää yleistä etua koskevasta syystä.
>
> Lupa voidaan antaa määräajaksi tai toistaiseksi ja siihen on liitettävä rekisteröidyn yksityisyyden suojaamiseksi tarpeelliset määräykset. Määräyksiä voidaan tietosuojavaltuutetun tai luvan saajan hakemuksesta muuttaa tai täydentää, jos se muuttuneiden olosuhteiden vuoksi on tarpeen.

Henkilötietolain mukaan poikkeuslupia on siis mahdollista antaa vain kahdenlaisista asioista. Ensinnäkin tietosuojalautakunta voi myöntää luvan henkilötietojen käsittelyyn, kun henkilötietolain 8.1 § 1–8 kohdan vaatimukset eivät täyty, henkilötietodirektiivin 7 artiklan d ─ f alakohtia vastaavin edellytyksin. Toiseksi lautakunta voi myöntää poikkeuksen arkaluonteisten henkilötietojen käsittelykiellosta (HetiL 11 §).[261] Sen sijaan muista henkilötietolain säännöksistä lautakunta ei enää voi myöntää poikkeusta. Lautakunta on esimerkiksi toistuvasti todennut, ettei se ole toimivaltainen myöntämään lupaa henkilötunnuksen käsittelyyn, josta on tyhjentävästi määrätty henkilötietolain 13 §:ssä (ratkaisut TSL 8/2000, TSL 10/2000, TSL 2/2003, TSL 3/2006 ja TSL 5/2007).

---

[259] *Rantalankila*, Tietosuojalautakunnan toimivalta täsmentyi, Tietosuoja 2/1999 s. 38 ja *Nurmi*, Henkilötietolain linjauksia, Tietosuoja 2/1999 s. 5–6.
[260] TK 1993 s. 15 ja TK 1994 s. 16.
[261] Arkaluonteisten tietojen osalta toimivalta perustuu henkilötietodirektiivin 8 artiklan 4 kohtaan. HE 96/1998 vp s. 48, 74.

Lupamääräysten osalta henkilötietolain sääntely ei olennaisesti eroa henkilörekisterilaista. Edelleen luvat voidaan myöntää määräajaksi tai toistaiseksi, ja niihin on liitettävä rekisteröidyn yksityisyyden suojaamiseksi tarpeelliset määräykset. Määräyksiä voidaan myös jälkikäteen muuttaa ja täydentää. Luvan peruuttamisen sääntelyä tosin tarkennettiin: henkilörekisterilain 37.3 § mahdollisti peruuttamisen ”milloin syytä siihen harkitaan olevan”, kun taas henkilötietolain 44 §:n 4 kohta asettaa peruuttamisen edellytykseksi sen, ettei edellytyksiä luvan myöntämiselle enää ole tai että rekisterinpitäjä toimii luvan tai siihen liitettyjen määräysten vastaisesti.

Muina uudistuksina tietosuojalautakunta ei enää myönnä ulkomailleluovutuslupia, arkistointilupia yksityisten henkilörekisterien arkistoimiseen eikä henkilörekisteriasetuksen 5.2 § 4 kohdassa tarkoitettuja lupia maksuhäiriötietojen tallettamiseen. Ensimmäiset korvasi tietojen vapaa liikkuvuus EU/ETA–alueella sekä henkilötietolain uusi sääntely (22–23 § ja lainmuutoksella 986/2000 lisätty 22 a §), toisten osalta toimivalta siirrettiin arkistolaitokselle, ja maksuhäiriötietojen tallettamisen oikeutti henkilötietolain alkuperäinen 20.1 §:n 4 kohta.[262] Viimeksi mainittu lainkohta kumottiin luottotietolain säätämisen yhteydessä vuonna 2007, ja sääntely siirrettiin luottotietolakiin.

2.2 Määräyksenantovalta sekä tarkastusoikeus– ja virheenoikaisuasiat

Määräyksenantovallan osalta henkilötietolain tuoma muutos ei ollut yhtä suuri. Henkilötietolain 44 § vastaa sisällöllisesti henkilörekisterilain 35 §:n 2 ja 3 momentin säännöksiä. Pykälän mukaan lautakunta voi 1) kieltää henkilötietolain tai sen nojalla annettujen säännösten ja määräysten vastaisen henkilötietojen käsittelyn, 2) velvoittaa muissa kuin 40 §:n 2 momentissa tarkoitetuissa asioissa asianomaisen määräajassa oikaisemaan sen, mitä on oikeudettomasti tehty tai laiminlyöty ja 3) määrätä rekisteritoiminnan lopetettavaksi, jos lainvastaiset toimet tai laiminlyönnit huomattavasti vaarantavat rekisteröidyn yksityisyyden suojaa tai hänen etujaan tai oikeuksiaan, jollei rekisteristä ole laissa säädetty. Lisäksi pykälän 4 kohdassa säädetään luvan peruuttamisesta edellä mainitulla tavalla aiemmasta poikkeavasti. Antamansa määräyksen tehosteeksi – tai asian käsittelemiseksi tarvitsemiensa tietojen saamiseksi – lautakunta voi henkilötietolain 46 §:n mukaan asettaa uhkasakon.

Henkilörekisterilain 35.1 §:n mukaan rekisterinpitäjä saattoi vastustaa tietosuojavaltuutetun tarkastusoikeuden toteuttamista tai virheen oikaisua koskevaa määräystä, jolloin määräys raukesi ja asia oli saatettavissa tietosuojalautakunnan käsiteltäväksi. Henkilötietolain myötä sitova päätösvalta tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa siirrettiin tietosuojavaltuutetulle, ja tietosuojavaltuutetun näissä asioissa tekemät päätökset

[262] *Rantalankila*, Tietosuojalautakunnan toimivalta täsmentyi, Tietosuoja 2/1999 s. 40–41.

ovat nyt valituskelpoisia hallintolainkäyttölain mukaisesti (HetiL 40.2 § ja 45.1 §). Näin ollen tietosuojalautakuntaan ei enää tule käsiteltäväksi asioita suoraan rekisteröidyn aloitteesta.[263]

2.3 Periaatteellisesti tärkeät kysymykset

Vuoden 1987 tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain 3 §:n ja sitä täydentäneen asetuksen 1.2 §:n mukaan tietosuojalautakunnan tehtäviin kuului käsitellä henkilörekisterilain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä ja antaa näissä asioissa lausuntoja sekä tehdä tarpeelliseksi katsomiaan aloitteita. Vuoden 1994 laissa periaatteellisesti tärkeistä asioista säädettiin 2 §:n 2 kohdassa. Henkilötietolain säätämisen yhteydessä tämä kohta poistettiin (L 524/1999) ja henkilötietolain 38.2 §:ään otettiin määräys, jonka mukaan tietosuojalautakunta käsittelee henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä.

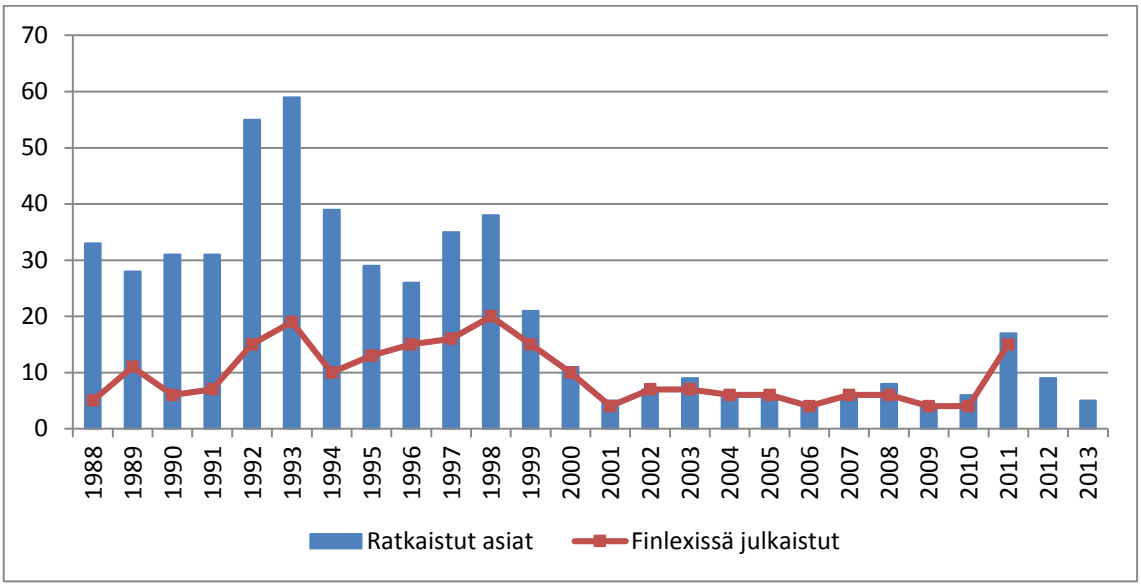
Periaatteellisesti tärkeiden asioiden käsittely on siis kuulunut tietosuojalautakunnan lakisääteisiin tehtäviin alusta alkaen. Lautakunta itse on kuitenkin suhtautunut varsin nihkeästi tähän tehtävään. Se on nähnyt toimivaltaansa kuuluvan tältä osin lähinnä lausuntojen antamisen eri tahoille sen sijaan, että se olisi pyrkinyt antamaan päätöksiensä yhteydessä yleisiä tai ennakollisia kannanottoja laintulkinnasta. Tällaisiakin asioita tietosuojavaltuutettu on toisinaan pyrkinyt lautakuntaan saattamaan. Näin oli erityisesti tietosuojavaltuutettu Kuopuksen toimikaudella (1992–1997).[264]

3. Asiamäärät ja päätösten julkaiseminen

Edellisessä luvussa kuvatut toimivallan muutokset ovat epäilemättä muuttaneet tietosuojalautakunnan roolia ja sen käsittelemien asioiden tyyppejä ja määriä. Helpoiten havaittava muutos on lautakunnan käsittelemien asioiden määrän lasku. Henkilörekisterilain voimaantulon jälkeen 1980– ja 1990–lukujen taitteessa lautakunta antoi vuosittain kolmisenkymmentä päätöstä.[265] Vuonna 1993 eli juuri ennen sukututkimus– ja henkilömatrikkelisäännösten lisäämistä henkilörekisterilakiin lautakunta antoi 59 päätöstä. Lainmuutoksen jälkeen päätösmäärä laski jälleen alkuvuosien tasolle. Henkilötietolain tultua voimaan ovat vuosittaiset asiamäärät jääneet pääasiassa alle kymmeneen, ja 2000–luvun huippuvuotenakin (2011) lautakunta ratkaisi vain 17 asiaa.[266] Vähimmillään lautakunta on ratkaissut vuodessa neljä asiaa (2006 ja 2009). Henkilötietolakia säädettäessä osattiin toki

[263] *Rantalankila*, Tietosuojalautakunnan toimivalta täsmentyi, Tietosuoja 2/1999 s. 40.
[264] Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki ja *Wallin – Nurmi*, Tietosuojalainsäädäntö (1991) s. 162.
[265] Varsinaisten päätösten lisäksi annetut lausunnot eivät sisälly tässä kappaleessa mainittuihin lukuihin.
[266] Piikki selittyy sillä, että lautakunta ratkaisi 11 tietosuojavaltuutetun pikavippiyrityksiä koskevaa hakemusta.

odottaa asiamäärään laskua, mutta laskun suuruus tuli pienenä yllätyksenä jopa lautakunnalle itselleen.[267]



Kuvaaja 33: Tietosuojalautakunnan antamat päätökset ja Finlexissä julkaistut päätökset 1988–2013.

Henkilörekisterilain aikaan selvästi suurimman asiaryhmän muodostivat rekisterinpitäjien poikkeuslupahakemukset, joita käsiteltiin henkilörekisterilain viimeisinä vuosina noin parikymmentä vuodessa. Lisäksi lautakunnassa käsiteltiin suhteellisen paljon tarkastusoikeuden toteuttamista ja virheen oikaisua koskevia asioita, joista merkittävimmän ryhmän 1990–luvun lopulla muodostivat luottotietorekisterissä olevien maksuhäirintämerkintöjen poistamista koskevat hakemukset, joita esimerkiksi vuonna 1998 käsiteltiin kahdeksan ja vuonna 1997 kymmenen.[268] Henkilörekisterilain 35 §:n mukaiset, tietosuojavaltuutetun hakemuksesta vireille tulevat määräysasiat olivat jonkin verran harvinaisempia, sillä vuonna 1997 niitä ei ollut yhtäkään ja vuonna 1998 viisi. Arkistointilupia koskevia asioita oli vuosittain muutama.[269]

Suurinta asiaryhmää eli poikkeuslupa–asioita koskeva toimivalta suppeni henkilötietolain myötä olennaisesti ja toiseksi suurinta eli tarkastusoikaisu– ja virheenoikaisuasioita koskevissa asioissa sitova päätösvalta siirtyi tietosuojavaltuutetulle. Myös arkistointilupia koskevat asiat siirtyivät pois lautakunnalta. Entisistä asiaryhmistä tietosuojalautakunnalle jäivät siis osa poikkeuslupa–asioista ja tietosuojavaltuutetun hakemuksesta vireille tulevat määräysasiat. Näistä selvästi suuremman ryhmän henkilötietolainkin aikana ovat muodostaneet poikkeuslupa–asiat. Tietosuojavaltuutetun aloitteesta vireille tulleita hakemuksia on vuosittain

[267] Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki.
[268] Näistä 18 asiasta vain yhdessä annettiin määräys poistaa maksuhäiriömerkintä luottotietorekisteristä.
[269] TK 1997 s. 22–23 ja TK 1998 s. 21–23.

ratkaistu korkeintaan muutama, poikkeuksena vuoden 2011 niin sanotut pikavippiasiat. Tuolloin lupa–asioita käsiteltiin kuusi ja hakemusasioita 11.[270]

Asiamäärien laskun osasyyksi on ehdotettu sitä, että henkilötietolaki korostaa neuvonnan ja ohjauksen merkitystä. *Vesa Muttilainen* pitää mahdollisena, että tämä on lisännyt osapuolten tietoja henkilötietojen käsittelyn keskeisistä periaatteista ja ehkäissyt kiistojen syntymistä näissä asioissa.[271] Vaikka tämä pitänee osittain paikkansa, asiaryhmien jakauman huomioiden olisi epärealistista ja yltiöoptimistista väittää laskun johtuvan pääasiallisesti neuvonnan ja ohjauksen tehoamisesta, varsinkin kun asiamäärien lasku on havaittavissa välittömästi lain voimaantulosta.[272] Kuvatut toimivallan muutokset ovat ilmeinen pääasiallinen syy asiamäärien laskulle.

Tietosuojalautakunnan ratkaisuja on julkaistu Finlex–tietokannassa. Edellisestä kuvaajasta ilmenevä Finlexissä julkaistujen päätösten määrä osoittaa, että henkilötietolain aikana Finlexissä on julkaistu noin 90 prosenttia tehdyistä päätöksistä, kun taas henkilörekisterilain aikaisista päätöksistä Finlexissä julkaistiin vain noin joka kolmas.[273] Ratkaisuista tiedottamisen voidaan tässä suhteessa nähdä parantuneen entisestä. Vuosina 2000–2009 julkaisematta jätetyt päätökset ovat koskeneet esim. aiemmin määräaikaisena myönnetyn luvan jatkamista ja tietosuojalautakunnan toimivaltaan kuulumattomia kysymyksiä.[274]

Lautakunnan omat, oikeusministeriön sivuston alaiset verkkosivut[275] ovat asiasisällöltään ja teknisesti vanhentuneet. Niiden päivittäminen on laiminlyöty, ja ne sisältävät toimimattomia linkkejä ja tyhjiä sivuja. Päätöksistä sivuilla on saatavilla vain kuusi tiivistelmää vuodelta 2008, ja jopa perustason informaatio lautakunnan toimivallasta on puutteellista. Sivuston laiminlyömiseen on ilmeisesti johtanut lautakunnan resurssien vähäisyys.

4. Esimerkkejä lautakunnan käsittelemistä asioista

4.1 Lupa–asiat

Tämän luvun tarkoituksena on selvittää, miten lautakunnan käsittelemät asiat ovat muuttuneet lainsäädännön, yhteiskunnan ja teknologian kehityksen edetessä. Käsittelen seuraavassa lautakunnan vuosina poikkeuslupa–asioissa antamia päätöksiä valittuina tarkasteluvuosina

[270] VK:t 2004–2006 ja KT:t 2007–2012.
[271] *Muttilainen*, Suomalaiset ja henkilötietojen suoja (2006) s. 56.
[272] Huomautettakoon, että tietosuojalautakunnan käsiteltäviksi tulevista asioista suuri osa on lupa–asioita, jotka eivät aina, tai välttämättä edes tyypillisesti, ole kiistanluonteisia. Tämä ei tosin estä neuvonnan ja ohjauksen mahdollista vaikutusta, mutta hyväkään tietoisuus ei poista tilanteita, joissa lupa on lain mukaan tarpeen.
[273] Vuosien 2012 ja 2013 päätöksistä ei tosin toistaiseksi ole julkaistu yhtäkään, mikä Pekka Nurmen haastattelussa 14.10.2013 antaman tiedon mukaan johtuu Finlexin päässä olevista ongelmista. Uusimpia päätöksiä ei ole julkaistu myöskään tietosuojalautakunnan verkkosivuilla.
[274] Eräs julkaisemattomista päätöksistä (TSL 3/2008) on lisäksi osittain salainen. Tutkimusta varten on ollut käytössä päätöslyhennelmät näinä vuosina annetuista julkaisemattomista päätöksistä (sekä osasta vuonna 1999 annetuista päätöksistä).
[275] http://oikeusministerio.fi/fi/index/ministerio/neuvottelu–jalautakunnat/tietosuojalautakunta.html, viitattu 20.3.2014.

1990, 1998, 2006 ja 2012. Poikkeuslupa–asioiden suuren määrän vuoksi on mielekästä ja tutkimusekonomisesti perusteltua keskittää huomio muutamaan valittuun tarkasteluvuoteen ja olennaisiin kehityslinjoihin. Tässä alaluvussa en käsittele tietosuojavaltuutetun lautakuntaan saattamia määräysasioita, joita käsittelen erikseen seuraavassa alaluvussa.

Vuonna 1990 lautakunta käsitteli kaikkiaan 31 asiaa, joista 27 koski poikkeuslupia ja loput neljä arkistointilupia. Poikkeuslupahakemuksista 20 hyväksyttiin (ainakin osittain), kolme hylättiin ja kolme jätettiin tutkimatta. Yksi hakemus peruutettiin. Arkistointilupia koskeneista hakemuksista kaksi hyväksyttiin ja kaksi jätettiin tutkimatta.[276] Tietosuojavaltuutettu ei saattanut lautakunnassa vireille yhtään asiaa. Seuraavassa on esimerkkejä vuonna 1990 käsitellyistä poikkeuslupa–asioista.[277]

> **TSL 2/1990**. LEL Työeläkekassa pyysi lupaa saada pitää hallussaan ja käyttää väestörekisterikeskukselta saamiaan väestöluetteloita vuosilta 1972 ja 1988. Tietosuojalautakunta katsoi, että hakija tarvitsi luvan poiketa yhteysvaatimuksesta. Lupa vuoden 1975 väestöluettelon hallussapitoon myönnettiin määräaikaisena. Muilta osin hakemus hylättiin.
>
> **TSL 5/1990**. Tietosuojalautakunta jätti tarpeettomana tutkimatta Helsingin yliopiston poikkeuslupahakemuksen henkilötietojen keräämiseen ja tallettamiseen Suomen valtiokalenterin julkaisemista varten. Syntymävuositiedon osalta tietosuojalautakunta myönsi poikkeusluvan.
>
> **TSL 6/1990**. Tietosuojalautakunta jätti Suomen Kansanopistoyhdistys – Finlands Folkhögskolförening ry:n oppilastietojen luovutusta koskevan hakemuksen tutkimatta siltä osin kuin kysymys oli tietojen saamisesta kunnallisten ja valtion koulujen manuaalisesti ylläpitämistä oppilasrekistereistä. Lautakunta myönsi hakijayhdistykseen kuuluville kansanopistoille poikkeusluvan saada käyttöönsä nimi– ja osoitetietoja yksityisten peruskoulujen ja lukioiden oppilasrekistereistä ja kunnallisten ja valtion peruskoulujen ja lukioiden atk:n avulla ylläpidetyistä oppilasrekistereistä koulutuspalveluista tiedottamista varten. Tiedot tuli päätöksen mukaan hävittää heti, kun ne eivät enää olleet tarpeen tiedotustoiminnassa.
>
> **TSL 13/1990**. Tietosuojalautakunta myönsi Ebeneser–säätiölle poikkeusluvan kerätä ja tallettaa henkilötietoja lastentarhaseminaari Ebeneseristä valmistuneita opettajia koskevan matrikkelin julkaisemista varten.
>
> **TSL 17/1990**. Tietosuojalautakunta myönsi Valtion sisäoppilaitoksen perinnetoimikunnalle poikkeusluvan saada kerätä ja tallettaa henkilötietoja sisäoppilaitoksessa vuosina 1945–47 opiskelleista oppilaitoksen historiikkiin liittyvää henkilömatrikkelia varten.
>
> **TSL 18/1990**. Tietosuojalautakunta myönsi puolustusministeriölle poikkeusluvan saada ajoneuvorekisteristä tietoja teknisellä käyttöyhteydellä sodanajan valmiusjärjestelmiin liittyvien lakisääteisten tehtäviensä hoitamiseksi ja valtion turvallisuuden ylläpitämiseksi.
>
> **TSL 19/1990**. Korkeimman hallinto–oikeuden palautettua asian uudelleen käsiteltäväksi tietosuojalautakunta katsoi, että päihtyneen säilöönottamista koskeva tieto on katsottava arkaluonteiseksi

[276] TK 1989–1990 s. 47.
[277] Finlexissä päätöksistä on julkaistu TSL 2/1990, TSL 19/1990 ja TSL 22/1990, joista on esitetty Finlex–otsikkotiedot. Muiden päätösten lyhennelmät ovat peräisin teoksesta *Konstari*, Henkilörekisterilaki (1992) s. 438–459 (Liite 4: Lyhennelmät tietosuojalautakunnan päätöksistä 5.4.1988–16.3.1992).

tiedoksi. Vartiointiliike tarvitsi näin ollen poikkeusluvan kyseisen tiedon keräämiseen ja tallettamiseen vartijoiksi hakevista henkilöistä. Lupaa ei myönnetty.[278]

TSL 22/1990. Espoon kouluvirasto pyysi lupaa henkilöllisesti rajoittamattoman selailuoikeuden saamiseksi pääkaupunkiseudun kuntien ylläpitämiin väestötietoihin. Tietosuojalautakunta katsoi, että kysymys oli massaluovutuksesta, johon hakija tarvitsi tietosuojalautakunnan luvan. Hakemus hylättiin.

TSL 26/1990. Tietosuojalautakunta hylkäsi Karjala–tietokantasäätiön hakemuksen saada kerätä ja tallettaa henkilötietoja luovutetun Karjalan alueen evankelis–luterilaisten ja ortodoksisten seurakuntien kirkonkirjoista ja siviilirekisteriasiakirjoista tulevaa tutkimuskäyttöä varten Karjala–tietokanta–nimiseen henkilörekisteriin.[279]

Kaikkiaan peräti 12 tapauksista koski henkilömatrikkeleita, –hakemistoja, –kalentereita tai vastaavia luetteloita. Tämänkaltaisten lupien tarve väheni olennaisesti edellä käsitellyn vuoden 1994 lainmuutoksen myötä. Myös väestötietojen saamista erilaisista laajoista henkilörekistereistä koskevat hakemukset olivat hyvin edustettuina. Lupahakemukset eivät koskeneet yksinomaan manuaalisessa muodossa olevia luetteloita, vaan myös atk–pohjaisia. Pääosa atk–pohjaisesta rekisterinpidosta oli kuitenkin vielä paikallista eikä verkottunutta. Myös teknisen käyttöyhteyden käyttämiseen myönnettiin kuitenkin lupa jo vuonna 1990.[280]

Vuonna 1998 tietosuojalautakunta teki 38 päätöstä, joista vain 20 koski poikkeuslupahakemuksia. Kahta arkistointilupa–asiaa lukuun ottamatta loput päätöksistä koskivat virheenoikaisu– ja tarkastusoikeusasioita. Virheenoikaisuasiat koskivat lähinnä maksuhäiriömerkintöjen poistamista luottotietorekistereistä, ja lautakunta hylkäsi kaikki hakemukset. Nämä asiat eivät siis henkilötietolain järjestelmässä enää tule lainkaan tietosuojalautakunnan käsiteltäväksi.[281]

Poikkeuslupa–asioista 14 tapauksessa lautakunta myönsi luvan ainakin osittain, kuudessa tapauksessa se hylkäsi hakemuksen kokonaan. Finlex–tietokannassa poikkeuslupapäätöksistä on 15 päätöstä, joiden otsikkotiedot on esitetty seuraavassa:

TSL 1/1998. Tietosuojalautakunta hylkäsi Karjala–tietokantasäätiön hakemuksen saada siirtää Karjala–tietokantaan sisältyviä vuotta 1900 vanhempia kirkonkirjatietoja Internet–tietoverkkoon. Henkilörekisterilaki tuli sovellettavaksi, koska tietokantaan sisältyi tietoja henkilöistä, joista jotkut saattoivat vielä olla elossa tai jotka olivat vasta hiljattain kuolleet. Tiedot oli tarkoitus siirtää Internetiin siten, että ne olisivat olleet vapaasti kaikkien saatavilla. Kysymyksessä oli henkilötietojen massaluovutus ja tällainen luovutus ulkomaille sekä tietokannan käyttötarkoituksen muutos.

TSL 2/1998. Tekniikan ja sosiaalialan oppilaitokselle myönnettiin määräaikainen poikkeuslupa saada luoda ja ylläpitää rekisteriä tietyltä alueelta kotoisin olevista ja alueella työskennelleistä ja opiskelleista diplomi–insinööreistä, insinööreistä ja teknikoista sekä lupa saada henkilötietoja oppilaitoksilta ja järjestöiltä rekisterin perustamista ja ylläpitoa varten. Rekisteriä oli tarkoitus käyttää insinööriyrittäjyyden

[278] Ks. TSL 10/1989 ja KHO 1990–A–6.
[279] Ratkaisussaan KHO 1992–A–29 korkein hallinto–oikeus kumosi tietosuojalautakunnan päätöksen ja palautti asian lautakunnalle, joka myönsi haetun poikkeusluvan uudella päätöksellään TSL 48/1992.
[280] Muista varhaisista teknistä käyttöyhteyttä koskevista asioista ks. myös päätökset TSL 25/1990, TSL 25/1992, TSL 36/1992, TSL 42/1992, TSL 51/1992 ja TSL 23/1993. Lautakunta arvioi näitä tilanteita massaluovutuksina.
[281] TK 1998 s. 21, 23.

edistämistä koskevassa opetusministeriön ja EU:n rahoittamassa tutkimusprojektissa. Rekisterin avulla selvitettiin alueella aloittavan tai jo toimivan yrityksen tarpeisiin sopivat henkilöt ja etsittiin sopiva otos yrittäjyys–, työllistymis– ja koulutuksen kehittämistutkimuksiin.

TSL 3/1998. Tietosuojalautakunta myönsi Teknisen Kaupan Liitto r.y:n jäsenyrityksinä oleville rakennuskonevuokraamoille määräaikaisen poikkeusluvan ylläpitää yhteistä sulkulistaa henkilöistä, jotka ovat syyllistyneet kyseisiin rakennuskonevuokraamoihin kohdistuviin väärinkäytöksiin.

TSL 5/1998. Telehallintokeskukselle myönnettiin poikkeuslupa saada säilyttää aikaisemman poikkeusluvan nojalla muodostettu ja television luvattoman käytön vähentämiseksi käytetty kirjekampanjarekisteri ja poikkeuslupa yhdistää rekisterin sisältämät henkilötiedot puhelinyhtiön numeropalvelurekisteriin puhelinkampanjan toteuttamista varten.

TSL 6/1998. Telehallintokeskukselle myönnettiin poikkeuslupa käyttää aikaisemman poikkeusluvan nojalla muodostettua ja television luvattoman käytön vähentämiseksi käytettävää vuoden 1998 kirjekampanjarekisteriä puhelinkampanjassa sekä keräämään ja tallettamaan puhelinnumeroita puhelinkampanjaa varten.

TSL 7/1998. Tietosuojalautakunta jätti toimivaltaansa kuulumattomana tutkimatta osakeyhtiön hakemuksen saada arvo–osuustilejä koskevia tietoja massaluovutuksena Suomen Arvopaperikeskus Oy:ltä. Lautakunta hylkäsi yhtiön hakemuksen saada yhdistää väestötietojärjestelmästä saatavat henkilötunnukset yhtiön muodostamaan osakeannin suoramarkkinoinnissa käytettävään kampanjarekisteriin ja näin syntyvän rekisterin yhdistämiseen Suomen Arvopaperikeskus Oy:n omistajaluetteloon arvo–osuustilin olemassaolon ja sen numeron selvittämiseksi.

TSL 12/1998. Kansanterveyslaitokselle myönnettiin poikkeuslupaa saada käyttää nk. äitirekisterin henkilötietoja ja neuvolaseulonta–aineiston seeruminäytteitä vastasyntyneisyyskauden B–streptokokki–infektioita koskevassa tieteellisessä tutkimuksessa.

TSL 19/1998. Suomen Asiakastieto Oy:lle myönnettiin määräaikainen poikkeuslupa tallettaa tieto kertaluottoon liittyvästä maksuhäiriöstä kun maksuerä on ollut maksamatta 60 päivää.

TSL 23/1998. Tietosuojalautakunta jatkoi Suomen Vakuutusyhtiöiden Keskusliitolle myönnettyä poikkeuslupaa kerätä, tallettaa ja käyttää tietoja sellaisista vakuutusyhtiöihin kohdistuneista väärinkäytöksistä, joista on tehty rikosilmoitus. Poikkeuslupaa jatkettiin myös siltä osin kuin se koski tietojen luovuttamista toisille vakuutusyhtiöille. Lupaan sisältyi useita lupamääräyksiä.

TSL 24/1998. Tietosuojalautakunta hylkäsi Enso Oyj:n poikkeuslupahakemuksen saada kerätä ja tallettaa pysyvään suoramarkkinointirekisteriin tietoja metsänomistajista, jotka saattaisivat tulevaisuudessa myydä puuta, eli potentiaalisista asiakkaista. Rekisteriä oli tarkoitus käyttää puukaupan markkinoinnissa ja metsäviestinnässä.

TSL 25/1998. Tietosuojalautakunta hylkäsi Metsäliitto Osuuskunnan poikkeuslupahakemuksen saada kerätä ja tallettaa pysyvään suoramarkkinointirekisteriin tietoja yli 5 hehtaarin metsätilojen omistajista. Rekisteriä oli tarkoitus käyttää puunostopalveluiden kohdentamiseen niihin tiloihin, joilla on hakkuukelpoista puuta, ja metsänhoitopalveluiden tarjoamiseen.

TSL 26/1998. Tietosuojalautakunta myönsi Videokauppiasliiton jäsenyrityksinä oleville videovuokraamoille määräaikaisen poikkeusluvan saada ylläpitää yhteistä sulkulistaa henkilöistä, jotka ovat jättäneet vuokrauskohteen palauttamatta ja/tai ylipäivien vuokran maksamatta. Lupaan sisältyi useita lupamääräyksiä.

TSL 33/1998. Väestötietolaissa ja –asetuksessa tarkoitetun henkilön osoitteen ei voitu kiistatta katsoa tarkoittavan myös henkilön postiosoitetta. Koska väestötietojärjestelmään talletettavista henkilötiedoista oli säädetty tyhjentävästi erityislainsäädännössä, tietosuojalautakunnalla ei ollut henkilörekisterilain mukaista toimivaltaa myöntää väestörekisterikeskukselle poikkeuslupaa postiosoitetta koskevien tietojen tallettamiseen väestötietojärjestelmään.

TSL 37/1998. Luottolaitoksille myönnettiin poikkeuslupa saada tallettaa entisiä asiakkaitaan koskevia saamisen maksuviivästymistietoja ja hakijoiden palveluihin kohdistuneita väärinkäytöstietoja asiakashäiriörekistereihinsä sekä luovuttaa väärinkäytöstietoja toisille luottolaitoksille. Hakijat tarvitsivat luvan poiketa yhteysvaatimuksesta ja arkaluonteisten tietojen rekisteröintikiellosta sekä luvan tietojen luovuttamiseen. Lupa myönnettiin määräaikaisena ja siihen asetettiin useita lupamääräyksiä.

TSL 38/1998. Tietosuojalautakunta myönsi Raha–automaattiyhdistykselle määräaikaisen poikkeusluvan kerätä ja tallettaa pelikasinon asiakkaita koskevia arkaluonteisia henkilötietoja.

Vuoden 1998 tapauksissa silmiinpistäviä ovat useat sulkulistoja tai muita asiakashäiriö– ja väärinkäytöstietoja koskevat hakemukset. Näihin hakemuksiin lautakunta suhtautui suopeasti, vaikkakin asetti lupapäätöksissään lukuisia lupamääräyksiä. Eräällä tavalla yhteiskunnan kehitystä kuvaa kirkonkirjatietojen Internetiin siirtämistä koskeva hakemus. Internetiin siirtämisen tulkittiin tarkoittavan massaluovutusta ulkomaille, ja hakemus hylättiin. Muuten avoimen Internetin tai verkossa tarjottavien palveluiden merkitys ei vielä vuonna 1998 ollut lupa–asioissa näkyvillä. Tyypillistä poikkeuslupa–asioille oli, että poikkeusta haettiin samalla useista eri henkilörekisterilainsäädännön vaatimuksista, esimerkiksi yhteysvaatimusta, käyttötarkoitussidonnaisuutta, massaluovutusta tai ulkomaille luovutusta koskevista säännöksistä.[282]

Kaikki neljä vuonna 2006 annettua päätöstä koskivat poikkeuslupa–asioita. Kolme hakemuksista hyväksyttiin, yhdessä todettiin hakijalla olleen oikeus henkilötietojen käsittelyyn myös ilman poikkeuslupaa. Päätösten Finlex–otsikot kuuluvat seuraavasti:

TSL 1/2006.Tietosuojalautakunta katsoi, että IP–osoitteet ovat pääsääntöisesti henkilötietoja. Tekijänoikeuden Tiedotus– ja Valvontakeskuksen (TTVK) käsittelemät tiedot henkilöistä, joiden se katsoi syyllistyneen tekijänoikeusrikkomukseen tai –rikokseen ja tiedot heidän käyttämistään IP–osoitteista olivat henkilötietolaissa tarkoitettuja arkaluonteisia henkilötietoja. TTVK:lla oli oikeus käsitellä kyseisiä tietoja ilman tietosuojalautakunnan lupaa, koska tietojen käsittely oli tarpeen tekijänoikeusloukkauksia koskevien oikeusvaateiden laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi.

TSL 2/2006. Kahdelle vakuutusyhtiölle myönnettiin lupa käsitellä vakuutussopimuslain mukaisen edunsaajan yksilöimiseksi THS–tunnistusohjelman avulla saatavia sellaisten henkilöiden tietoja joilla ei ole asiallista yhteyttä hakijoiden toimintaan. Mainittu kyselyohjelma mahdollistaa väestötietojärjestelmään merkittyjen henkilötietojen vapaan selailumahdollisuuden suorakäyttöyhteyden avulla, ja annettujen hakuehtojen perusteella voidaan saada vastauksena samalla usean henkilön tietoja.

TSL 3/2006. Ylivieskan teknologiakylä YTEK Oy:lle myönnettiin lupa käsitellä oppilaitoksilta pyydettäviä henkilötietoja valmistuneista, jotka ovat kotoisin ja/tai ovat opiskelleet Keski–Pohjanmaalla ja eteläisellä Pohjois–Pohjanmaalla. Tietojen avulla heidän osoitetietonsa voitiin päivittää

[282] Ks. myös TK 1998 s. 21.

Väestörekisterikeskuksesta ja heille voitiin postittaa kysely, jossa tiedustellaan heidän kiinnostustaan tulla alueella toimivien tai aloittavien yritysten palvelukseen tai kiinnostusta perustaa yritys tälle alueelle. Tietosuojalautakunnalla ei ollut toimivaltaa myöntää lupaa henkilötunnusten käsittelyyn.

TSL 4/2006. Tietosuojalautakunta myönsi vakuutuslaitoksille (vakuutusyhtiöille ja vakuutusyhdistyksille) määräaikaisen luvan käsitellä toisilta vakuutuslaitoksilta saatavia vahinkotietoja vakuutusrikollisuuden ehkäisemiseksi. Tietosuojalautakunta asetti lisäksi ehdot vahinkotietojen luovuttamiselle ja vahinkotietojen muulle käsittelylle.

Tapausta TSL 1/2006 voidaan pitää tyypillisenä esimerkkinä kysymyksestä, jonka on tehnyt oikeudellisesti merkitykselliseksi osittain tekninen kehitys, mutta pääasiassa yhteiskunnan toimintojen, tässä tapauksessa erityisesti musiikkipiratismin, siirtyminen tietoverkkoihin. IP–osoitteet ovat perinteisiin nimen tai kuvan kaltaisiin henkilötietoihin verrattuna uudenkaltaisia, verkkoympäristössä keskeisiä tunnistetietoja, joiden avulla pystytään usein selvittämään yksittäisen Internet–käyttäjän henkilöllisyys. Henkilötietojen suojaa ja henkilörekistereitä koskevassa varhaiskeskustelussa ne eivät olleet nykyisessä mielessä merkityksellisiä. IP–osoitteita on toki ollut olemassa jo kauan ennen tietosuojalautakunnan perustamista.

Kolme jälkimmäistä tapausta ovat tyyppiesimerkkejä henkilötietolain järjestelmässä tarpeellisista poikkeusluvista. Kaikissa näissä tapauksissa oli kyse henkilötietolain 8 §:n mukaisesta, käsittelyn yleisiä edellytyksiä koskevasta poikkeuksesta hakijan oikeutetun edun perusteella. Erityisesti THS–tunnistusohjelman käyttämistä koskevat luvat ovat olleet lautakunnassa esillä usein, ja niitä on myös usein myönnetty vakuutusyhtiöille ja vielä useammin ammattimaista perimistoimintaa harjoittaville.[283] Vakiintuneen lautakuntakäytännön myötä asiasta säätäminen laissa olisi harkitsemisen arvoinen mahdollisuus. Myös vakuutuslaitosten vahinkotietojen keskinäistä jakamista[284] sekä alueen oppilaitoksista valmistuneiden henkilöiden tietojen käsittelyä koskevia lupia[285] on käsitelty lautakunnassa useampaan otteeseen.

Vuoden 2012 päätöksiä ei siis ole julkaistu Finlexissä eikä lautakunnan kotisivuilla. Vuonna 2012 tietosuojalautakunta ratkaisi yhdeksän asiaa: seitsemän rekisterinpitäjän lupahakemusta ja kaksi tietosuojavaltuutetun tekemää hakemusta. Vain yksi lupahakemus hylättiin, muut hakemukset hyväksyttiin. Ratkaisuista kolmessa myönnettiin lupa THS–tunnistusohjelman käyttöön ammattimaisessa perintätoiminnassa. Lisäksi lautakunta myönsi kahdelle yritykselle

[283] Ks. päätöksessä TSL 2/2006 viitatut TSL 5/2000, TSL 6/2000, TSL 2/2002, TSL 7/2003, TSL 5/2004, TSL 6/2004, TSL 2/2005, TSL 3/2005 ja TSL 4/2005 sekä muut väestötietojärjestelmän THS–tunnistuskyselyn käyttöä koskevat päätökset TSL 1/2003, TSL 2/2003, TSL 8/2003, TSL 3/2004, TSL 2/2007, TSL 3/2007, TSL 5/2008, TSL 8/2008, TSL 3/2010, TSL 2/2011 ja TSL 4/2011. Myös vuonna 2012 myönnettiin kolme lupaa THS–tunnistuskyselyn käyttöön. KT 2012 s. 57.
[284] Ks. päätöksessä TSL 4/2006 viitatut TSL 1/2001, TSL 4/2001, TSL 4/2002 ja TSL 5/2002 sekä tuoreempi vahinkotietojen luovuttamista koskeva päätös TSL 4/2009.
[285] Ks. päätöksessä TSL 3/2006 viitatut TSL 2/1998, T 17/1999 ja TSL 9/2000.

aiempaa päätöstään TSL 2/2004 vastaavan luvan tallettaa asiakashäiriörekistereihin entisiä asiakkaita koskevia tietoja.[286]

Teknologisen kehityksen kuvaajina mielenkiintoisempia ovat Nokialle ja Microsoftille myönnetyt paikannus– ja karttapalveluihin liittyvät luvat. Niistä ensimmäinen (TSL 1/2012) koski katunäkymäpalvelua varten tarpeellisten tietojen keräämistä eli käytännössä näkymien kuvaamista kadulla liikkuvasta autosta käsin. Katunäkymäpalvelua koskevat asiat eivät olleet ensimmäistä kertaa esillä tietosuojalautakunnassa, vaan tällainen asia oli tullut lautakuntaan jo vuonna 2010 tietosuojavaltuutetun aloitteesta. Tuolloin tietosuojavaltuutettu pyysi lautakuntaa arvioimaan, käsitteleekö Fonecta Oy Virtuaalikierros–katunäkymäpalvelua ylläpitäessään henkilötietoja, ja velvoittamaan Fonecta määräajassa oikaisemaan sen, mitä on oikeudettomasti tehty tai laiminlyöty. Päätöksellä TSL 4/2010 ratkaistiin sekä tietosuojavaltuutetun hakemus että Fonectan asian käsittelyn aikana toissijaisesti tekemä lupahakemus. Tietosuojalautakunta katsoi Fonectan käsitelleen henkilötietoja ja myönsi kolmen vuoden määräaikaisen luvan, jolle se asetti kolme lupamääräystä. Määräaikaisuutta lautakunta perusteli alan voimakkaalla teknisellä kehityksellä, jonka myötä se arvioi saattavan olla aihetta asian arvioimiseen uudelleen. Lupamääräysten mukaan Fonectan tuli muokata kuvissa näkyvät henkilöt ja ajoneuvot tunnistamattomiksi ennen kuvien julkaisemista katunäkymäpalvelussa, Fonecta sai säilyttää raakadataa vain siihen saakka, kunnes katunäkymäpalvelu on luotu, eikä se ei saanut luovuttaa raakadataa kolmansille osapuolille. Vastaavat ehdot lautakunta sisällytti myös Googlelle vuonna 2011 vastaavaa Street View –palvelua varten myöntämäänsä kolmivuotiseen lupaan (TSL 3/2011).[287]

Nokia ja Microsoft olivat pyytäneet lupaa säilyttää osaa raakadatasta 12 kuukautta kuvien julkaisemisesta ja enintään 15 kuukautta niiden ottamisesta, ja osaa raakadatasta koko kolmen vuoden lupa–ajan. Tämän lautakunta hyväksyi, koska hakijat olivat perustelleet tarvetta esittämilleen säilytysajoille yksityiskohtaisesti muun muassa datan käyttötarkoituksilla, merkityksellä palvelun ja kuvien sumentamiseen käytettävien algoritmien ja menettelyjen kehittämisessä, datan suojauksella sekä kokemuksillaan muissa maissa. Henkilöjen ja ajoneuvojen tunnistamattomaksi muokkaamista ja raakadatan luovutuskieltoa koskevat määräykset annettiin myös Nokialle ja Microsoftille, ja lisäksi päätökseen kirjattiin erityinen määräys siitä, että yritysten on varmistettava, että rekisteröityjä informoidaan selkeästi näiden oikeuksista ja siitä, miten rekisteröidyt voivat olla yhteydessä rekisterinpitäjään oikeuksiensa toteuttamiseksi. Viimeksi mainitun määräyksen lisääminen johtui tietosuojavaltuutetun asiassa antamasta lausunnosta, jossa hän nosti esiin tietosuojavaltuutetun toimistoon tulleet yhteydenotot koskien vaikeuksia saada yhteyttä aiemmin Street View –palveluun luvan

[286] KT 2012 s. 57–58. Vrt. myös edellä mainittu TSL 37/1998.
[287] Ks. myös KT 2011 s. 32.

saaneeseen Googleen, ja korosti informoinnin merkityksestä erityisesti, kun lupaa pyysi kaksi erillistä rekisterinpitäjää, ja tietoja voitiin käyttää useissa eri palveluissa.[288]

Toinen lautakunnan Nokialle ja Microsoftille myöntämä lupa (TSL 3/2012) koski WiFi–tietojen[289] keräämistä ja käsittelyä paikannuspalveluinfrastruktuurin rakentamiseksi ja paikkatietoihin perustuvien palveluiden tarjoamiseksi ja kehittämiseksi.[290] Myös WiFi–tietojen käsittelyä koskevaan lupaan lautakunta sisällytti siihen lupamääräykset, joilla se rajoitti raakadatan säilyttämistä ja kielsi sen luovuttamisen ulkopuolisille. Lautakunta määräsi myös, että hakijoiden on huolehdittava siitä, että kerättäessä tietoja päätelaitteen käyttäjiltä heidän suostumuksensa perusteella suostumus täyttää lainsäädännössä asetetut edellytykset. Tämäkin lupa myönnettiin hakemuksen mukaisesti kolmeksi vuodeksi, mitä lautakunta piti perusteltuna yksityisyyden ja henkilötietojen suojaa turvaavan tekniikan kehityksen seuraamisen tarpeen vuoksi.

Mainitut tapaukset kertovat ennen kaikkea siitä, että teknologinen kehitys on mahdollistanut entistä laajemman massaluontoisen tiedonkeruun, mikä taas avaa ovia erilaisten uudentyyppisten palveluiden rakentamiselle. Massaluonteiseen tiedonkeruuseen taas sisältyy usein mittavia henkilötietojen suojaa koskevia riskejä.

Karttapalveluja rakennettaessa kerättävät henkilötiedot (tunnistettavat kuvat henkilöistä ja ajoneuvoista) eivät sinänsä ole lainkaan tarpeellisia tai hyödyllisiä palvelun loppukäyttäjän näkökulmasta, mutta kuva–aineiston kerääminen ilman henkilöjen tai ajoneuvojen kuvaamista ei käytännössä olisi mahdollista. Niinpä palveluntarjoajat joutuvat käsittelemään suurta määrää henkilötietoja, joiden käsittelyä lakiin kirjatut edellytykset eivät mahdollista; kaikilta kuvilta esiintyviltä on käytännössä mahdotonta pyytää suostumusta heidän tietojensa käsittelyyn. Tällaisen toiminnan täydellinen kieltäminen olisi innovaatioita lamaannuttava ja joustamaton keino, eikä lakiin toisaalta ole helppo kirjata teknologianeutraalisti niitä edellytyksiä, joiden täyttyessä henkilötietojen käsittely on erilaisten uudentyyppisten palveluiden rakentamisessa tarpeen. Juuri tämäntapaisten tilanteiden ratkaisemisessa lupamenettelyä onkin pidettävä tarpeellisena: se on joustava, prosessi ei rasita suhteettomasti palveluntarjoajaa ja samalla se mahdollistaa lautakunnalle yksittäistapauksellisen henkilötietojen käsittelyn asianmukaisuuden kontrolloimisen.

Karttapalvelua koskevassa päätöksessä tärkeimpinä huomioitavina kehityspiirteinä on pidettävä keräämisen tapaa ja laajuutta. Kerättävät tiedot ovat kuitenkin käytännössä tunnistettavia valokuvia henkilöistä ja ajoneuvoista. WiFi–tietojen kerääminen paikkatietoihin perustuvien palvelujen kehittämiseksi on esimerkki siitä, että kerättäessä massaluonteisesti

[288] Ks. myös KT 2012 s. 57.
[289] WiFi–liityntäpisteiden MAC–osoite (laitteen yksilöivä tunnus), signaalivahvuus ja radiotyyppi. WiFi–paikannusta voidaan käyttää GPS–paikannusta täydentävästi alueilla, joilla GPS–satelliittiyhteys on huono. Ks. WP 29:n lausunto 13/2011 älykkäiden mobiililaitteiden paikkatietopalveluista (WP 185).
[290] Tähänkin lupaan asetettiin raakadatan säilyttämistä ja luovuttamista koskevat ehdot. Ks. myös KT 2012 s. 57.

tietoja uudenlaisten palveluiden rakentamista varten voidaan kerätä myös uudentyyppisiä henkilötietoja, tässä tapauksessa WiFi–liityntäpisteen tietoja, joiden avulla liityntäpisteen omistaja voi olla epäsuorasti tunnistettavissa.[291]

Itse paikkatietojen käsittely taas on hyvinkin tyypillistä verkkoyhteiskunnan palveluille. Esimerkiksi useiden älypuhelinsovellusten toimivuus on täysin riippuvainen verkkoon jatkuvasti liitetyn mobiilin päätelaitteen ja sen käyttäjän sijainnista. Paikkatietojen ja niitä hyödyntävien sovellusten avulla palvelun käyttäjää on mahdollista myös valvoa erilaisia tarkoituksia varten, mikä voi vaarantaa käyttäjän yksityisyyttä ja henkilötietojen suojaa. On luultavaa, että paikkatietojen käsittely niihin perustuvan palvelun tarpeisiin itsessään ei kuitenkaan jatkossakaan tule usein lautakunnan käsittelyyn lupa–asian muodossa, sillä palvelun kultakin käyttäjältä voidaan yleensä hankkia suostumus paikkatiedon käyttöön. Paikkatietojen käsittelyyn ja jatkohyödyntämiseen varsinaisen palvelun tarjoamisen jälkeen liittyy toki tietosuojakysymyksiä. Tietosuojalautakunnan poikkeuslupa–asioiden kannalta relevantit paikkatieto–ongelmat tulevat jatkossakin todennäköisesti liittymään uusien palveluiden rakentamiseen, ei niinkään palveluiden tarjoamiseen.

4.2 Määräysasiat

Koska määräysasioita on käsitelty sekä henkilörekisterilain että henkilötietolain aikana merkittävästi vähemmän kuin lupa–asioita, käsillä ei ole esitystekniseen tai tutkimusekonomiseen rajaukseen liittyvää syytä rajoittaa tarkastelua vain valikoituihin tarkasteluvuosiin. Seuraava on tarkoitettu jokseenkin kattavaksi kuvaukseksi siitä, millaisia määräysasioita tietosuojalautakunta on toimintansa aikana käsitellyt ja miten yhteiskunnallinen ja teknologinen kehitys näissä asioissa ilmenee.

Henkilörekisterilain ollessa voimassa tietosuojavaltuutettu saattoi lautakunnan käsiteltäväksi muun muassa seuraavanlaisia rekisteritoiminnan oikaisemista tai kieltämistä koskevia tapauksia (Finlex–otsikkotiedot):

> **TSL 6/1991**. Henkilötunnusta voitiin pitää henkilörekisterilain tarkoittamalla tavalla tarpeellisena televisioluparekisterissä. Telehallintokeskuksella ei ollut oikeutta ylläpitää väestön keskusrekisterin ja televisioluparekisterin yhdistämisen tuloksena syntynyttä lupatarkastusluetteloa puuttuvan yhteysvaatimuksen vuoksi. Tietosuojalautakunta velvoitti telehallintokeskuksen hävittämään mainitun rekisterin 200.000 markan sakon uhalla. Korkein hallinto–oikeus kumosi osittain tietosuojalautakunnan asettaman velvoitteen rekisterin hävittämisestä (KHO 1992–A–6).
>
> **TSL 56/1993**. Tietosuojavaltuutetun hakemuksessa oli kysymys henkilötunnuksen tarpeellisuudesta Turun kaupunginkirjaston lainaajarekisterissä. Lautakunta katsoi toisin kuin tietosuojavaltuutettu, että

[291] Ks. WP 29:n lausunto 13/2011 älykkäiden mobiililaitteiden paikkatietopalveluista (WP 185) s. 11. Yleisemmin ks. myös WP 29:n lausunto 4/2007 henkilötietojen käsitteestä (WP 136). Päätöksessään tietosuojalautakunta lausui, että WiFi–liityntäpisteen MAC–osoitetta yhdistettynä sen laskettuun sijaintiin on pidettävä henkilötietona.

henkilötunnuksen käyttö Turun kaupunginkirjaston lainaajarekisterissä oli rekisterin käyttötarkoituksen kannalta tarpeellista. Henkilötunnusta tuli voida käyttää vain lainaajakortin antamista ja lainausoikeuden lakkaamista koskevissa tilanteissa sekä perintätilanteissa.

TSL 18/1994. Tietosuojalautakunta katsoi, ettei käteiskortin haltijan henkilötunnuksen käyttö Oy Stockmann Ab:n asiakasrekisterissä ollut rekisterin käyttötarkoituksen kannalta tarpeellista. Lautakunta määräsi yhtiön lopettamaan käteiskortin haltijoiden henkilötunnustietojen keräämisen ja poistamaan jo rekisteröidyt henkilötunnukset asiakasrekisteristä.

TSL 20/1994. Tietosuojalautakunta katsoi, ettei henkilötunnuksen käyttö Rautakirja Oy:n Vip–Video Clubin jäsenrekisterissä ollut rekisterin käyttötarkoituksen kannalta tarpeellista. Lautakunta määräsi yhtiön lopettamaan henkilötunnuksen keräämisen ja poistamaan jäsenrekisteristä jo kerätyt henkilötunnukset. Tietosuojalautakunta katsoi kuitenkin, että henkilötunnuksen käyttö asiakasrekisterissä videovuokraustapahtuman yhteydessä oli rekisterin käyttötarkoituksen kannalta tarpeellista.

TSL 3/1995. Tietosuojalautakunta katsoi, että kaupparekisterilain nojalla kaupparekisteriin kerätyt ja talletetut elinkeinonharjoittajien henkilötunnukset ja kotiosoitteet eivät ole henkilörekisterilaissa tarkoitettuja henkilötietoja eikä kaupparekisteriä, vaikka se sisältääkin myös luonnollisten henkilöiden henkilötunnuksia ja osoitteita, ole miltään osin pidettävä henkilörekisterilaissa tarkoitettuna henkilörekisterinä.

TSL 8/1995. Tietosuojalautakunta hylkäsi tietosuojavaltuutetun hakemuksen, jossa hän pyysi, että tietosuojalautakunta kieltäisi Osuusliike Elantoa keräämästä ja tallettamasta henkilörekisterilain 6 ja 7 §:n ja hyvän rekisteritavan vastaisesti näpistyksestä ym. rikoksista epäiltyjä henkilöitä koskevia, arkaluonteisia henkilötietoja henkilörekisteriin. Lautakunta katsoi, että hakemuksessa tarkoitettu rekisteri oli henkilörekisteri, koska tiettyä epäiltyä koskevat tiedot voitiin löytää helposti ja kohtuuttomitta kustannuksitta epäillyn rikoksen tapahtuma–ajan perusteella.

Rekisterin perustamista ei ollut pidettävä henkilörekisterilain tarkoituksen vastaisena perusteettomana puuttumisena rekisteröidyn yksityisyyteen, etuihin tai oikeuksiin. Ottaen huomioon henkilörekisterilain tarkoituksen ja asianomistajalle Suomen lain mukaan kuuluvat oikeudet tietosuojalautakunta katsoi, että hakemuksessa tarkoitetun rekisterin perustaminen ja pitäminen johtui välittömästi asianomistajalle kantajana säädetystä tehtävästä näyttää toteen ne seikat, jotka tukevat kannetta ja joihin kantajan vaatimus nojautuu.

TSL 9/1995. Tietosuojalautakunta hylkäsi tietosuojavaltuutetun hakemuksen, jolla hän pyysi, että tietosuojalautakunta kieltäisi Oy Stockmann Ab:tä keräämästä ja tallettamasta henkilörekisterilain 6 ja 7 §:n ja hyvän rekisteritavan vastaisesti näpistyksestä ym. rikoksista epäiltyjä henkilöitä koskevia, arkaluonteisia henkilötietoja henkilörekisteriin. Tietosuojalautakunta katsoi, että rekisterin perustamista ei ollut pidettävä henkilörekisterilain tarkoituksen vastaisena perusteettomana puuttumisena rekisteröidyn yksityisyyteen, etuihin tai oikeuksiin. Ottaen huomioon henkilörekisterilain tarkoituksen ja asianomistajalle Suomen lain mukaan kuuluvat oikeudet lautakunta katsoi, että hakemuksessa tarkoitetun rekisterin perustaminen ja pitäminen johtui välittömästi asianomistajalle kantajana säädetystä tehtävästä näyttää toteen ne seikat, jotka tukevat kannetta ja joihin kantajan vaatimus nojautuu.

TSL 22/1995. Tietosuojalautakunta hylkäsi tietosuojavaltuutetun hakemuksen, jossa hän pyysi, että tietosuojalautakunta määräisi henkilörekisterilain 35 [§]:n nojalla Sanoma Osakeyhtiön välittömästi lopettamaan henkilötunnusten keräämisen ilmoituksia jättäviltä henkilöiltä tilanteissa, joissa ilmoitus jätetään puhelimitse tai muutoin siten, ettei ilmoituksen jättäjän henkilöllisyyttä voida tarkastaa. Lautakunta katsoi, että henkilötunnusten kerääminen em. tilanteissa on henkilörekisterilain 5 [§]:n 2 momentin tarkoittamalla tavalla tarpeellista. Henkilötunnuksia kerättäessä ei poikettu

huolellisuusvelvoitteesta eikä loukattu hyvää rekisteritapaa. Rekisteröidyn yksityisyyden suojaa ei muutoinkaan loukattu perusteettomasti. (Äänestys 5–2)

TSL 24/1996. Tietosuojalautakunta määräsi henkilörekisterilain 35 §:n nojalla Metsästäjäin Keskusjärjestön lopettamaan henkilötunnusten merkitsemisen metsästyskortteihin.

TSL 15/1997. Video Film Town Oy määrättiin lopettamaan välittömästi niiden asiakkaiden henkilötunnustietojen kerääminen ja tallettaminen asiakasrekisteriinsä, joilla ei ole mitään tuotetta vuokralla. Yhtiö määrättiin poistamaan näitä asiakkaita koskevat henkilötunnukset asiakasrekisteristään määräaikaan mennessä.

TSL 16/1997. Visa–korttiostoissa syntyvät maksutositteet muodostivat osan Luottokunnan asiakasrekisteriä. Maksutositteeseen kaupoissa merkittävä henkilötunnuksen loppuosa muodosti henkilötiedon esiintyessään allekirjoituksen yhteydessä. Luottokunta ei toiminut vastoin henkilörekisterilaissa säädettyä huolellisuusvelvoitetta ja hyvää rekisteritapaa antaessaan Visa–kortin maksuvälineeksi hyväksyville kauppaliikkeille ohjeen kerätä maksutositteisiin asiakkaan henkilötunnuksen loppuosa. Luottokunta ei näin menetellessään toiminut myöskään vastoin henkilörekisterilaissa säädettyä suojaamisvelvoitetta. Henkilötunnuksen loppuosan keräämistä maksutositteisiin voitiin pitää tarpeellisena, koska merkinnän avulla voitiin jälkikäteen todeta henkilöllisyyden tarkistamisen tapahtuneen Luottokunnan kauppiaille antamien ohjeiden mukaisesti.

TSL 27/1997. Hyvään rekisteritapaan kuuluu, että rekisteröidylle annetaan oikea ja selkeä kuva hänen oikeuksistaan. Sen vuoksi sellaisissa arvontakupongeissa, joissa mainitaan "Osoitetietojani voidaan käyttää ja luovuttaa suoramarkkinointiin", tulee samalla myös selvästi ilmaista, että rekisteröidyllä on oikeus kieltää henkilötietojensa käyttö ja luovutus suoramarkkinointiin.

TSL 29/1997. Väestörekisterikeskuksella ei ollut oikeutta luovuttaa henkilötietoja pankeille ja vakuutusyhtiöille osoitetietojen päivittämistä varten tapauksissa, joissa henkilö on kieltänyt tietojensa käyttämisen ja luovuttamisen osoitepalveluun.

Noin puolet tietosuojavaltuutetun tekemistä hakemuksista hyväksyttiin ainakin osittain, ja vastaavasti noin puolet hylättiin. Kuten otsikkotiedoista ilmenee, valtaosassa henkilörekisterilain aikaisista määräysasioista oli kyse henkilötunnuksen käsittelystä eri yhteyksissä, usein erilaisiin jäsen– tai asiakasrekistereihin liittyen. Yksikään 1990–luvun määräysasioista ei koskenut kuluttajille tarjottaviin verkkopalveluihin liittyvää henkilötietojen käsittelyä, sillä tällaiset palvelut eivät vielä olleet kovin yleisessä käytössä.

Henkilötietolain aikaisista määräysasioista ylivoimaisesti suurimman ryhmän ovat muodostaneet jo edellä mainitut pikavippiasiat. 2000–luvun ensimmäisen vuosikymmenen lopulla Internetin ja tekstiviestien kautta välittömästi myönnettävien pienien, korkeakorkoisten luottojen suosio kasvoi nopeasti, ja alasta muodostui varsin villi ja säätelemätön. Ensimmäisen kerran pikaluottoalan henkilötietojen käsittelyä selvitettiin tietosuojavaltuutetun toimistossa jo vuonna 2006. Tuolloin tietosuojavaltuutettu teki hakemuksen, jonka johdosta tietosuojalautakunta määräsi tekstiviestin välityksellä pikaluottoja myöntävän yrityksen välittömästi muuttamaan luotonhakijoiden tunnistamiseen liittyvän toimintatapansa sellaiseksi, että voidaan varmistaa, että väärää henkilöä ei rekisteröidä luotonhakijaksi. Yritys valitti

asiasta hallinto–oikeuteen ja korkeimpaan hallinto–oikeuteen, jotka kuitenkin asettuivat tietosuojavaltuutetun ja tietosuojalautakunnan ottamalle kannalle (KHO 8.1.2010 T 15[292]).

Alan ongelmiin reagoitiin myös lainsäädännöllisesti: ensimmäinen osa uudesta pikaluottoja koskevasta, kuluttajansuojalain (KSL, 38/1978) 7 lukuun sijoitetusta säätelystä tuli voimaan 1.2.2010.[293] Tämän jälkeen keväällä 2010 tietosuojavaltuutettu toteutti yhdessä Kuluttajaviraston kanssa valvontakampanjan, jolla selvitettiin alan toimintatapojen lainmukaisuutta sekä tietosuojan että kuluttajansuojan näkökulmasta. Valvontakampanjan yhteydessä tietosuojavaltuutettu lähetti selvityspyynnön 81 alan yritykselle ja tutustui yritysten verkkosivuihin. Asiakkaiden tunnistamisessa havaitsemiensa puutteiden vuoksi tietosuojavaltuutettu teki 16 alan yrityksiä koskevaa hakemusta, joissa lautakuntaa pyydettiin velvoittamaan kutakin yritystä muuttamaan luotonhakijoiden tunnistamiseen liittyvää toimintatapaansa siten, ettei väärien henkilöiden henkilötietojen käsittely luottohakemuksien käsittelyn yhteydessä olisi mahdollista puutteellisen tunnistamisen seurauksena.[294]

Hakemuksissaan tietosuojavaltuutettu katsoi yritysten käyttämien tunnistamistapojen olleen henkilötietolain huolellisuusvelvoitteen (HetiL 5 §), suunnitteluvelvoitteen (HetiL 6 §) ja virheettömyysvaatimuksen (HetiL 9 §) vastaisia. Yhdestätoista vuonna 2010 vireille tulleesta pikavippiasiasta annettiin päätökset yhdellä kertaa 6.9.2011 (TSL 5–15/2011). Neljän hakemuksen johdosta lautakunta määräsi yrityksen muuttamaan käyttämäänsä tunnistamistapaa sellaiseksi, että se vastaa KSL 7:15:n (746/2010) vaatimuksia. Lopuissa seitsemässä tapauksessa lautakunta katsoi yritysten tunnistavan lainanhakijat lain edellyttämällä tavalla. Yritykset olivat muuttaneet toimintatapojaan tietosuojavaltuutetun tekemien hakemusten jälkeen.

Pikavippiasioiden lisäksi tietosuojavaltuutettu on henkilötietolain voimassaoloaikana saattanut lautakuntaan vain hyvin harvoja asioita. Asiakkaan tunnistaminen verkkopalvelussa on tullut käsiteltäväksi kuitenkin myös toisessa yhteydessä. Päätös TSL 5/2012 koski optiikka–alan yrityksen sähköistä ajanvarauspalvelua, jonka kautta asiakas saattoi varata ajan näöntarkastukseen. Ajanvarauspalvelussa asiakas tunnistettiin vain tämän nimen ja henkilötunnuksen perusteella. Näin kuka tahansa henkilötunnuksen tietävä sivullinen saattoi tarkastella käyttäjän järjestelmästä ilmeneviä tietoja ja esimerkiksi muuttaa käyttäjän tekemää varausta. Lautakunta katsoi, ettei järjestelmää ollut suojattu riittävästi tietojen laatu huomioon ottaen ja määräsi yrityksen muuttamaan tunnistamiskäytäntöään.

---

[292] http://www.tietosuoja.fi/fi/index/ratkaisut/korkeimmanhallinto–oikeudenpaatosns.pikavippiasiassa.html, viitattu 9.5.2014.

[293] Ks. HE 64/2009 vp. KSL:n 7 luvun muutosten ja lisäysten (844/2009) lisäksi paketti sisälsi RL 36:6:n (kiskonta) ja korkolain 4 §:n muutokset (845–846/2009). Tämän sääntelyn korvasi myöhemmin samana vuonna KSL:n 7 luvun kokonaisuudistus (746/2010) ja siihen liittyvät muut lait, joista ks. HE 24/2010 vp.

[294] Ks. Kuluttajaviraston ja tietosuojavaltuutetun tiedotteet *Kuluttajavirasto ja tietosuojavaltuutettu valvovat pikavippiyritysten toimia* (2.2.2010*)* sekä *Kuluttajaviraston ja tietosuojavaltuutetun valvontakampanja: Pikaluottojen tarjonnassa edelleen lainvastaisuuksia* (7.6.2010). Saatavilla http://www.tietosuoja.fi/49706.htm ja http://www.tietosuoja.fi/51009.htm, viitattu 11.12.2013.

Päätöksellä TSL 5/2003 tietosuojalautakunta ratkaisi yhdellä kertaa rekisterinpitäjän lupahakemuksen ja tietosuojavaltuutetun kieltohakemuksen. Tapauksessa oli kyse matkakorttia hakeneiden henkilötunnusten tallettamisesta asiakasrekisteriin, ja sen otsikko kuuluu seuraavasti:

> **TSL 5/2003**. Pääkaupunkiseudun yhteistyövaltuuskunnalla YTV:llä oli oikeus kerätä ja tallettaa matkakortin hakeneiden henkilötunnuksia pääkaupunkiseudun matkakorttiasiakkaiden asiakasrekisteriin. Oikeus johtui YTV:lle laissa säädetystä tehtävästä hoitaa pääkaupunkiseudun joukkoliikenne. Henkilötunnuksen kerääminen oli tarpeellista myös matkustajien oikeusturvan kannalta.

Tietosuojavaltuutettu oli pyytänyt lautakuntaa kieltämään YTV:tä keräämästä ja tallettamasta matkakortin hakeneiden henkilötunnuksia asiakasrekisteriin. Lautakunta katsoi, ettei henkilötunnuksen käsittely ollut henkilötietolain tai sen nojalla annettujen säännösten ja määräysten vastaista. Siten se hylkäsi tietosuojavaltuutetun hakemuksen. YTV:n lupahakemus hylättiin tarpeettomana.

Tietosuojalautakunnan päätökset TSL 1/2004 ja 3/2009 liittyivät verotustietojen julkaisemiseen. Tietosuojavaltuutettu pyysi lautakuntaa kieltämään Satakunnan Markkinapörssi Oy:tä käsittelemästä luonnollisia henkilöitä koskevia verotustietoja Veropörssi–julkaisua varten siinä laajuudessa ja tavalla kuin se on tapahtunut vuoden 2001 verotustietojen osalta, sekä luovuttamasta tietoja edelleen tekstiviestipalvelua varten tai muuhunkaan tarkoitukseen. Ensimmäisellä kertaa lautakunta hylkäsi tietosuojavaltuutetun hakemuksen. Korkeimman oikeuden sittemmin palautettua asian lautakunnalle tietosuojavaltuutetun hakemus tuli toisella kertaa hyväksytyksi.[295]

Päätöksessä TSL 2/2009 oli pääasiassa kyse henkilötietojen suojan ulottumisesta kuolleiden henkilötietoihin. Tietosuojavaltuutetulle oli tullut yksityishenkilöiltä yhteydenottoja avoimessa tietoverkossa olleesta Lepopaikka.fi –sivustosta, jolla oli julkaistu kymmeniätuhansia hautamuistomerkkien kuvia. Kuvia pystyi hakemaan vainajan etunimen, sukunimen sekä entisen sukunimen perusteella, jos ne oli mainittu hautamuistomerkissä. Tietosuojavaltuutettu pyysi tietosuojalautakuntaa kieltämään tietojen käsittelyn, jos henkilön kuolemasta oli kulunut 25 vuotta tai vähemmän eikä vainajan oikeudenomistajien suostumusta tietojen automaattiseen käsittelyyn ollut hankittu.

Tietosuojalautakunnan mukaan sivustoa ylläpitäneellä yrityksellä ei ollut hautakiveen merkityn henkilön tai hänen oikeudenomistajiensa yksiselitteisesti antamaa suostumusta tietojen käsittelyyn, yrityksen suorittamasta henkilötietojen käsittelystä ei säädetty laissa eikä käsittely johtunut laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta. Tämän vuoksi yrityksellä ei ollut henkilötietolain mukaista oikeutta käsitellä hautakivistä ilmeneviä henkilötietoja. Lautakunta katsoi myös, että kysymys ei ollut henkilötietolain 2.4 §:ssä tarkoitetusta henkilötietolain soveltamisalan ulkopuolelle jäävästä henkilörekisteristä, joka

[295] Ks. KHO 2007:9, KHO 2009:82, EYT:n tuomio 16.12.2008, C–73/07 ja III.5.

sisältää vain tiedotusvälineessä julkaistua aineistoa sellaisenaan, kuten yritys oli väittänyt. Niinpä lautakunta asettui tietosuojavaltuutetun kannalle ja antoi tämän hakeman kieltomääräyksen. Yritys valitti kuitenkin asiasta hallinto–oikeuteen, joka otti kielteisemmän kannan kuolleiden henkilötietojen suojaan ja kumosi lautakunnan päätöksen (Helsingin HAO 8.12.2009 T 09/1083/3, lainvoimainen).

Edellisessä alaluvussa jo käsitelty Fonectan katunäkymäpalvelua koskenut tapaus TSL 4/2010 tuli lautakuntaan alun perin juuri tietosuojavaltuutetun kieltohakemuksena. Lautakunta jätti tietosuojavaltuutetun hakeman määräyksen antamatta. Lautakunnan mukaan hakiessaan lupaa henkilötietojen käsittelylle katunäkymäpalvelussaan Fonectan voitiin katsoa oikaisseen sen, mitä oli oikeudettomasti tehty tai laiminlyöty. Kun lupa myönnettiin, ei ollut aihetta velvoittaa Fonectaa ryhtymään enempiin toimiin laiminlyöntinsä korjaamiseksi.

Päätöksessä TSL 6/2012 oli kyse siitä, millä tavoin kansalainen voi toteuttaa henkilötietolain 30 §:ssä turvatun suoramarkkinoinnin kielto–oikeutensa. Olennaisia kysymyksiä olivat, käykö sähköpostin liitteenä toimitettu jäljennös valtakirjasta, ja kävivätkö kyseisestä valtakirjasta ja kieltoilmoituksen välittäneen yhdistyksen viestistä riittävän yksilöidysti ilmi kielto–oikeuden toteuttamiseen tarvittavat tiedot. Lautakunnan vastaus oli myöntävä, joten se hyväksyi tietosuojavaltuutetun hakemuksen ja määräsi puhelinmarkkinointia harjoittaneen teleoperaattorin noudattamaan jo esitettyä kieltoa.

Kuten edeltä käy ilmi, päinvastoin kuin henkilörekisterilain aikana, lähes kaikissa 2000–luvun määräysasioissa kyse on ollut erilaisista Internetissä tai tekstiviestien välityksellä toteutettavista palveluista ja niihin liittyvästä henkilötietojen käsittelystä. Täysin toisenlaisesta, eräällä tavalla hyvin vanhanaikaisesta ja tietoverkoista sekä teknologian kehityksestä erillisestä asiasta oli kuitenkin kyse tapauksessa TSL 3/2013, jossa tietosuojavaltuutettu pyysi tietosuojalautakuntaa kieltämään Jehovan todistajia keräämästä henkilötietoja ilman kyseessä olevien henkilöiden suostumusta ovelta ovelle –saarnaustyössä. Lautakunta kielsikin Jehovan todistajien uskonnollista yhdyskuntaa käsittelemästä henkilötietoja henkilötietolain 8 ja 12 §:ien edellytysten puuttuessa, ja velvoitti uskonnollisen yhdyskunnan omalta osaltaan myös huolehtimaan siitä, ettei henkilötietoja kerätä sen tarkoituksia varten kerätä ilman henkilötietolain edellytysten täyttymistä. Tapaus osoittaa, että vaikka useat henkilötietojen käsittelyä koskevat tulkintatilanteet liittyvätkin nykyään tietoverkkoihin, eivät muunlaiset asiat suinkaan ole menettäneet merkitystään. Myös perinteisiä tiedonkeruu– ja käsittelymenetelmiä ja vakiintuneita käytäntöjä on arvioitava nykyisen lain ja nykyisten tulkintojen valossa.

5. Muutoksenhaku tietosuojalautakunnan päätöksistä

Henkilörekisterilain 38 §:n mukaan tietosuojalautakunnan päätöksiin haettiin muutosta valittamalla korkeimpaan hallinto–oikeuteen. Henkilötietolain 45.1 §:ssä sen sijaan todetaan, että tietosuojalautakunnan 43 ja 44 §:n nojalla tekemään päätökseen haetaan muutosta valittamalla noudattaen, mitä hallintolainkäyttölaissa säädetään, ja että valittajana voi olla

myös tietosuojavaltuutettu. Alun perin viittaus hallintolainkäyttölakiin tarkoitti valitusten ohjaamista lääninoikeuteen. Hallinto–oikeudet ovat sittemmin korvanneet lääninoikeudet. Hallinto–oikeuden päätöksestä voidaan valittaa edelleen korkeimpaan hallinto–oikeuteen.

Muutoksenhakutie on siis pidentynyt, mikä voi olla ongelmallista kahdella tapaa: ensinnäkin lopullisen ratkaisun saaminen voi kestää entistä kauemmin, jos valitustie käydään loppuun. Asiaa on ehkä selvitetty jo pitkään tietosuojavaltuutetun toimistossa ennen huomattavissa määrin tuomioistuinmenettelyä muistuttavaa lautakuntakäsittelyä, jonka jälkeen asia voidaan käsitellä vielä kahdessa oikeusasteessa ilman valituslupaa. Toisaalta jos valitustietä ei käydä loppuun, lopullinen ratkaisu tulee vain harvoin julkaistuksi, sillä hallinto–oikeudet julkaisevat ratkaisujaan huomattavasti harvemmin kuin korkein hallinto–oikeus. Tämä voi olla ongelmallista ratkaisujen ohjaavan merkityksen toteutumisen kannalta.

Finlex–tietokannasta löytyy tätä kirjoitettaessa 21 korkeimman hallinto–oikeuden ratkaisua asioissa, jotka koskevat muutoksenhakua tietosuojalautakunnan päätöksestä. Näistä asioista 18 on henkilörekisterilain ja vain kolme nykyisen henkilötietolain voimassaoloajalta. Tätä selittää paitsi valitustien muuttuminen, myös tietosuojalautakunnan käsittelemien asioiden väheneminen edellisessä alaluvussa kuvattujen toimivallan muutosten seurauksena.

Henkilörekisterilain aikaisista tapauksista 15 koski poikkeuslupa–asioita. Valittajana oli 11 tapauksessa hakemuksen tehnyt rekisterinpitäjä, kolme kertaa tietosuojavaltuutettu. Yhden kerran kyse oli rekisteröidyn ja muun tahon valitusoikeudesta, jonka todettiin puuttuvan. Henkilörekisterilain aikaisista poikkeuslupa–asioista kahdeksassa tietosuojalautakunnan ratkaisu säilyi ennallaan (KHO 1989–A–9, KHO 1989–A–10, KHO 1990–A–3, KHO 1990–A–4, KHO 1990–A–5, KHO 1995–A–11, KHO 1996–A–6, KHO 3.3.1999 T 339). Muissa seitsemässä tapauksessa tietosuojalautakunnan ratkaisua muutettiin tai se kumottiin osittain tai kokonaan (KHO 1989–A–12, KHO 1990–A–6, KHO 6.3.1991 T 770, KHO 1992–A–10, KHO 1992–A–11, KHO 1992–A–29, KHO 1993–A–4). Yleensä asia myös palautettiin tietosuojalautakunnalle (muut paitsi KHO 1989–A–12 ja KHO 6.3.1991 T 770).

Kaksi henkilörekisterilain aikaisista, korkeimman hallinto–oikeuden käsittelemistä tapauksista koski tietosuojavaltuutetun hakemaa, tietosuojalautakunnan antamaa kieltomääräystä. Toinen näistä lautakunnan päätöksistä kumottiin kokonaan (KHO 1995–A–13, ään. 4–1) ja toinen osittain (KHO 1992–A–6, ään. 3–2). Lisäksi yhdessä tapauksessa korkein hallinto–oikeus hylkäsi valituksen tietosuojalautakunnan päätöksestä jättää yritysluottotietoa koskeva virheenoikaisuasia tutkimatta lautakunnan puuttuvan toimivallan vuoksi (KHO 1998:35).

Nykyisen lain aikaisista tapauksista yksi (KHO 2011:16) koski lautakunnan lupatoimivallan laajuutta, jota korkein hallinto–oikeus tulkitsi samoin kuin lautakunta itse ja hylkäsi hakijan valituksen. Kaksi muuta julkaistua ratkaisua (KHO 2007:9 ja KHO 2009:82) liittyvät jo edellä mainittuun, tietosuojavaltuutetun Satakunnan Markkinapörssi Oy:tä vastaan hakemaan kieltomääräykseen verotustietojen julkaisemista koskevassa asiassa. Korkein hallinto–oikeus

kumosi – ennakkoratkaisun Euroopan yhteisöjen tuomioistuimelta hankittuaan[296] – tietosuojalautakunnan päätöksen, jolla lautakunta oli hylännyt tietosuojavaltuutetun hakemuksen, ja palautti asian lautakunnalle kieltomääräyksen antamiseksi.[297]

Korkeimpaan hallinto–oikeuteen lautakunnan päätöksistä on siis päätynyt harva, erityisesti henkilötietolain aikana valitustien muutoksen jälkeen. Korkeimmassa hallinto–oikeudessa noin puolessa käsitellyistä, Finlexissä julkaistuista tapauksista tietosuojalautakunnan ratkaisu on säilynyt ennallaan. On arvioitavissa, että kokonaisuudessaan muutosprosentti on ollut huomattavasti pienempi kuin julkaistujen päätösten osalta.[298] Hallinto–oikeuksien suhtautumista tietosuojalautakunnan päätöksiin ei ole tilastoitu, mutta tietosuojalautakunnan päätökset ovat pysyneet pääsääntöisesti ennallaan muutoksenhaun jälkeenkin. Lautakunnan päätöksistä on myös valitettu melko harvakseltaan.[299] Tämän näyttäisi vähentävän muutoksenhakutien pidentymisestä ja oikeusratkaisujen vähäisemmästä julkaisemista aiheutuvaa haittaa, mutta asettavan toisaalta vaatimuksia lautakunnan päätösten entistä tehokkaammalle ja nopeammalle julkaisemiselle. Hallinto–oikeuksien tai korkeimman hallinto–oikeuden kokonaistyömäärään tietosuojalautakunnan päätöksistä tehdyillä valituksilla ei kuitenkaan siis ole sanottavaa vaikutusta. Tästäkin huolimatta jatkossa voitaisiin arvioida, onko tietosuojalautakunnan käsittelemissä asioissa hallinto–oikeuden päätöksistä tarpeen voida valittaa korkeimpaan hallinto–oikeuteen, tulisiko näissä asioissa mahdollisesti edellyttää valituslupaa, vai olisiko oikeuskäytännön yhtenäisyyden ja menettelyn joutuisuuden vuoksi parasta palata vanhaan valitustiehen ja ohjata valitukset suoraan korkeimpaan hallinto–oikeuteen.

[296] Ks. EYT:n tuomio 16.12.2008, C–73/07.
[297] Ks. edellä III.4.2 ja tietosuojalautakunnan päätökset TSL 1/2004 ja TSL 3/2009.
[298] Selvästi aiheettomia valituksia koskevien päätösten julkaisemiseen ei yleensä ole suurta tarvetta. Finlexissä julkaistujen ratkaisujen lisäksi ks. tietosuojavaltuutetun hakemuksesta ns. pikavippiasiassa annettua määräystä koskeva KHO 8.1.2010 T 15 (julkaistu http://www.tietosuoja.fi/fi/index/ratkaisut/korkeimmanhallinto–oikeudenpaatosns.pikavippiasiassa.html, viitattu 9.5.2014; ei muutosta). Henkilörekisterilain aikaisista julkaisemattomista tapauksista ks. myös KHO 21.11.1997 T 2957 (seloste Tietosuoja 4/97 s. 45; ei muutosta) ja KHO 15.1.1998 T 44 (seloste Tietosuoja 4/98 s. 41–42; lautakunnan lupahakemuksen hylännyt päätös kumottiin). Lisäksi korkein hallinto–oikeus hylkäsi ainakin päätöksistä TSL 17/1989 (KHO 13.3.1991 T 871), TSL 11/1993 (KHO 10.12.1993 T 4970), TSL 21/1993 (KHO 4.11.1994 T 5422) ja TSL 4/1994 (KHO 2.11.1994 T 5377) tehdyt valitukset.
[299] Tietosuojalautakunnan puheenjohtaja Pekka Nurmen haastattelu, 14.10.2013, Helsinki.

IV Johtopäätöksiä ja silmäys tulevaan

1. Tietosuojan viranomaisvalvonnan haasteita

Vaikka lainsäädännölliset uudistukset ovat merkittävästi määrittäneet Suomen tietosuojaviranomaisten kehitystä, tekniset edistysaskeleet ja yleinen verkkoyhteiskuntakehitys ovat myös vaikuttaneet siihen, minkälaisten kysymysten, oikeudellisten ongelmien ja yhteydenottojen kanssa viranomaiset ovat joutuneet tekemisiin. Viranomaistoiminnan alkuaikoina manuaalisesti tai tietokoneella paikallisesti ylläpidetyt henkilörekisterit olivat tietosuojan tärkein sääntelykohde. Nykyään lähes kaikki henkilötietojen käsittely on tietokoneistettua, ja samaan aikaan käsiteltyjen tietojen määrä on kasvanut ja kasvaa edelleen. Tietoverkoista on tullut henkilötietojen siirtämisen tavallisin väylä, ja tiedot liikkuvatkin nykyään usein ja nopeasti valtionrajojen yli jo pelkästään teknisistä syistä. Tietoverkkoja ja yksilöiden Internet–käyttäytymisen valvontaa käytetään myös laajamittaiseen henkilötietojen keräämiseen, *data mining* –toimintaan ja suoranaiseen vakoiluun. Yksityisyyteen ja henkilötietojen suojaan kohdistuvat uhkat ja riskit ovatkin sekä luonteeltaan että mittakaavaltaan varsin erilaisia 2010–luvulla kuin 1980–luvulla. Tämä näkyy selvästi viranomaisten jokapäiväisessä toiminnassa, mikä käy ilmi niin tässä tutkimusraportissa esitellyistä tilastotiedoista kuin tapauksistakin. Samaten niistä käy ilmi kehityksen vaiheittaisuus. Muutos ei ole tapahtunut yhdessä yössä. Toisaalta muutoksen ei voida sanoa olleen hidastakaan, onhan tutkimuksessa tarkasteltu aikaväli vain hieman yli neljännesvuosisadan mittainen.

Tilastoista käy ilmi myös yksittäisiin lainsäädännöllisiin tapahtumiin kytkeytyviä muutoksia niin tietosuojavaltuutetun kuin tietosuojalautakunnankin toimintamuodoissa ja työmäärissä. Erityisen selvänä jakolinjana monessa suhteessa voidaan pitää henkilötietolain voimaantuloa. Henkilötietolaki siirsi toiminnan painopistettä lautakunnan myöntämistä luvista ja jälkikäteisistä reaktioista tietosuojavaltuutetun neuvontaan ja ongelmien ennakointiin, mikä oli myös uuden lain yhtenä tavoitteena. Voimaan tullessaan uusi laki myös välittömästi lisäsi neuvonnan ja informaation tarvetta ja toisaalta lain uudet ilmoitusvelvollisuutta koskevat säännökset nostivat tilapäisesti ilmoitusasioiden määrää. Asiamäärien nopea, jopa kiihtyvä kasvu aivan viime vuosina ei kuitenkaan selity lainsäädännöllisillä muutoksilla vaan edellä mainituilla yhteiskunnalliseen kehitykseen ja toimintaympäristön muutokseen liittyvillä seikoilla. Toisaalta suuri yhteydenottojen määrä kertoo siitä, että tietosuojavaltuutetun toimisto on onnistunut ottamaan paikkansa viranomaistahona, joka tunnetaan laajasti, jonka asiantuntemukseen luotetaan ja johon on matala kynnys ottaa yhteyttä.

Vaikka Suomen nykyinen viranomaismalli ei suinkaan ole ainoa mahdollinen, nykyaikana tuskin enää on mahdollista kyseenalaistaa tietosuojaviranomaisten olemassaolon tarvetta. Valtiontalouden heikosta tilanteesta huolimatta kenenkään mieleen ei tulisi enää ehdottaa

tietosuojaviranomaisten lakkauttamista, kuten eräässä selvitysmiehen raportissa 1990–luvun laman aikaan tehtiin. Tämänlaisen säästöajatuksen estää toki jo Suomea sitova Euroopan unionin oikeus, mutta ennen kaikkea tietosuojan nykyinen valtava käytännön merkitys ja tietosuojan viranomaisvalvonnan ehdoton käytännön välttämättömyys.

Jos tietosuojavaltuutetun, tietosuojavaltuutetun toimiston ja tietosuojalautakunnan toimintaa tarkastellaan puhtaasti kansallisesta näkökulmasta, ei ole havaittavissa sellaisia merkittäviä puutteita tai perustavanlaatuisia ongelmia, jotka vaatisivat viranomaisvalvonnan perusratkaisujen uudelleenmäärittelyä.[300] Yleisesti ottaen nykyinen järjestelmä näyttää ainakin vielä asiamäärien ja tietosuojaan kohdistuvien uhkien lisääntymisestä ja monimutkaistumisesta huolimatta toimivan. Sen sijaan erilaisia pienempiä kehittämistarpeita ja puutteita toiminnassa löytyy luonnollisesti lukuisia. Niihin syynä on usein resurssien puute, toisinaan mahdollisesti myös niiden puutteellinen hyödyntäminen. Tällaisia seikkoja on tuotu ilmi jo tutkimusraportin kahdessa edellisessä osassa. Seuraavassa nostetaan kuitenkin erikseen esille vielä kaksi valvontaviranomaisten toiminnan luonteeseen liittyvää keskeistä ongelmakenttää.

Ensinnäkin ongelmia tuottaa teknologisen ja yhteiskunnallisen kehityksen nopeus. Kun kyse on perus– ja ihmisoikeuksista kuten henkilötietojen suojasta ja yksityisyydestä, jälkikäteinen reagointi ei nykyisen ajattelun mukaan ole riittävää. Ennakoiva strategia on välttämätön, jotta näiden oikeuksien toteutuminen voidaan turvata mahdollisimman hyvin nopeasti muuttuvassa maailmassa. Tietosuojaviranomaiset eivät voi toimia pelkästään jälkikäteen reagoivina lainsoveltajina, vaan niiden on kyettävä myös ennakoimaan, tunnistamaan tulevia riskejä ja ehkäisemään perusoikeusloukkauksia ennen niiden tapahtumista. Nykyisessä suomalaisessa järjestelmässä tietosuojavaltuutettu on selvästi ennakoivaan toimintaan enemmän suuntautuva, omatoiminen ja oma–aloitteinen valvontaviranomainen lautakunnan ollessa lähinnä sille tulevien tapausten ratkaisija. Tietosuojavaltuutetun toimisto käyttääkin valtaosan resursseistaan juuri ennaltaehkäisevään toimintaan.

Ennaltaehkäisevässä toiminnassa on korostunut erityisesti neuvonta, ohjaus, tiedonvälitys ja yhteistyö eri intressitahojen kanssa. Toimiston resurssit esimerkiksi teknologian kehitykseen ja uusiin palveluihin liittyvien riskien tunnistamiseen ja tutkimiseen ovat kuitenkin rajalliset, eikä toimisto käytännössä pysty toimimaan tietosuoja– ja tietoturvaongelmien teknisenä tutkimuslaboratoriona. Monesti uuden teknologian, palvelun tai toimintamallin oikeudellisiin ongelmiin havahdutaan vasta, kun se on jo yleistynyt, ellei kehittäjä oma–aloitteisesti ota yhteyttä toimistoon. Ongelma saattaa myös liittyä ulkomailla kehitettyihin malleihin, jotka tuodaan Suomeen huomioimatta suomalaisen tai eurooppalaisen lainsäädännön vaatimuksia.

Uusien teknologioiden, palvelujen ja toimintamallien kehityksen maailmanlaajuinen seuraaminen olisi tehtävänä mittava ja haastava. Se edellyttäisi paitsi monialaista asiantuntemusta ja tehokasta verkostoitumista niin viranomaisten, yritysmaailman kuin

[300] Nykytilanteessa pelkkä kansallinen tarkastelu ei tietystikään ole riittävää. Tästä lisää jäljempänä.

akateemisten tutkijoiden kanssa, myös suurta taloudellista panostusta, joka ei ainakaan nykyisessä taloustilanteessa vaikuta todennäköiseltä. Jos varsinaisen tietosuoja–asioiden tutkimuslaboratorion resursointiin ei löydy tarpeeksi poliittista tahtoa, joudutaan esimerkiksi uusien henkilötietoihin tavalla tai toisella perustuvien tai liittyvien palveluiden kehittäjille – rekisterinpitäjille ja henkilötietojen käsittelijöille – sälyttämään osa vastuuta. Ajatus ei ole uusi, mutta sitä on tuotu voimakkaasti esille myös ehdotuksessa yleiseksi tietosuoja–asetukseksi. Tätä ilmentävät erityisesti asetusehdotuksen 23 artiklan sisäänrakennettu ja oletusarvoinen tietosuoja ja 33 artiklan mukainen tietosuojaa koskeva vaikutuksenarviointi.

Asetusehdotus kuvastaa myös tietosuojan viranomaisvalvonnan ja tietosuojasääntelyn ehkäpä jopa suurinta ongelmaa. Kansainvälisistä sopimuksista ja suosituksista huolimatta tietosuojalainsäädäntö on loppujen lopuksi ollut kansallista, henkilötietojen väärinkäyttöön kohdistuvat uhkat sen sijaan eivät. Toiminta tietoverkoissa, joissa liikkuu valtava määrä henkilötietoja, ei kunnioita maantieteellisiä rajoja. Valvontaviranomaisten keinot ovat yleensä vähissä rajat ylittävissä tapauksissa. Valvontaviranomaisilla ei ole juurikaan keinoja vaikuttaa ulkomaisiin, ainakaan EU:n ulkopuolisiin rekisterinpitäjiin. Periaatteellisesti merkittävänä ja toivoa antavana poikkeuksena voidaan pitää Euroopan unionin tuomioistuimen tuoretta ratkaisua EUT 13.5.2014, C–131/12, joka näyttää antavan kansalaisille ja tietosuojaviranomaisille tehokkaita keinoja yhdysvaltalaista Google–hakukonetta vastaan siltä osin kun se käsittelee EU–kansalaisten vanhentuneita henkilötietoja. Ratkaisun käytännön merkitystä on kuitenkin vielä kirjoitushetkellä vaikea arvioida. Pääsääntöisesti tietosuojaviranomaisten toimintamahdollisuudet riippuvat edelleen täysin toisten maiden laeista ja niiden viranomaisten yhteistyöhalukkuudesta ja –kykyisyydestä.

Asetuksen tärkeimpänä tavoitteena onkin eurooppalaisen tietosuojalainsäädännön ja viranomaisvalvonnan saaminen aiempaa selvästi yhtenäisemmäksi ja kattavammaksi. Tämä on varmasti askel oikeaan suuntaan. Toisaalta ei ole syytä kuvitella, että pelkkä eurooppalainen harmonisointi riittäisi poistamaan kaikki maailmanlaajuisten tietoverkkojen perusluonteeseen liittyvät tietosuojaongelmat. Niinpä kansainväliset tietosuojakysymykset tulevat säilymään myös eurooppalaisten hallitusten ja tietosuojaviranomaisten haasteena, jonka ratkaisemiseen on pohdittava useita erilaisia toimintamalleja.

2. Tietosuoja–asetus ja viranomaisten uudet tehtävät

Jo moneen otteeseen mainitulla Euroopan unionin tulossa olevalla yleisellä tietosuoja–asetuksella tulee olemaan lähivuosina suuri vaikutus tietosuojaviranomaisten toimintaan kaikissa jäsenvaltioissa, myös Suomessa. Siksi on myös tämän tutkimusraportin lopuksi syytä luoda nopea katsaus ehdotuksen keskeisimpiin tietosuojaviranomaisten toimintaa sääteleviin säännöksiin.

Lähtökohtana on, että asetuksessa tullaan säätelemään paitsi tietosuojan aineellista sisältöä myös sen viranomaisvalvontaa huomattavasti tarkemmin kuin nykyisessä direktiivissä. Asetus

tulee tuomaan kansallisille tietosuojaviranomaisille merkittäviä uusia tehtäviä. Näihin kuuluvat erityisesti sanktioiden määrääminen sekä henkilötietojen tietoturvaloukkauksista tehtävien ilmoitusten käsitteleminen.

Valvontaviranomaisten tehtävistä ja toimivallasta yleisesti säädetään asetusehdotuksen VI luvun 2 jaksossa (artiklat 51–54). Toimivallan jaossa pääsääntönä on, että kukin kansallinen viranomainen on toimivaltainen omalla alueellaan. Kuitenkin kun rekisterinpitäjä tai käsittelijä toimii useassa maassa tai käsittelee useiden eri valtioiden kansalaisten tietoja, toimii rekisterinpitäjän pääasiallisen toimipaikan viranomainen vastuullisena, kaikissa jäsenvaltioissa toimivaltaisena valvojana tämän rekisterinpidon suhteen. Rekisteröidyllä on toisaalta oikeus tehdä rekisterinpitäjän toiminnasta valitus minkä tahansa jäsenvaltion viranomaiselle.

Tehtävien ja valtuuksien määrittely on varsin yksityiskohtaista. Osin tehtävät ovat sellaisia, joista tietosuojavaltuutettu huolehtii jo nykyisen kansallisen lainkin nojalla ja puitteissa. Komission ehdottaman 52 artiklan 1 kohdan mukaan valvontaviranomainen:

> a) valvoo tämän asetuksen soveltamista ja varmistaa sen;
>
> b) käsittelee rekisteröidyn tai tätä 73 artiklan mukaisesti edustavan yhdistyksen tekemiä valituksia, tutkii mahdollisuuksien mukaan asiaa ja ilmoittaa rekisteröidylle tai yhdistykselle asian etenemisestä sekä valitusta koskevasta ratkaisustaan kohtuullisen ajan kuluessa, erityisesti jos asia edellyttää lisätutkimuksia tai koordinointia toisen valvontaviranomaisen kanssa;
>
> c) jakaa tietoa ja tarjoaa keskinäistä apua muille valvontaviranomaisille ja varmistaa tämän asetuksen johdonmukaisen soveltamisen täytäntöönpanon;
>
> d) suorittaa tutkimuksia omasta aloitteestaan tai valituksen perusteella tai toisen valvontaviranomaisen pyynnöstä ja, jos rekisteröity on tehnyt valituksen tälle valvontaviranomaiselle, ilmoittaa rekisteröidylle tutkimusten tuloksesta kohtuullisen ajan kuluessa;
>
> e) seuraa erityisesti tieto– ja viestintäteknologian sekä kauppatapojen asiaan liittyvää kehitystä, siltä osin kuin sillä on vaikutusta henkilötietojen suojaan;
>
> f) esittää jäsenvaltioiden toimielimille ja elimille näkemyksiään yksilön oikeuksien ja vapauksien suojelua henkilötietojen käsittelyssä koskevista lainsäädännöllisistä ja hallinnollisista toimenpiteistä;
>
> g) hyväksyy 34 artiklassa tarkoitetut käsittelytoimet ja antaa niistä lausuntoja;
>
> h) antaa lausunnon käytännesääntöjen luonnoksista 38 artiklan 2 kohdan mukaisesti;
>
> i) hyväksyy yritystä koskevat sitovat säännöt 43 artiklan mukaisesti;
>
> j) osallistuu Euroopan tietosuojaneuvoston toimintaan.

Lisäksi saman artiklan 2 kohdan mukaan kaikkien valvontaviranomaisten on edistettävä henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, takeista ja oikeuksista tiedottamista kansalaisille. Erityisesti on kiinnitettävä huomiota lapsille suunnattuihin toimiin. 3 kohdan mukaan valvontaviranomaisen on pyynnöstä autettava rekisteröityä käyttämään tässä asetuksessa vahvistettuja oikeuksia ja tarvittaessa tehtävä tätä varten yhteistyötä muiden jäsenvaltioiden valvontaviranomaisten kanssa. Artiklassa on kaikkiaan kuusi kohtaa.

Tietosuojaviranomaisen valtuuksia koskeva 53 artikla on yhtä laaja ja yksityiskohtainen kuin tehtävät määrittävä 52 artikla. Sen mukaan tietosuojaviranomainen muun muassa voi tarvittaessa määrätä rekisterinpitäjän tai käsittelijän korjaamaan tekemänsä rikkomukset, noudattamaan rekisteröidyn asetukseen perustuvien oikeuksien käyttöä koskevia pyyntöjä ja antamaan tehtäviensä suorittamiseen tarvittavat tiedot, sekä antaa rekisterinpitäjälle tai käsittelijälle huomautuksen, kieltää käsittelyn väliaikaisesti tai lopullisesti, ja antaa lausuntoja henkilötietojen suojaan liittyvistä kysymyksistä.

Ehdotetun 79 artiklan mukaan jokaisella laissa tarkoitetulla kansallisella valvontaviranomaisella tulee olemaan mahdollisuus langettaa asetuksen säännösten rikkojalle hallinnollisia sanktioita, joita ovat kirjallinen varoitus, säännölliset tarkastukset ja hallinnolliset sakot. Euroopan parlamentin hyväksymässä versiossa sakon ylärajaa on nostettu alkuperäisestä komission ehdotuksesta 100 000 000 euroon tai 5 prosenttiin yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta.

Erityisesti sanktioinnin osalta muutos nykyiseen olisi merkittävä, sillä kansallisessa järjestelmässä ainoa tietosuojaviranomaisille mahdollinen, käytännössä harvoin käytetty sanktio on ollut uhkasakkolain mukainen uhkasakko.[301] Nykyisessä henkilötietolain järjestelmässä sanktioiden roolin voidaankin todeta olevan vähäinen. Tietosuoja–asetus siirtäisi viranomaistoiminnan painopistettä ennakollisesta vaikuttamisesta ainakin hieman jälkikäteistä sanktiointia kohden. Toisaalta myös ennakollisen vaikuttamisen keinoja on pyritty tehostamaan ehdotuksen 33 artiklan mukaisen tietosuojaa koskevan vaikutusarvioinnin ja 34 artiklan mukaisen ennakkohyväksyntä– ja ennakkokuulemismenettelyn myötä. Lisäksi asetusehdotuksessa korostuu entistä enemmän myös tietosuojaviranomaisten nopea reaktiovalmius ja sitä kautta vahinkojen ehkäisy ja minimointi: ehdotuksen 31 artiklassa asetetaan rekisterinpitäjälle velvollisuus ilmoittaa tapahtuneesta henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle ilman aiheetonta viivytystä. Näihin ilmoituksiin on myös ilmoituksen vastaanottavan viranomaisen kyettävä reagoimaan nopeasti.

Asetuksen mukaisten tehtävien jakautuminen kansallisille valvontaviranomaisille ei tätä kirjoitettaessa ole vielä selvillä. On kuitenkin oletettavaa, että tehtävät tullaan Suomessa antamaan lähinnä tietosuojavaltuutetun toimistolle, joka tullee olemaan myös asetusehdotuksen 46 artiklassa tarkoitettu yhteyspisteenä toimiva viranomainen. On ajateltavissa oleva mahdollisuus, että tietosuojalautakunta jatkaisi toimintaansa kutakuinkin

[301] Henkilötietolain 46 §:n mukaan tietosuojavaltuutettu voi langettaa uhkasakon valvonnan mahdollistavan tietojenantovelvollisuuden taikka tarkastusoikeutta tai tiedon korjaamista koskevan päätöksensä noudattamisen tehosteeksi, ei sen sijaan jälkikäteiseksi seuraukseksi lainvastaisesta henkilötietojen käsittelystä yleisesti. Sähköisen viestinnän tietosuojalain 41 §:ssä säädetään lisäksi, että tietosuojavaltuutettu voi kyseisen lain 32 §:ssä tarkoitettuja tehtäviä hoitaessaan velvoittaa lain rikkojan korjaamaan virheensä tai laiminlyöntinsä, sekä asettaa velvoitteen noudattamisen tehosteeksi uhkasakon tai uhan, että tekemättä jätetty toimenpide teetetään asianomaisen kustannuksella. Niin ikään tietosuojalautakunta voi mainitun henkilötietolain pykälän mukaan langettaa uhkasakon tietojenantovelvollisuuden taikka tekemänsä päätöksen tehosteeksi. Ks. *Pitkänen – Tiilikka – Warma*, Henkilötietojen suoja (2013) s. 274–275.

nykyiseen tapaan myös asetuksen tultua voimaan, sillä asetus ei suinkaan tee tyhjäksi kaikkea kansallista lainsäädäntöä. Viestintävirastolle asetuksen valvonnassa mahdollisesti annettava rooli olisi erittäin ongelmallinen, sillä on selvää, ettei Viestintävirasto organisaationsa ja toimintatapojensa vuoksi täytä ainakaan EU–oikeuden itsenäisyysvaatimusta, johon asetuksessa on vieläpä kiinnitetty entistä enemmän huomiota.

Kunhan asetuksen lopullinen muoto on selvillä, on Suomessakin syytä kriittisesti arvioida, onko nykyinen, sinänsä hyväksi havaittu kaksijakoinen viranomaismalli tehokkain ja paras tapa suoriutua sekä asetuksen että jäljelle jäävän kansallisen tietosuojalainsäädännön valvonnasta. Samalla on syytä pohtia myös sitä, kuinka paljon verkkoyhteiskuntaan siirtyneen oikeusvaltion tulisi olla valmis panostamaan tietosuojan viranomaisvalvontaan ja sen asianmukaiseen resursointiin. Ennen kaikkea lainvalmistelijoiden, poliitikkojen ja viranomaisten itsensä on syytä säilyä valppaina muuttuvassa maailmassa, jotta kansalaisten henkilötietojen suoja olisi jatkossa taattu parhaalla mahdollisella tavalla.

APPENDIX:
FINLAND 17TH
ARTICLE 29 WORKING PARTY ANNUAL REPORT 2013

FINLAND

A. Summary of activities and news

As part of the implementation of the strategy of the Office of the Data Protection Ombudsman during the year under review, we restructured our personnel planning system and integrated our internal competence management programme more thoroughly into the system. To ensure continued success in a volatile operating environment, we must secure the quality and quantity of internal competencies. Other cornerstones of our strategy include the ability to predict the impact of new phenomena and to prioritise our measures, the utilisation of information as a steering tool, and the formation of necessary alliances while retaining our independence and impartiality.

The Office also succeeded in achieving the level required by the Government decree on information security. As part of the effort, the entire personnel was obligated to take an information security test. Information security training is a permanent part of our competence management programme.

We initiated measures to launch an entirely new service function, information services, and to restructure our personnel. Development of internal information management forms a part of this path. I believe that the greater part of issues raised with us have already been commented or acted upon by us earlier. Efficient management of resources and continued maintenance of the service level require that we focus on essential issues.

Independent of the completion of the data protection regulation or directive, we are aware that there is a dire need of competence in our country to be able to fill the increasing number of positions opening up for Privacy Officers. Therefore, we launched an internal survey to investigate our potential of creating a brand for the required training. This product development effort is to be carried out in cooperation with educational organisations in accordance with our strategy.

As part of striving towards maximum effectiveness, we continued our business sector– and phenomenon–specific surveys. These surveys concerned targets such as telephone services financed through advertising, the payday loan industry, commercial use of personal data, and website information security surveyed in international cooperation (Sweep Day).

Consistency mechanism and international cooperation were practiced in cooperation with our Norwegian colleagues by launching a joint audit of a global online music services conglomerate. The audit was completed during the current year.

Our areas of emphasis included data protection of entrepreneurs. Entrepreneurs have been targeted by a variety of forced selling operations. To ensure legal protection, the proper balance of information between the parties of the dispute is important. Within our sphere of competence, we supported the Federation of Finnish Enterprises in conquering the problem.

Biobanks were introduced as a new target group among the Data Protection Ombudsman's personal data protection duties. National Supervisory Authority for Welfare and Health (Valvira) will act as the primary supervising authority.

Organisation	
Chair and/or College	Reijo Aarnio has been the Data Protection Ombudsman since 1 st November 1997.
Budget	The overall annual budget is € 1 708 000.
Staff	The total number of staff is 20.
General Activity	
Decisions, opinions, recommendations	3157
Notifications	535
Prior checks	see notifications
Requests from data subjects	958
Complaints from data subjects	(access and rectifications) 269
Advice requested by parliament or government	127
Other relevant general activity information	Cooperation work with data controllers in the following sectors: Education, Health Care, Social Affairs, Telecommunications, Employment and Economy, Marketing
Inspection Activities	
Inspections, investigations	119
Sanction Activities	233
Sanctions	N/A
Penalties	N/A
DPOs	
Figures on DPOs	>1000

B. Information on case–law

POLICE CASES

It became publically known that personal data of the President of Russia had been recorded into the information system of the Finnish police. At the same time, investigations were in progress concerning the unauthorised viewing of the data of a deceased Olympic gold medallist. The investigation led to dozens of employees of the police being found guilty of a violation of the provisions of personal data file legislation. The situation threatened to affect public trust in the police and the position of the commanding officers of the Finnish police. My personal view is that the chain of command within the police from the top to the officers who process information is too long and requires the inclusion of supervision carried out closer to the actual operations.

FOOD SAFETY

Frequent shopper systems have traditionally gathered information on the consumers' shopping habits at a general level with the consumers' permission. Product–specific information has not been gathered. The Finnish Food Safety Authority Evira was informed of the possibility that a product sold by a retail chain with a frequent shopper system had contained toxic Datura stramonium, leading to consumers having to seek medical treatment at hospitals. Based on Article 19 of the general European food regulation (Regulation (EC) No 178/2002 of the European Parliament and of the Council), Evira required that the retail operator takes measures to connect the frequent shopper system's information to the shop's purchase data in order to warn the consumers who had purchased the product in question. It was revealed that the shop was indeed able to connect these data. This resulted in lively discussion concerning the credibility of frequent shopper systems and, on the other hand, the relationship between data protection and product safety.

AFFILIATE MARKETING

The Act on the Protection of Privacy in Electronic Communications states that prior consent is required for electronic direct marketing targeted at consumers. To circumvent this unambiguous rule, affiliate marketing has been developed. In affiliate marketing, the actual marketing measure is taken by a company operating in an opt–out country, for example. The company that wishes to sell its products purchases marketing services from the other company, but claims not to purchase personal data processing services or personal data content. In one type of affiliate marketing operations, publishing space is purchased from another company's marketing communication materials or other communication materials. The Data Protection Ombudsman intervened in these operations. Codes of conduct concerning such marketing actions are now being prepared together with the direct marketing industry.

DEFINITION OF A CONTROLLER OF A PERSONAL DATA FILE

It has come to my attention that the representatives of a religious group have visited homes and collected personal data, neglecting to observe the obligations set out in the Personal Data Act. The issue was not whether the denomination is allowed to gather data as part of its operations, but who was responsible for the data collection operations as the controller. The denomination denied its responsibility and explained that the case concerned use of personal data for domestic purposes for which the Personal Data Act does not apply. My view of the matter differed from this, and the Data Protection Board, which acted as competent authority in the matter, shared my view. The denomination appealed against the decision at an administrative court.

C. Other important information

The new ecosystem of mobile communications set an increasing challenge to data protection and the position and rights of consumers on a more general level. Smartphones have taken us to the age of apps, or applications. Processing of personal data is moving from traditional central register files to increasingly complicated systems where large numbers of applications are run over the operating systems of devices connected to a network infrastructure.

In this context, a national cyber security strategy was issued in Finland.

The Ministry of Transport and Communications carried out a survey of the current Big Data theme, and the Ministry of Finance appointed a working group to implement an open data programme. Operators continued to suffer from the deficient transfer of information between authorities. To remove the part of the problem that is due to the lack of an overall information system architecture, it was decided that a new authority to employ more than a thousand people (Valtori) would be established as a corrective measure. Similarly, the citizens' service channel was developed, partly based on Estonian experience.

The legislative framework concerning the protection of personal data has been continuously developed. On the other hand, the process has increased our supervisory duties. The adequacy, or more appropriately, the scarcity of our resources seems to be a permanent condition, based on the survey carried out in connection with the NETSO project and pending publication.

The Information Society Code legislation project led by the Ministry of Transport and Communications proceeded swiftly. The project also raised the issue of net neutrality, or whether all Internet communications should continue to flow freely or should the operators, for example, have the right to give priority to some messages, i.e. those that are paid for with higher rates.

The report by Professor Ahti Saarenpää discussed, in accordance with the assignment, the potential need of a positive credit record. The rapporteur reached the conclusion that it would be better to first observe the impact of the European data protection regulation on the processing of financial information. On the other hand, the rapporteur proposed that credit records should be identified as one of society's fundamental data files, resulting in special statutory privileges being allocated to it.

Emotions were also raised by the work of the road traffic taxation working group chaired by Mr Ollila. I was opposed to real–time tracking of drivers and proposed that when data is required for use as a basis for taxation, it should be collected in a distributed manner.

A survey carried out by us showed that nearly all telecommunication operators who offer mobile subscriptions to consumers also offer an option with partial financing through advertising. The consumer consents to receiving advertisements in exchange for a discount on call prices. According to consumer authorities, a telephone is a necessity. The Data Protection Directive defines consent as a one–sided, withdrawable legal act. Consumers frequently subscribed to a service partially financed through the reception of advertisements, and then immediately withdrew their consent. The Data Protection Ombudsman established that in the case of such necessity product, the consent cannot constitute part of the customer agreement, but must be considered a separate declaration of intent instead. As a result, operators developed a special double pricing system.

Communication of necessary information to the public constitutes one of the biggest challenges of data protection. To relay correct and well–timed information, a restructuring of our website was in process in 2013. We also participated in the development of the overall concept of the Tietosuoja magazine and made a decision to establish an information service group.

MEMBERS OF THE ART. 29 DATA PROTECTION WP IN 2013

Austria	Belgium
Mrs. Eva Souhrada–Kirchmayer (from July 2010) Mrs Waltraut Kotschy (till June 2010) Austrian Data Protection Commission (Datenschutzkommission) Hohenstaufengasse 31 – AT – 1014 Wien Tel: +43 1 531 15 / 2525 Fax: +43 1 531 15 / 2690 E–mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Mr Willem Debeuckelaere Commission for the protection of privacy (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute, 139 – BE – 1000 Bruxelles Tel: +32(0)2/213.85.40 Fax : +32(0)2/213.85.65 E–mail: commission@privacycommission.be Website: http://www.privacycommission.be/
Bulgaria	**Cyprus**
Mr Krassimir Dimitrov Commission for Personal Data Protection –CPDP (Комисия за защита на личните данни) 15 Acad. Ivan Evstratiev Geshov blvd. Sofia 1431 Republic of Bulgaria Tel. + 359 2 915 35 31 Fax: + 359 2 915 35 25 E–mail: kzld@cpdp.bg Website: http://www.cdpd.bg	Mrs Panayiota Polychronidou Commissioner for Personal Data Protection (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2nd floor – CY – 1082 Nicosia (P.O. Box 23378 – CY – 1682 Nicosia) Tel: +357 22 818 456 Fax: +357 22 304 565 E–mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy
Czech Republic	**Denmark**
Mr Igor Nemec Office for Personal Data Protection (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 – CZ – 170 00 Praha 7 Tel: +420 234 665 111 Fax: +420 234 665 501 E–mail: posta@uoou.cz Website: http://www.uoou.cz/	Mrs Janni Christoffersen Danish Data Protection Agency (Datatilsynet) Borgergade 28, 5th floor – DK – 1300 Koebenhavn K Tel: +45 3319 3200 Fax: +45 3319 3218 E–mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk

Estonia	Finland
Mr Viljar Peep Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) 19 Väike–Ameerika St., 10129 Tallinn Tel: +372 627 4135 Fax: +372 627 4137 e–mail: info@]aki.ee or international@aki.ee Website: http://www.aki.ee	Mr Reijo Aarnio Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) Ratapihantie 9, 6th floor – FIN – 00521 Helsinki (P.O. Box 800) Tel: +358 295 666 700 Fax: +358 295 666 735 E–mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi
France	**Germany**
Mr Alex Türk Chairman President of the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés – CNIL) Rue Vivienne, 8 –CS 30223 FR – 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 Mr Georges de La Loyère French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés – CNIL) Rue Vivienne, 8 –CS 30223 FR – 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E–mail: laloyere@cnil.fr Website: http://www.cnil.fr	Mr Peter Schaar The Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) Husarenstraße 30 – DE –53117 Bonn Tel: +49 (0) 228 99–7799–0 Fax: +49 (0) 228 99–7799–550 E–mail: poststelle@bfdi.bund.de Website: http://www.datenschutz.bund.de Mr. Alexander Dix (representing the German States / Bundesländer) The Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit) An der Urania 4–10 – DE – 10787 Berlin Tel: +49 30 13 889 0 Fax: +49 30 215 50 50 E–mail: mailbox@datenschutz–berlin.de Website: http://www.datenschutz–berlin.de

Greece	Hungary
Mr Christos Yeraris Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1–3, PC 115 23 Athens – Greece Tel: +30 210 6475608 Fax: +30 210 6475789 E–mail: christosyeraris@dpa.gr Website: http://www.dpa.gr	Mr András Jóri Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary (Adatvédelmi Biztos) Nador u. 22 – HU – 1051 Budapest Tel:+36 1 475 7186 Fax: +36 1 269 3541 E–mail: adatved@obh.hu Website: www.adatvedelmibiztos.hu
Ireland	**Italy**
Mr Billy Hawkes Data Protection Commissioner (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE –Co.Laois Tel: +353 57 868 4800 Fax:+353 57 868 4757 E–mail: info@dataprotection.ie Website: http://www.dataprotection.ie	Mr Francesco Pizzetti Italian Data Protection Authority (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 – IT – 00186 Roma Tel: +39 06.69677.1 Fax: +39 06.69677.785 E–mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Website: http://www.garanteprivacy.it
Latvia	**Lithuania**
Mrs Signe Plumina Data State Inspectorate of Latvia (Datu valsts inspekcija) Blaumana street 11/13–15 Riga, LV–1011 Latvia e–mail: info@dvi.gov.lv website: www.dvi.gov.lv Tel: + 371 67223131	Mr Algirdas Kunčinas State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) A.Juozapaviciaus str. 6 / Slucko str. 2, LT–01102 Vilnius Tel: +370 5 279 14 45 Fax: + 370 5 261 94 94 E–mail: ada@ada.lt Website: http://www.ada.lt

Luxembourg	Malta
Mr Gérard Lommel National Commission for Data Protection (Commission nationale pour la Protection des Données – CNPD) 41, avenue de la Gare – L – 1611 Luxembourg Tel: +352 26 10 60 –1 Fax: +352 26 10 60 – 29 E–mail: info@cnpd.lu Website: http://www.cnpd.lu	Mr Joseph Ebejer Information and Data Protection Commissioner Office of the Information and Data Protection Commissioner 2, Airways House High Street Sliema SLM 1549 MALTA Tel: +356 2328 7100 Fax: +356 23287198 E–mail: joseph.ebejer@gov.mt Website: http://www.idpc.gov.mt
The Netherlands	**Poland**
Mr Jacob Kohnstamm Dutch Data Protection Authority (College Bescherming Persoonsgegevens – CBP) Visiting address (only with an appointment): Juliana van Stolberglaan 4–10 2595 CL DEN HAAG Postal address: P.O. Box 93374 2509 AJ DEN HAAG Tel: +31 70 8888500 Fax: +31 70 8888501 E–mail: info@cbpweb.nl Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl	Mr Wojciech Rafał Wiewiórowski Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 – PL – 00193 Warsaw Tel: +48 22 860 7312; +48 22 860 70 81 Fax: +48 22 860 73 13 E–mail: desiwm@giodo.gov.pl Website: http://www.giodo.gov.pl
Portugal	**Romania**
Mr Luís Novais Lingnau da Silveira National Commission of Data Protection (Comissão Nacional de Protecção de Dados – CNPD) Rua de São Bento, 148, 3º PT – 1 200–821 Lisboa Tel: +351 21 392 84 00 Fax: +351 21 397 68 32 E–mail: geral@cnpd.pt Website: http://www.cnpd.pt	Mrs Georgeta Basarabescu National Supervisory Authority for Personal Data Processing (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, RO – Bucharest Tel: +40 21 252 5599 Fax: +40 21 252 5757 E–mail: georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Website: www.dataprotection.ro
Slovakia	**Slovenia**
Mr Gyula Veszelei Office for the Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky)	Mrs Natasa Pirc Musar Information Commissioner (Informacijski pooblaščenec) Vošnjakova 1, SI – 1000 Ljubljana

Odborárske námestie 3 – SK – 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441 E–mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	Tel: +386 1 230 97 30 Fax: +386 1 230 97 78 E–mail: gp.ip@ip–rs.si Website: http://www.ip–rs.si
Spain	**Sweden**
Mr José Luis Rodriguez Álvarez Spanish Data Protection Agency (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES – 28001 Madrid Tel: +34 91 399 6219/20 Fax: + +34 91 445 56 99 E–mail: director@agpd.es Website: http://www.agpd.es	Mr Göran Gräslund Data Inspection Board (Datainspektionen) Fleminggatan, 14 (Box 8114) – SE – 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E–mail: datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
United Kingdom	**European Data Protection Supervisor**
Mr Christopher Graham Information Commissioner's Office Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel: +44 1625 545700 Fax: +44 1625 524510 E–mail: please use the online enquiry form on our website Website: http://www.ico.gov.uk	Mr Peter Hustinx European Data Protection Supervisor – EDPS Postal address: 60, rue Wiertz, BE – 1047 Brussels Office: rue Montoyer, 63, BE – 1047 Brussels Tel: +32 2 283 1900 Fax: +32 2 283 1950 E–mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

Observers of the Art. 29 Data Protection Working Party in 2013

Iceland	Norway
Mrs Sigrun Johannesdottir Data Protection Authority (Persónuvernd) Raudararstigur 10 – IS – 105 Reykjavik Tel: +354 510 9600 Fax: +354 510 9606 E–mail: postur@personuvernd.is Website: http://www.personuvernd.is	Kim Ellertsen Director, Head of Legal Departement Data Inspectorate (Datatilsynet) P.O.Box 8177 Dep – NO – 0034 Oslo Tel: +47 22 396900 Fax: +47 22 422350 E–mail: postkasse@datatilsynet.no Website: http://www.datatilsynet.no
Liechtenstein	**Republic of Croatia**
Mr Philipp Mittelberger Data Protection Commissioner Data Protection Office (Datenschutzstelle, DSS) Kirchstrasse 8, Postfach 684 – FL –9490 Vaduz Tel: +423 236 6090 Fax: +423 236 6099 E–mail: info@dss.llv.li Website http://www.dss.llv.li	Mr. Franjo Lacko Director Mrs Sanja Vuk Head of department for EU and Legal Affairs Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka – AZOP) Republike Austrije 25, 10000 Zagreb Tel. +385 1 4609 000 Fax +385 1 4609 099 e–mail: azop@azop.hr or info@azop.hr website: http://www.azop.hr/default.asp
the former Yugoslav Republic of Macedonia	
Mr Dimitar Gjeorgjievski Directorate for Personal Data Protection (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tel: +389 2 3230 635 Fax: +389 2 3230 635 E–mail: info@dzlp.mk Website: www.dzlp.mk	

Secretariat of the Art. 29 Working Party

Mrs. Marie–Hélène Boulanger
Head of unit
European Commission
Directorate–General Justice
Data Protection Unit
Office: MO59 02/13 – BE – 1049 Brussels
Tel: +32 2 295 12 87
Fax: +32 2 299 8094
E–mail: JUST–ARTICLE29WP–SEC@ec.europa.eu
Website: http://ec.europa.eu/justice/data–protection/index_en.htm

BIBLIOGRAPHY

1. $500 Million Worth Of Bitcoin Has Been Stolen Since 2010 (2014) seen on: http://www.businessinsider.com/how–many–bitcoins–have–been–stolen–2014–3#ixzz3BJEkXrZx
2. 'Bitcoin is a currency': Federal judge says the virtual cash is real money (2013) seen on: http://www.nbcnews.com/tech/tech–news/bitcoin–currency–federal–judge–says–virtual–cash–real–money–f6C10874611
3. "The World's First Freedom of Information Act", published by the Chydenius Foundation (2006) available at: http://www.chydenius.net/pdf/worlds_first_foia.pdf.
4. "Growing the Digital Business: Accenture Mobility Research 2015. Saatavilla, http://www.slideshare.net/fullscreen/AccentureDigital/mobility–research–2015–digital–overview–final/3.
5. 35th International Conference of Data Protection and Privacy Commissioners – Privacy: A Compass in Turbulent World, Warsaw 23–26 September 2013: verkkosivut. Saatavilla https://privacyconference2013.org. Viitattu 14.11.2013.
6. Aalto–yliopisto. "Tuhannet automaatiolaitteet Suomessa haavoittuvia kyberhyökkäyksille". 20.03.2013. Saatavilla, www.aalto.fi/fi/current/news/view/2013–03–20/.
7. Aarnio, Reijo. Data Protection Ombudsman. Helsinki, 5.5.2014.
8. Adrian Blundell–Wignall (2014), 'The Bitcoin Question Currency Versus Trust–Less Transfer Technology', OECD Working Papers on Finance, Insurance and Private Pensions, No. 37.
9. Ajibola Ogunbadewa (2014), 'The Virtues and Risks Inherent in the 'Bitcoin' Virtual Currency', seen on: http://ssrn.com/abstract=2425114 on 2014.09.08.
10. Alapuranen, Leena. Henkilötietojen käsittelyn yleiset lähtökohdat. Teoksesta: Henkilötietojen käsittely työelämässä. Muut kirjoittajat: Koskinen Seppo, Heino Anna Maija ja Salli Minna. Edita Publishing Oy 2005.
11. Álvaro Núñez Vaquero (2013), 'Five Models of Legal Science', Revus, No. 19.
12. Andreasson Ari & Koivisto Juha. Tietoturvaa toteuttamassa. Tietosanoma. Tallinna 2013.
13. Arkistolaitoksen www–sivut: www.arkisto.fi (11.11.2015).
14. Article 1, as to the Consolidated version of the Treaty on European Union and the

Treaty on the Functioning of the European Union. http://eur–lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:EN:HTML.

15. Article 29 Working Party (WP 29): Opinion 4/2007 on the concept of personal data. WP 136. Adopted on 20th June. Brussels 2007. Available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> [23.5.2014].
16. Article 29 Working Party (WP 29): Web site. Available at <http://ec.europa.eu/justice/data–protection/article–29/index_en.htm> [16.4.2014].
17. Avgöranden. Saatavilla http://www.tietosuoja.fi/sv/index/ratkaisut.html. Viitattu 9.5.2014.
18. Ball, J. NSA monitored calls of 35 world leaders after US official handed over contacts, 25 October 2013, http://www.theguardian.com/world/2013/oct/24/nsa–surveillance–world–leaders–calls/ (access September 2015),
19. Barnes, S. B., A privacy paradox: Social networking in the United States, First Monday, Volume 11, Number 9 – 4 September 2006, http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523 (access September 2015),
20. Barzallo – Valdés – Reyes Olmedo – Amoroso Fernándes (eds.) XVI Congreso Iberoamericano de Derecho e Informatica (2012)
21. Barzallo, J. Luiz, Valdes, J. Tellez, Olmedo, P. Reyes, Fernandez, Y. Amoroso (ed.), XVI Congreso Iberoamericano de Derecho e Informatica, Quito 2012,
22. Beaud, Michel (2001) A History of Capitalism, 1500–2000. New York: Monthly Review Press.
23. Benjamin Wallace (2011), 'The Rise and Fall of Bitcoin', Wired Magazine.
24. Bert–Jaap Koops, 'The Crypto Controversy – A Key Conflict in the Information Society', (Kluwer Law International, Hague 2001).
25. Bitcoin price index chart 2013–2014, seen on: http://www.coindesk.com/price/
26. Bitcoin Taxes on: https://bitcointaxes.info/faq
27. Bitcoin: Decentralized, Peer–to–peer, Cryptocurrency (2011) seen on: http://cs.stanford.edu/people/eroberts/cs201/projects/2010–11/DigitalCurrencies/advantages/index.html
28. Boettger, Larry. The Morris Worm: How it Affected Computer Security and Lessons Learned by it. SANS Reading Room. 24.12.2000. (Saatavilla: http://www.giac.org/paper/gsec/405/morris–worm–affected–computer–security–

lessons–learned/100954, 16.11.2016).
29. BSI:n (British Standards Institution) www–sivut (Saatavilla: http://www.bsigroup.com, 10.11.2015).
30. Bucher, Eugen 1988: Schweizerisches Obligationenrecht. Allgemeiner Teil. 2. Auflage. Zürich: Schulthess.
31. Bygrave, L., Data Protection Law: Approaching its Rationale, Logic and Limits, Kluwer Law International 2002,
32. Bygrave, L.A.: Data Protection Law: Approaching Its Rationale, Logic and Limits. The Hague: Kluwer Law International. 2002.
33. Bygrave, L.A.: The body as data? Reflections on the relationship of data privacy law with the human body. Available at: http://www.privacy.vic.gov.au/privacy/web2.nsf/files/body–as–data–conference–2003–lee–bygrave–presentation/$file/conference_03_no2.pdf
34. Case C–288/12. Commission v Hungary, Judgment of 8 April 2014.
35. Case C–518/07. Commission v Germany, Judgment of 9 March 2010.
36. Case C–614/10. Commission v Austria, Judgment of 16 October 2012.
37. Case C–73/07. Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, Judgment of 16 December 2008.
38. Cashing in on Cybercrime: New Malware Target Bitcoin (2012) seen on: http://www.trendmicro.de/media/misc/spotlight–cybercrime–cashing–in–on–bitcoin–en.pdf on 2014.09.10.
39. Cate, F., Dempsey, J., Rubinstein, I., Systematic government access to private–sector data, International Data Privacy Law, volume 2, number 4, 2012,
40. Cavoukian, A., El Emam, K., Introducing Privacy–Protective Surveillance: Achieving Privacy and Effective Counter–Terrorism, September 2013, http://www.privacybydesign.ca/content/uploads/2013/12/pps.pdf (access September 2015),
41. Cavoukian, A.: Public Safety is Paramount – But Balanced Against Privacy. Available at: http://www.ipc.on.ca/images/Resources/public–safety–e.pdf
42. CEN/ISSS (European Committee for Standardisation/ Information Society Standardisation System) lisätietoa EU:n IDABC:n www–sivuilta (Saatavilla: http://ec.europa.eu/idabc/en/document/6990.html, 10.11.2015).
43. CERT/CC:n (CERT Coordination Center) www–sivut: www.cert.org (16.11.2015).
44. CERT–EU, tietoa meistä. CERT–EU:n www–sivut: http://cert.europa.eu (Saatavilla:

http://cert.europa.eu/cert/plainedition/en/cert_about.html, 16.11.2015)
45. Cf. Wikipedia s.v. Meaning (philosophy of language).
46. Cfr. Lauritsen Liberty, Justice and Legal automata in address http://www.kentlaw.iit.edu/Documents/Institutes%20and%20Centers/CAJT/88–3_09_Liberty_Justice_and_Legal_Automata.pdf
47. Cfr. Reiling Information Technology in the courts in Europe pp 601–616, where Dory Reiling also does open different points of view to analyse e–justice.
48. Christopher Mann and Daniel Loebenberger (2014), Realizing Two–Factor Authentication For The Bitcoin Protocol soon on: https://eprint.iacr.org/2014/629.
49. Cindy Williamson, Jason Vazquez, Jason Thomas, Katherine Sagona–Stophel (2013), Thomson Reuters Accelus Report –'Technology in the Fight Against Money Laundering in the New Digital Currency Age' seen on: http://accelus.thomsonreuters.com/sites/default/files/GRC00403_0.pdf
50. Commission staff working document SEC(2011) 1552 final; https://ec.europa.eu/digital–agenda/en/news/commission–notice–guidelines–recommended–standard–licences–datasets–and–charging–re–use.
51. Commodity on: http://www.investorwords.com/975/commodity.html
52. Communication on Open Data, http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/open_data.pdf.
53. Council of Europe, Treaty Office: verkkosivut. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 108 (lista sopimukseen liittyneistä valtioista). Saatavilla http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG. Viitattu 30.9.2013.
54. Court of Justice of the European Union PRESS RELEASE No 106/15, Luxembourg, 23 September 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015–09/cp150106en.pdf (access September 2015)
55. Court of Justice of the European Union PRESS RELEASE No 117/15, Luxembourg, 6 October 2015, Judgment in Case C–362/14, Maximillian Schrems v Data Protection Commissioner, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015–10/cp150117en.pdf (access October 2015)
56. Crouch, Colin (2004) Post–Democracy. Cambridge: Polity.
57. Curran, James (2011) Media and Democracy. Abingdon: Routledge.

58. Dahrendorf, Ralf (1959) Class and Class Conflict. Stanford: Stanford University Press.
59. Danton Bryans (2014), 'Bitcoin and Money Laundering: Mining for an Effective Solution', Indiana Law Journal, Vol. 89, No. 441.
60. Datainspektionen (Åland): Web site. Available at <http://www.di.ax> [20.5.2014].
61. Datainspektionen (Sweden): Årsredovisning 2012. Stockholm 2013. Available at <http://www.datainspektionen.se/Documents/arsredovisning–2012.pdf> [6.5.2014].
62. Datainspektionen, Åland: verkkosivut: http://www.di.ax. Viitattu 20.3.2014.
63. Datainspektionen, Sverige: Årsredovisning 2012. Stockholm 2013. Saatavilla http://www.datainspektionen.se/Documents/arsredovisning–2012.pdf. Viitattu 6.5.2014.
64. Datatilsynet (Denmark): Datatilsynets årsberetning 2012. København 2013. Available at <http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsberetninger/Aarsberet_2012.pdf> [6.5.2014].
65. Datatilsynet (Norway): Årsmelding for 2013. Hva rører seg på personvernfeltet – og hva har Datatilsynet gjort i året som gikk. Oslo 2014. Available at <http://www.datatilsynet.no/Global/04_planer_rapporter/aarsmelding/Aarsmelding_2013.pdf> [6.5.2014].
66. Datatilsynet, Danmark: Datatilsynets årsberetning 2012. København 2013. Available at http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsberetninger/Aarsberet_2012.pdf. Viitattu 6.5.2014.
67. Datatilsynet, Norge: Årsmelding for 2013. Hva rører seg på personvernfeltet – og hva har Datatilsynet gjort i året som gikk. Oslo 2014. Saatavilla https://www.datatilsynet.no/Global/04_planer_rapporter/aarsmelding/Aarsmelding_2013.pdf. Viitattu 6.5.2014.
68. David Kinley, 'Money: A Study of the Theory of the Medium of Exchange', (Macmillan, London 1904).
69. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: verkkosivut. Informationsfreiheit – Dienststelle – Aufgaben. Saatavilla http://www.bfdi.bund.de/IFG/Dienststelle/Aufgaben/Aufgaben_node.html. Viitattu 20.3.2014.
70. Diffie, W., Landau, S., Privacy on the Line. The Politics of Wiretapping and Encryption. Updated and Expanded Edition, MIT 2007,
71. Digitaalistrategia: Euroopan komissio tarkastelee jäsenvaltioiden suojautumista tietoverkko-hyökkäyksiltä European Commission – IP/11/395 01/04/2011 (Saatavilla:

http://europa.eu/rapid/press–release_IP–11–395_fi.htm,16.11.2015).

72. Digitalisaatio, valtiovarainministeriön www–sivut (Saatavilla: http://vm.fi/digitalisaatio, 16.11.2015).
73. Digitalisaation viisi tasoa: 1. yksittäiset manuaaliset prosessit on korvattu digitaalisilla, mutta järjestelmät eivät keskustele keskenään; 2. tieto kulkee sähköisesti organisaation sisällä; 3. tieto kulkee sähköisesti organisaatioiden välillä; 4. organisaation prosessit on muokattu hyödyntämään digitalisaatiota; 5. koko liiketoimintaekosysteemi tai toimitusketju on muokattu IT:tä ja digitalisaation mahdollisuuksia hyödyntäväksi. Ks. Venkatraman. IT enabled business transformation: From automation to business scope redefinition. MIT Sloan Management Review.
74. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309/15.
75. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319/2.
76. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, OJ L 267/7.
77. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304/64.
78. Discourse on the Method of Rightly Conducting One's Reason and of Seeking Truth, http://www.literature.org/authors/descartes–rene/reason–discourse/chapter–02.html…
79. Dixon, H., Warman, M., Google gets 'right to be forgotten' requests hours after EU ruling, May 14, 2014, http://www.telegraph.co.uk/technology/google/10832179/Google–gets–right–to–be–forgotten–requests–hours–after–EU–ruling.html (access September 2015),
80. Does Marginal Cost Pricing of Public Sector Information Spur Firm Growth?', Heli Koski, The Research Institute of the Finnish Economy. http://www.etla.fi/files/2696_no_1260.pdf.

81. Duménil, Gérard & Dominique Lévy (2013) The Crisis of Neoliberalism. Harward: Harward University Press.
82. ec.europa.eu/information_society/policy/psi/docs/pdfs/implementation/fi_trans_19990621.pdf.
83. EESSI:n (Electronic Exchange of Social Security Information) www–sivut (Saatavilla: http://ec.europa.eu/social/main.jsp?catId=869&langId=fi, 10.11.2015).
84. Ehdotus Euroopan parlamentin ja neuvoston asetukseksi: yksilöiden suojelusta
85. Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko– ja tietoturvan varmistamiseksi koko unionissa COM(2013) 48 final – 2013/0063 (COD) (Saatavilla: http://eur–lex.europa.eu/legal–content/FI/TXT/PDF/?uri=CELEX:52013PC0048&from=EN, 16.11.2015 ja http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0027(COD), 16.11.2015).
86. Eight Business Model Archetypes for PSI Re–Use by Osella – Ferro,www.w3.org/2013/04/odw/odw13_submission_27.pdf; Open growth Stimulating demand for open data in the UK – by Deloitte's and The Open Data Institute, http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/deloitte–analytics/open–growth.pdf; Open data business models, by Jeni Tennison, www.theodi.org; D. Girardi, M. Palmirani, Legal Issues and Economic Exploitation of Open Government Data, "Jusletter IT" 15. Mai 2013; C. Bonina, New business models and the value of open data: definitions, challenges and opportunities, http://www.nemode.ac.uk/wp–content/uploads/2013/11/Bonina–Opendata–Report–FINAL.pdf; Magalhaes, Roseira, Manley, Business models for open government data, opendata500.thegovlab.org/files/Business_Models_for_OGD.pdf.
87. E–money seen on: http://ec.europa.eu/internal_market/payments/emoney/index_en.htm
88. Ervasti, Kaijus: Eräitä näkökohtia empiirisen tiedon hyväksikäyttämisestä oikeustieteessä. Lakimies 3/1998, s. 364–388.
89. ETSI:n (European Telecommunications Standards Institute) www–sivut (Saatavilla: http://www.etsi.org, 10.11.2015).
90. ETSK, Euroopan talous– ja sosiaalikomitea, Täysistunnossa 15.–16. Helmikuuta 2007 annetut lausunnot, Bryssel 23. helmikuuta 2007, s. 6 (Saatavilla: http://www.eesc.europa.eu/resources/docs/grf_ces25–2007_d_fi.pdf, 16.11.2015).
91. EU Banks Must Shut Bitcoin Until Rules in Place, EBA Says (2014), seen on: http://www.bloomberg.com/news/2014–07–04/eu–banks–must–shun–bitcoin–until–

rules–in–place–eba–says.html

92. Euroopan komissio: Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja–asetus). COM(2012) 11 final. Bryssel 2012. Saatavilla http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FI:PDF. Viitattu 28.1.2014.
93. Euroopan komissio: Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta. COM(2012) 10 final. Bryssel 2012. Saatavilla http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:FI:PDF. Viitattu 28.1.2014.
94. Euroopan Kommissio. “EU Cybersecurity plan to protect open internet and online freedom and opportunity”. 7.2.2013. Saatavilla URL: http://europa.eu/rapid/press–release_IP–13–94_en.htm.
95. Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, (EYVL nro L 008 12.1.2001).
96. Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, sähköisen viestinnän tietosuojadirektiivi (EYVL L 201, 31.7.2002).
97. Euroopan parlamentin ja neuvoston direktiivi 2003/98/EY, annettu 17 päivänä marraskuuta 2003, julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (EUVL nro L 345, 31.12.2003).
98. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, henkilötietodirektiivi (EYVL L 281, 23.11.1995).
99. Euroopan talous– ja sosiaalikomitealle ja alueiden komitealle, Turvallisen tietoyhteiskunnan strategia – "Lisää vuoropuhelua, yhteistyötä ja vaikutusmahdollisuuksia" (KOM(2006) 251 lopullinen) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:FI:PDF,

16.11.2015).

100. Euroopan tietosuojavaltuutettu: verkkosivut. Data protection – Glossary – J. Saatavilla https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/pid/79. Viitattu 16.1.2014.
101. Euroopan verkkorikostorjuntakeskus toiminut vuoden, Bryssel 10. helmikuuta 2014 (Saatavilla: http://europa.eu/rapid/press–release_IP–14–129_fi.htm, 16.11.2015).
102. European Central Bank (2012), 'Virtual Currency Schemes' (European Central Bank, Frankfurt am Main).
103. European Central Bank seen on: http://europa.eu/about–eu/institutions–bodies/ecb/index_en.htm on 2014.09.02.
104. European Commission – IP/99/953, Bryssel, 8. joulukuuta 1999. (Saatavilla: http://europa.eu/rapid/press–release_IP–99–953_fi.htm, 11.11.2015). G8 Declaration, Renewed Commitment for Freedom and Democracy, G8 Summit of Deauville, toukokuu 26.–27.2011 (Saatavilla: http://news.dot–nxt.com/2011/05/27/g8–declaration, 16.11.2015).
105. European Commission: A Digital Agenda for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2010) 245 final/2. Brussels 2010. Available at <http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> [30.1.2014].
106. European Commission: Progress on EU data protection reform now irreversible following European Parliament vote. MEMO/14/186. Press release. Strasbourg, 12 March 2014. Saatavilla http://europa.eu/rapid/press–release_MEMO–14–186_en.htm. Viitattu 20.3.2014.
107. European Commission: Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final. Brussels 2012. Available at <http://ec.europa.eu/justice/data–protection/document/review2012/com_2012_11_en.pdf> [30.1.2014].
108. European Commission: verkkosivut. Enlargement – TAIEX. http://ec.europa.eu/enlargement/taiex/index_en.htm. Viitattu 1.4.2014.
109. EVPSI & LAPSI Final Meeting Turin, 9–10/7/2012 Eleonora Bassi University of Turin. In this work are indicated the recommended tools in order to fulfil the EDPS purposes such as: PETs, Privacy by Design, Anonymisation, Privacy Policies, PIA,

Codes of Conduct, Guidelines, Anonymisation by Default. www.lapsi–project.eu.
110. FinCEN, Guidance – Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (2013) seen on: http://fincen.gov/statutes_regs/guidance/html/FIN–2013–G001.html.
111. Finland: Act on Openness of Government Activities: ec.europa.eu/information_society/policy/psi/docs/pdfs/implementation/fi_trans_19990621.pdf.
112. Finlex: Web site. Available at <http://www.finlex.fi> [7.4.2014].
113. Finnish Mass Media (2012) Joukkoviestimet 2011 – Finnish Mass Media. Kulttuuri ja viestintä – Culture and the media 2012. Helsinki: Statistics Finland.
114. FISC:n (Finnish Information Security Cluster) www–sivut (Saatavilla: http://fisc.fi/, 14.11.2015).
115. Frågor. Saatavilla http://www.tietosuoja.fi/sv/index/useinkysyttya.html. Viitattu 9.5.2014.
116. Frank Tudor, 'Making Money with Bitcoins, Litecoins and Other', (Smashwords Inc., Los Gatos CA 2014).
117. Friedmann, Hermann 1900: Die unkörperliche Sache. Zur systematik des Privatrechts. Nach einem Vortrage. Basel: R. Reich Buchhandlung.
118. Friedmann, Hermann 1904: Die Konvergenz der Organismen. Eine empirisch begründete Theorie als Ersatz für die Abstammungslehre. Berlin 1904: Gebrüder Paetel.
119. Friedmann, Hermann 1925: Die Welt der Formen. System eines morphologischen Idealismus. Berlin: Paetel.
120. Friedmann, Hermann 1950: Sinnvolle Odyssee. Geschichte eines Lebens und einer Zeit 1873–1950. München: C. H. Beck.
121. G8 Principles for Protecting Critical Information Infrastructures, toukokuu 2003 (Saatavilla: http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf, 16.11.2015).
122. Garfinkel, S: Database Nation: The Death of Privacy in the 21st Century. Published by O´Reilly Media, Inc. 2000.
123. Gottwald (ed), Festschrift für Martin Schneider: neu bei Editions Weblaw (2014).
124. Greenstein, S. (ed.), Vem reglerar informationssamhället?, Stockholm 2010,
125. Grossman, L., The Secret Web: Where Drugs, Porn and Murder Live Online,

November 11, 2013, http://time.com/630/the–secret–web–where–drugs–porn–and–murder–live–online/ (access September 2015),

126. Hakala M, Vainio M & Vuorinen O. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell 2006.
127. Hal Varian on how the Web challenges managers http://www.mckinsey.com/client_service/business_technology
128. Hallintomenettelyn perusteet (2008)
129. Hallituksen kärkihanke: Digitaalisen liiketoiminnan kasvuympäristön rakentaminen, LVM:n www–sivut (Saatavilla: http://www.lvm.fi/web/hanke/digitalisaatio, 11.11.2015).
130. Hallituksen kärkihanke: Norminpurku, LVM:n www–sivut (Saatavilla: http://www.lvm.fi/hanke/norminpurku, 11.11.2015).
131. Harsági, Digital Technology and the Character of Civil Procedure pp. 122–133 in Kengyel – Nemessányi (eds) Electronic Technology and Civil Procedure New Paths to Justice from Around the World New Paths to Justice from Around the World (2012) .
132. HaVM 26/1998 vp. Hallintovaliokunnan mietintö hallituksen esityksestä henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi (HE 96/1998 vp). Helsinki 1998.
133. HE 122/2008 vp. Hallituksen esitys Eduskunnalle laeiksi viestintämarkkinalain 15 a §:n ja sähköisen viestinnän tietosuojalain 39 §:n muuttamisesta.
134. HE 137/2000 vp. Hallituksen esitys eduskunnalle laiksi henkilötietolain muuttamisesta. Helsinki 2000.
135. HE 139/2012 vp Hallituksen esitys eduskunnalle Suomen ja Pohjois–Atlantin liiton kesken vaihdettavan tiedon suojaamisesta tehdyn hallinnollisen järjestelyn hyväksymisestä sekä laiksi järjestelyn ja Pohjois–Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.
136. HE 146/1998 vp. Holhoustoimilain 67 §:n 2 momenttia ei tarkennettu samalla, kun lain 88 §:ään vaihdettiin ilmaisu ”…siten kuin viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään”. Muutos tuli voimaan 1.11.2007. Myös 88 §:ssä oli aiemmin ilmaisu ”… siten kuin siitä erikseen säädetään.” Ks. muutoksen perusteluista HE 52/2006 vp. s. 55
137. HE 153/2006 vp. Hallituksen esitys eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain,

pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta.
138. HE 169/2009 vp. Hallituksen esitys eduskunnalle maksupalvelulaiksi ja eräiksi siihen liittyviksi laeiksi. Helsinki 2009.
139. HE 176/1999 vp. Hallituksen esitys eduskunnalle laiksi tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain 6 §:n muuttamisesta. Helsinki 1998.
140. HE 19/2008 vp. Hallituksen esitys eduskunnalle laeiksi yksityisyyden suojasta työelämässä annetun lain muuttamisesta ja henkilötietolain muuttamisesta annetun lain voimaantulosäännöksen 2 momentin kumoamisesta. Helsinki 2008.
141. HE 202/2010 vp. Hallituksen esitys eduskunnalle laiksi henkilötietolain 2 §:n 4 momentin kumoamisesta. Helsinki 2010.
142. HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi
143. HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö– ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta. Helsinki 2013.
144. HE 232/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.
145. HE 24/2010 vp. Hallituksen esitys eduskunnalle laeiksi kuluttajansuojalain muuttamisesta ja eräiden luotonantajien rekisteröinnistä sekä eräiksi niihin liittyviksi laeiksi. Helsinki 2010.
146. HE 241/2006 vp. Hallituksen esitys eduskunnalle luottotietolaiksi ja siihen liittyviksi laeiksi. Helsinki 2006.
147. HE 246/2010 vp. Hallituksen esitys eduskunnalle laeiksi julkisen hallinnon tietohallinnon ohjauksesta sekä viranomaisten toiminnan julkisuudesta annetun lain 18 ja 36 §:n muuttamisesta. Helsinki 2010.
148. HE 286/2010 vp. Hallituksen esitys eduskunnalle syyttäjälaitosta koskevan lainsäädännön uudistamiseksi. Helsinki 2010.
149. HE 30/1998 vp. Hallituksen esitys eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi (Julkisuuslaki). Helsinki 1998.
150. HE 30/1998 vp., Wallin – Konstari: Julkisuus– ja salassapitolainsäädäntö (2000) s. 257, Kulla: Hallintomenettelyn perusteet (2008) s. 333 ja Mäenpää: Julkisuusperiaate (2009) s. 153
151. HE 309/1992 vp. Hallituksen esitys Eduskunnalle perustuslakien

perusoikeussäännösten muuttamisesta. Helsinki 1992.
152. HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.
153. HE 309/1993 vp. Hallituksen esitys eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta. Helsinki 1993.
154. HE 311/1993 vp. Hallituksen esitys eduskunnalle laeiksi henkilörekisterilain ja yleisten asiakirjain julkisuudesta annetun lain 18 a §:n muuttamisesta sekä laiksi tietosuojalautakunnasta ja tietosuojavaltuutetusta. Helsinki 1993.
155. HE 49/1986 vp. Hallituksen esitys Eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi. Helsinki 1986.
156. HE 49/1986 vp. Hallituksen esitys eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi. Helsinki 1986.
157. HE 53/2010 vp. Hallituksen esitys Eduskunnalle laeiksi kansainvälisistä tietoturvallisuusvelvoitteista annetun lain sekä viestintähallinnosta annetun lain 2 §:n muuttamisesta.
158. HE 57/1989 vp. Hallituksen esitys eduskunnalle nimikirjalaiksi ja laiksi henkilörekisterilain 7 §:n 5 kohdan kumoamisesta. Helsinki 1989.
159. HE 57/2013 vp. Hallituksen esitys eduskunnalle turvallisuusselvityslaiksi sekä siihen liittyviksi laeiksi.
160. HE 64/2009 vp. Hallituksen esitys eduskunnalle laeiksi kuluttajansuojalain 7 luvun, rikoslain 36 luvun 6 §:n ja korkolain 4 §:n muuttamisesta. Helsinki 2009.
161. HE 72/2002 vp. s. 89
162. HE 94/1993 vp. Hallituksen esitys eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi. Helsinki 1993.
163. HE 96/1998 vp. Hallituksen esitys eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi (Tietosuojalaki). Helsinki 1998.
164. HE 96/1998 vp. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.
165. HE 96/1998 vp. Hallituksen esitys eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Helsinki 1998.
166. Heino, Petteri. Pilvipalvelut. Talentum. Kariston Kirjapaino Oy Hämeenlinna 2010.
167. Helpman, Elhanan. 1998. General Purpose Technologies and Economic Growth. The MIT Press tai Liikenne– ja viesintäministeriön julkaisu ”Digitalisaatio keskisuurissa

yrityksissä". 14/2014, http://www.lvm.fi/c/document_library/get_file?folderId=3082174&name=DLFE–24299.pdf&title=Julkaisuja%2014–2014.

168. Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma) Työryhmän loppuraportti. Sisäasiainministeriön julkaisuja 32/2010. (Saatavilla: http://www.intermin.fi/download/16144_Identiteettiohjelman_loppuraportti.pdf, 16.11.2015),
169. henkilötietojen käsittelyssä. Tietosanoma Oy. Tallinna 2010.
170. henkilötietojenkäsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja–asetus) COM(2012) 11 Final, annettu 25.1.2012.
171. Henkilötietolain (1999/523) 3 §:n mukaan henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.
172. Herberger E–justice Kompetenz: Plädoyer für einAusbildungskonzept in Gottwald (ed), Festschrift für Martin Schneider: neu bei Editions Weblaw (2014).
173. Hietanen E-Justice in Finland – Trends and Challenges pp 757–770 in Gottwald (ed), Festschrift für Martin Schneider: neu bei Editions Weblaw (2014).
174. Hoeren Eine kontraktualistische Konzeption der Informationsgerechtigkeit; Rechtstheorie 34 (2003)
175. How is all this bitcoin theft happening (2013), http://bitcoin.stackexchange.com/questions/5162/how–is–all–this–bitcoin–theft–happening
176. http://blogs.microsoft.com/on–the–issues/2015/01/28/data–privacy–day–2015–putting–people–control/ (access September 2015)
177. http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
178. http://digital–era.net/active–surveillance–program–xk–eyscore/ (access September 2015)
179. http://dublincore.org/ Dublin Core is one important vocabulary for assigning metadata to the sources in the Web.
180. http://ec.europa.eu/digital–agenda/en/open–data–0
181. http://ec.europa.eu/digital–agenda/en/our–goals/pillar–i–digital–single–market.
182. http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf

183. http://ec.europa.eu/justice/criminal/european–e–justice/portal/index_en.htm
184. http://ec.europa.eu/justice/news/consulting_public/0003/contributions/citizens/kilian_wolfgang_en.pdf (access September 2015)
185. http://e–estonia.com/component/x–road
186. http://en.ilmatieteenlaitos.fi/open–data–licence.
187. http://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects (access September 2015)
188. http://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX:32013L0037.
189. http://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX:52011DC0882.
190. http://eur–lex.europa.eu/legal–content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.
191. http://eurovoc.europa.eu/.
192. http://globetrotter.berkeley.edu/people/Castells/castells–con4.html (access September 2015)
193. http://lod–cloud.net/.
194. http://lumiaconversations.microsoft.com/2015/01/28/stop–think–connect–safeguarding–online–reputation/ (access September 2015)
195. http://net–security.org/secworld.php?id=15328 (access September 2015)
196. http://networksociety.org/about (access September 2015)
197. http://opendatacommons.org/licenses/odbl/
198. http://opendatahandbook.org/.
199. http://opendatahandbook.org/guide/en/.
200. http://opendatahandbook.org/guide/en/what–is–open–data/
201. http://opendatahandbook.org/guide/en/what–is–open–data/.
202. http://opendefinition.org/licenses/.
203. http://opendefinition.org/ofd/.
204. http://tomgruber.org/writing/ontology–definition–2007.htm
205. http://webarchive.nationalarchives.gov.uk/20130109092234/http://number10.gov.uk/news/letter–to–government–departments–on–opening–up–data/.
206. http://www.economist.com/news/technology–quarterly/21590766–virtual–currency–it–mathematically–elegant–increasingly–popular–and–highly
207. http://www.europeana.eu/portal/.
208. http://www.fatf–gafi.org/countries/
209. http://www.finlex.fi/en/

210. http://www.formez.it/iodl/.
211. http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf (access September 2015)
212. http://www.ictparliament.org/node/2040.
213. http://www.informationshield.com/ (access September 2015)
214. http://www.informationshield.com/usprivacylaws.html(access September 2015)
215. http://www.law.wm.edu/academics/intellectuallife/researchcenters/clct/
216. http://www.maanmittauslaitos.fi/en/NLS_open_data_licence_version1_20120501.
217. http://www.microsoft.com/security/online–privacy/prevent.aspx (access September 2015)
218. http://www.nationalarchives.gov.uk/doc/open–government–licence/version/2/.
219. http://www.oecd.org/sti/ieconomy/privacy.htm (access September 2015)
220. http://www.oed.com/view/Entry/151596?redirectedFrom=privacy (access September 2015)
221. http://www.refworld.org/docid/3ddcafaac.html, 16.11.2015)
222. http://www.staysafeonline.org/ (access September 2015)
223. http://www.teamliquid.net/forum/general/229525–nsfw–exploring–the–hidden–internet–deep–web/ (access September 2015)
224. http://www.tietosuoja.fi/49706.htm, viitattu 11.12.2013.
225. http://www.tietosuoja.fi/51009.htm, viitattu 11.12.2013.
226. http://www.tietosuoja.fi/fi/index/useinkysyttya.html. Viitattu 9.5.2014.
227. http://www.ulapland.fi/InEnglish/Units/Faculty–of–Law/Institutes/Institute–for–Law–and–Informatics/NETSO–Project (access September 2015)
228. http://www.w3.org/2009/Talks/0204–ted–tbl.
229. http://www.w3.org/DesignIssues/LinkedData.html.
230. http://www.w3.org/Metadata/.
231. http://www.w3.org/People/Berners–Lee/
232. http://www.w3.org/TR/prov–o/.
233. http://www.w3.org/TR/vocab–adms/.
234. http://www.w3.org/TR/vocab–dcat/.
235. http://www.w3.org/wiki/LinkedData.
236. http://www.whitehouse.gov/open/documents/open–government–directive.
237. http://www.xe.com/currencyconverter/
238. https://bitcoin.org/en/how–it–works Bitcoin under pressure (2013)

239. https://en.wikipedia.org/wiki/Semantic_Web_Stack.
240. https://googleonlinesecurity.blogspot.fi/2014/07/announcing–project–zero.html (access September 2015)
241. https://joinup.ec.europa.eu/software/page/eupl/licence–eupl.
242. https://www.aclu.org/about–aclu–0 (access September 2015)
243. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207772/Open_Data_Charter.pdf
244. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207772/Open_Data_Charter.pdf
245. https://www.staysafeonline.org/data–privacy–day/ (access September 2015)
246. https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
247. Huoltovarmuuskeskuksen www–sivut (Saatavilla: www.huoltovarmuus.fi, 20.11.2013).
248. Husa – Pohjolainen: Julkisen vallan oikeudelliset perusteet (2014) s. 35
249. Huuhtanen, Heidi. Tietoyhteiskuntaa rakentamassa. TIEKE Tietoyhteiskunnan kehittämiskeskus ry. Helsinki 2001.
I. Kant's Critique of Pure Reason, Translated by N.K. Smith, London 1929; Kritik der reinen Vernunft: Ein großer Theil und vielleicht der größte von dem Geschäfte unserer Vernunft besteht in Zergliederungen der Begriffe, die wir schon von Gegenständen haben. Dieses liefert uns eine Menge von Erkenntnissen, die, ob sie gleich nicht weiter als Aufklärungen oder Erläuterungen desjenigen sind, was in unseren Begriffen (wiewohl noch auf verworrene Art) schon gedacht worden, doch wenigstens der Form nach neuen Einsichten gleich geschätzt werden, wiewohl sie der Materie oder dem Inhalte nach die Begriffe, die wir haben nicht erweitern, sondern nur auseinander setzen.
250. IETF:n (Internet Engineering Task Force) www–sivut (Saatavilla: http://www.ietf.org, 10.11.2015).
251. Information Commissioner, Republic of Slovenia: verkkosivut. Competencies – Access to Information. Saatavilla https://www.ip–rs.si/index.php?id=338. Viitattu 20.3.2014.
252. Information Commissioner's Office, The United Kingdom: verkkosivut. What we cover. Saatavilla http://ico.org.uk/what_we_cover. Viitattu 20.3.2014.
253. Information systems Act: Act on the national information systems of the law court administration (2010).
254. International review of criminal policy – United Nations Manual on the prevention and control of computer–related crime

(http://www.uncjin.org/Documents/EighthCongress.html, viitattu 20.11.2013)
255. IRS Rules Bitcoin Is Property, Not Currency seen on: http://techcrunch.com/2014/03/25/irs–rules–bitcoin–is–property–not–currency
256. ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä. SFS:n www–sivut, ISO/IEC 27000 Tietoturvallisuuden hallinta (Saatavilla: http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta, 10.11.2015).
257. ISO/IEC 27001 (Saatavilla: http://www.sfs.fi/ajankohtaista/tuoteuutiset/uusi_versio_tietoturvastandardista_iso_iec_27001.1777.news, 10.11.2015)
258. ISO:n www–sivut: http://www.iso.org/, 10.11.2015.
259. Italy: Law 241/90 on Administrative Procedure and Access to Administrative Documents:
260. ITU–T lyhyesti, ITU:n www–sivut, About ITU–T (Saatavilla: http://www.itu.int, 10.11.2015).
261. Jack Weatherford, 'The History of Money', (Three Rivers Press, New York 1997).
262. Juan C. Zarate (2013), 'Conflict by Other Means – The Coming Financial Wars', Parameters, Vol. 43, No. 4.
263. Jyränki, Antero: Toiset työt, toiset metodit. Teoksessa Häyhä, Juha (toim.): Minun metodini. WSLT, Porvoo 1997, s. 74–89.
264. Kanninen, Heikki. Euroopan yhteisön oikeuden normihierarkia ja kansallinen lainsoveltaja. Teoksesta: Puhuri käy, muuttuva suomalainen ja eurooppalainen valtiosääntömme. Toimittaneet: H. Kanninen, H. Koskinen, A. Rosas, M. Saksin ja K. Tuori. Edita. Helsinki 2009.
265. Kansallinen turvallisuusviranomainen. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje 30.11.2010. (Saatavilla: http://formin.finland.fi/public/download.aspx?ID=68032&GUID=%7B25313BDA–49BD–43EF–B106–3E9CE01AF6B0%7D, viitattu 13.11.2013).
266. Katsaus kyberturvallisuuteen vuonna 2014 (Saatavilla: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/02/ttn201502021446.html, 14.11.2015).
267. Katsh Digital Lawyers: Orienting The Legal Profession To Cyberspace, 55 Pitt Law Review (1994).
268. Kekkonen, Jukka: Oikeudellisen muutoksen tutkimisesta – minun metodini. Teoksessa

Häyhä, Juha (toim.): Minun metodini. WSLT, Porvoo 1997, s. 131–150.
269. KHO 13.11.2008 T 2861
270. KHO 18.8.2006 T 1976
271. KHO 1989–A–10
272. KHO 1989–A–12
273. KHO 1989–A–9
274. KHO 1990–A–3
275. KHO 1990–A–4
276. KHO 1990–A–5
277. KHO 1990–A–6
278. KHO 1992–A–10
279. KHO 1992–A–11
280. KHO 1992–A–29
281. KHO 1992–A–6
282. KHO 1993–A–4
283. KHO 1995–A–11
284. KHO 1995–A–13
285. KHO 1996–A–6
286. KHO 1998:35
287. KHO 2007:9
288. KHO 2009:82
289. KHO 2011:16
290. KHO 2012:51
291. KHO 23.4.2001 T 926
292. KHO 27.2.2007 T 457
293. KHO 27.9.2013 T 3084
294. KHO 3.3.1999 T 339
295. KHO 6.3.1991 T 770
296. Kindt, E.J.: Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis. Springer. Netherlands 2013.
297. Kleemola, Maija: Katsaus tietosuojavaltuutetun toimiston 15 vuoteen. Tietosuoja 1/2003, s. 4–9.
298. KM 1972:B 31. Tietosuojatoimikunnan mietintö. Helsinki 1972.
299. KM 1974:110. Tietojärjestelmäkomitean I osamietintö. Komitean työn lähtökohdat ja

tavoitteet. Helsinki 1974.
300. KM 1981:66. Tietosuojakomitean mietintö. Helsinki 1981.
301. KM 1992:3. Perusoikeuskomitean mietintö. Helsinki 1992.
302. KM 1997:9. Henkilötietotoimikunnan mietintö. Helsinki 1997
303. Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti, Viestintäviraston julkaisu (Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf, 14.11.2015).
304. Kohdistetut haittaohjelmahyökkäykset, Viestintäviraston www–sivut (Saatavilla: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2013/11/ttn201311011336.html, 14.11.2015).
305. Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous– ja sosiaalikomitealle ja alueiden komitealle, pilvipalvelujen potentiaali käyttöön Euroopassa (COM(2012) 529 final) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:FI:PDF, 16.11.2015).
306. Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous– ja sosiaalikomitealle ja alueiden komitealle, Elintärkeiden tietoinfrastruktuureiden suojaamisesta ”Euroopan suojaaminen laajoilta tietoverkkohyökkäyksiltä ja –häiriöiltä: valmiuden, turvallisuuden ja sietokyvyn parantaminen” (KOM(2009) 149 lopullinen) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:FI:PDF, 16.11.2015).
307. Komission tiedonanto euroopan parlamentille, neuvostolle, Euroopan talous– ja sosiaalikomitealle ja alueiden komitealle, Euroopan digitaalistrategia (KOM(2010) 245 lopullinen) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:FI:PDF, 16.11.2015).
308. Komission tiedonanto neuvostolle ja Euroopan parlamentille, eEurope2002 Vaikutukset ja painopisteet, Tiedonanto Eurooppa–neuvoston Tukholman kokoukselle 23.–24. maaliskuuta 2001 (KOM(2001) 140 lopullinen) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0140:FIN:FI:PDF, 16.11.2015).
309. Komission tiedonanto neuvostolle, Euroopan parlamentille, Talous– ja

sosiaalikomitealle sekä Alueiden komitealle, eEurope 2005: Tietoyhteiskunta kaikille (KOM(2002) 263 lopullinen) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:FI:PDF, 16.11.2015).

310. Konstari, Timo: Henkilörekisterilaki. Säännökset ja käytäntö. Lakimiesliiton kustannus, Helsinki 1992.
311. Korhonen, Rauno: Perusrekisterit ja tietosuoja. Edita, Helsinki 2003.
312. KPMG (2013), Virtually Unregulated, Countering Virtual Currency Money Laundering in the 21st Century, seen on: http://www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG–Countering–Money–Laundering.pdf
313. Kyberturvallisuuskeskus vahvistaa Viestintäviraston nykyisiä tietoturvatehtäviä, Julkaistu 24.10.2013, https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2013/kyberturvallisuuskeskusvahvistaaviestintavirastonnykyisiatietoturvatehtavia.html, 16.11.2015
314. Laiho, Erna. Johdon sihteeri, tietosuojavaltuutetun toimisto. 6.5.2014, Helsinki.
315. Lait – Erityislainsäädäntö. Saatavilla http://www.tietosuoja.fi/fi/index/lait/erityislainsaadanto.html. Viitattu 9.5.2014.
316. Lait – Kansainväliset normit ja ohjeet – Euroopan neuvoston antamia suosituksia. Saatavilla http://www.tietosuoja.fi/fi/index/lait/kansainvalisetnormitjaohjeet/euroopanneuvostonantamiasuosituksia.html. Viitattu 9.5.2014.
317. Lapin yliopiston oikeusinformatiikan instituutti: verkkosivut. NETSO–tutkimusprojekti 2010–2013 (englanniksi). Saatavilla http://www.ulapland.fi/Suomeksi/Yksikot/Oikeustieteiden–tiedekunta/Tutkimus–ja–jatko–opinnot/Instituutit/Oikeusinformatiikan–instituutti/NETSO–tutkimusprojekti–2010%E2%80%932013–%28englanniksi%29. Viitattu 20.11.2013.
318. Law 241/90 on Administrative Procedure and Access to Administrative Documents: http://www.ictparliament.org/node/2040.
319. Liikenne– ja viestintäministeriön hallinnonala, LVM:n www–sivut: hallinnonala (Saatavilla: http://www.lvm.fi/hallinnonala, viitattu 11.11.2015).
320. Lilius, Reijo (koonnut). Suomi tietoyhteiskunnaksi – kansallisten linjausten arviointi. Suomen itsenäisyyden juhlarahasto, SITRA 159. Helsinki 1997.
321. Liu, N.Y.: Bio–Privacy: Privacy Regulations and the Challenge of Biometrics.

Routledge 2012.
322. Loevinger, Jurimetrics — The Next Step Forward. Minnesota Law Review 1949.
323. Lyon, David: Surveillance Society: Monitoring Everyday Life. Open University Press. Buckingham 2001.
324. M. Palmirani, M. Martoni, D. Girardi, Open Government Data Beyond Transparency [in:] Electronic Government and the Information Systems Perspective, A. K˝o, E. Francesconi (eds.), Third International Conference, EGOVIS 2014 Munich, Germany, September 1–3, 2014 – Proceedings.
325. M. Palmirani, M. Mockus, Open Government Data Licensing Framework [in:] Electronic Government and the Information Systems Perspective, A. Kő, E. Francesconi (eds.) Fourth International Conference, EGOVIS 2014, Valencia, Spain, September 1–4, 2015, Proceedings, Springer, 2015.
326. Mäenpää, Olli. Eurooppalainen hallinto–oikeus. Talentum. Helsinki 2011.
327. Mäenpää: Hallintolaki ja hyvän hallinnon takeet (2011) s. 184–185, Kulla: Hallintomenettelyn perusteet (2008) s. 181 ja HE 72/2002 vp. s. 89
328. Mäenpää: Julkisuusperiaate (2009) s. 121–122
329. Mäenpää: Julkisuusperiaate (2009) s. 124
330. Mäenpää: Julkisuusperiaate (2009) s. 145 ja 147
331. Mäenpää: Julkisuusperiaate (2009) s. 150
332. Mäenpää: Julkisuusperiaate (2009) s. 152
333. Mäenpää: Julkisuusperiaate (2009) s. 153
334. Mäenpää: Julkisuusperiaate (2009) s. 153
335. Mäenpää: Julkisuusperiaate (2009) s. 155–156
336. Mäenpää: Julkisuusperiaate (2009) s. 158
337. Mäenpää: Julkisuusperiaate (2009) s. 163
338. Mäenpää: Julkisuusperiaate (2009) s. 163
339. Magnusson Sjöberg – Wahlgren Festskrift till Peter Seipel (2006)
340. Makkonen Zur Problematik der juridischen Entscheidung : eine strukturanalytische Studie.
341. Marglin, Stephen Alan & Juliet B. Schor (eds.) (1990) The Golden Age of Capitalism: Reinterpeting the Postwar Experience. Oxford: OUP.
342. Materiaalia – Lomakkeet. Saatavilla http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet.html. Viitattu 9.5.2014.
343. Materiaalia – Oppaat. Saatavilla http://tietosuoja.fi/fi/index/materiaalia/oppaat.html.

Viitattu 9.5.2014.

344. Material – Broschyrer. Saatavilla http://www.tietosuoja.fi/sv/index/materiaalia/oppaat.html. Viitattu 9.5.2013.
345. Memorandum for the Heads of Executive Departments and Agencies, SUBJECT: Transparency and Open Government, http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
346. Merriam–Webster´s Dictionary of Law. 14th printing. Harrisonburg, Virginia, United States of America. 2011.
347. Michael Koeding (2007), 'Active Transposition of EU Legislation', EIPASCOPE, No. 3.
348. Michalis, Maria (2007) Governing European Communications: From Unification to Coordination. Lanham: Lexington.
349. Mitchell, R., Revised OECD Privacy Guidelines Focus On Accountability, Notification of Breaches, September 16, 2013, http://www.bna.com/revised–oecd–privacy–n17179877087/ (access September 2015),
350. Mm. professori Ahti Saarenpää sekä eduskunnan oikeusasiamies ovat puoltaneet yleisen tietoturvalain säätämistä. Ks. esim. Saarenpää, Ahti. (2015). Oikeusinformatiikka. Teoksessa: Oikeus tänään. osa 1. Toim. Marja–Leena Niemi. 3. painos. Lapin yliopiston oikeustieteellisiä julkaisuja. C63. Rovaniemi: Lapin yliopisto tai Saarenpää, Ahti et al. Sähköinen viestintä, tietoturvallisuus ja perusoikeudet. 2004. Rovaniemi: Lapin yliopisto.
351. Monica Palmirani, Michele Martoni, Dino Girardi – Open Government Data Beyond Transparency in: Andrea K″o Enrico Francesconi (Eds.) Electronic Government and the Information Systems Perspective Third International Conference, EGOVIS 2014 Munich, Germany, September 1–3, 2014 – Proceedings.
352. Mordini, E. – Tzovaras, D. – Ashton, H.: Introduction in Emilio Mordini and Dimitrios Tzovaras (eds.), Second Generation Biometrics: The Ethical, Legal and Social Context. Springer. 2012. p. 1–22.
353. Morten Hagedal has the opinion, that Norway had been number one. When participating that conference I could however see, that Finland and Austria were at top. Cfr Hagedal IT in the Norwegian Courts p. 77 in Oskamp – Lodder – Apistola IT Support of the Judiciary (2004).
354. Muttilainen, Vesa: Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistilastojen tietoja 1990–luvulta ja 2000–luvun alusta. Oikeuspoliittisen

tutkimuslaitoksen julkaisuja 218. Oikeuspoliittinen tutkimuslaitos, Helsinki 2006.

355. Muut kirjalliset lähteet ja verkkolähteet
356. N. Ilkka, Informaatio, Tieto ja Yhteiskunta (Information, Knowledge, and Society), Helsinki 1989, p.57.
357. Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a Networked World. Wiley Tech Brief Series. Published by John Wiley & Sons, Inc. (2002).
358. National Audit Office, www.vtv.fi/en.
359. Neuvonen, Riku: Tapaoikeus oikeuslähdeopissa. Lakimies 3/2006, s. 405–432.
360. New York State forges ahead in the virtual currency arena with proposed licensing requirements (2014) seen on: http://www.regulationtomorrow.com/us/new–york–state–forges–ahead–in–the–virtual–currency–arena–with–proposed–licensing–requirements/
361. Niels Vandezande (2014), 'Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?', International Journal of Law and Information Technology, Vol. 1, No. 16, p. 6.
362. Nielsen, Rasmus Klein (2010) The Changing Business of Journalism and its Implications for Democracy. Oxford: Reuters Institute for the Study of Journalism.
363. Nieminen, Hannu & Trappel, Josef (2011) 'Media Serving Democracy', pp. 135–51 in J. Trappel, W. A. Meier, L. d'Haenens, J. Steemers and B. Thomass (eds.) Media in Europe Today. Bristol: Intellect.
364. NIST Cloud Computing Program, NIST:n www–sivut: Cloud Computing (Saatavilla: http://www.nist.gov/itl/cloud/, viitattu 16.11.2015).
365. NSA:n www–sivut: www.nsa.gov, About NSA, päivitetty 29.11.2011 (Saatavilla: http://www.nsa.gov/about/index.shtml, 16.11.2015).
366. Nurmi, Pekka. Tietosuojalautakunnan puheenjohtaja. 14.10.2013, Helsinki.
367. Nurmi, Pekka: Henkilötietolain linjauksia. Tietosuoja 2/1999.
368. Nurmi, Pekka: Tietosuojalautakunta toiselle vuosikymmenelle. Tietosuoja 4/1997.
369. OECD Digital Economy Outlook 2015, OECD Publishing, Paris. (Saatavilla: http://dx.doi.org/10.1787/9789264232440–en, 11.11.2015).
370. OECD:n neuvoston suositus, Tietojärjestelmien ja tietoverkkojen turvallisuusperiaatteet. Turvallisuuskulttuurin kehittäminen OECD:n Neuvoston suositus 1037. (http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/24335_fi.pdf, viitattu 11.11.2013).

371. OECD:n neuvoston suositus, Tietosuojasäännöt – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 (Saatavilla: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 16.11.2015).
372. OECD:n neuvoston tietoturvallisuusperiaatteita koskeva suositus 26.11.1992 (Saatavilla: http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm, 16.11.2015).
373. OECD:n tietosuojatyö – OECD work on privacy (Saatavilla: http://www.oecd.org/sti/ieconomy/privacy.htm, 16.11.2015).
374. Office of the Australian Information Commissioner: verkkosivut (englanniksi). About Us – What we do. Saatavilla http://www.privacy.gov.au/about–us/what–we–do/what–we–do. Viitattu 20.3.2014.
375. Öhquist, Johannes 2006: Pietarista kolmanteen valtakuntaan. Helsinki: Fenix–kustannus.
376. Oikeushallinnon informaatiojärjestelmän kehittämissuunnitelma : kehittämistyön organisointi, järjestelmän edellyttämä koulutus ja teknisten ratkaisujen perusteet: KM 1974:6.
377. Oikeushallinnon informaatiojärjestelmän kehittämissuunnitelma, KM 1973:58
378. OMLJ 10/1978. Sinisalo, Kari – Immonen, Heikki – Leistén, Martti – Pöyhönen, Juhani – Savolainen, Matti – Tulkki, Hannu – Virtanen, Ilpo: Henkilörekisterityöryhmän väliraportti. Oikeusministeriön lainvalmisteluosaston julkaisu 10/1978. Helsinki 1978.
379. OMLJ 10/1982. Wallin, Anna–Riitta: Lausunnot tietosuojakomitean mietinnöstä. Tiivistelmä. Oikeusministeriön lainvalmisteluosaston julkaisu 10/1982. Helsinki 1982.
380. OMLJ 19/1977. Virtanen, Ilpo: Lausunnot henkilörekisterityöryhmän väliraportista. Tiivistelmä. Oikeusministeriön lainvalmisteluosaston julkaisu 19/1977. Helsinki 1977.
381. OMLJ 22/1975. Holopainen, Irja: Yksilö ja rekisterit. Oikeusministeriön lainsäädäntöosaston julkaisu 22/1975. Helsinki 1975.
382. Online Currency Exchange Accused of Laundering $6 Billion (2013) on: http://www.nytimes.com/2013/05/29/nyregion/liberty–reserve–operators–accused–of–money–laundering.html?pagewanted=all&_r=0
383. Open Data Handbook Documentation, Release 1.0.0 p. 4, http://opendatahandbook.org/guide/en/

384. Open Government Data website http://opengovernmentdata.org/
385. OPHOK 2013:7. Vehkamäki, Pirjo – Lahtinen, Matti – Tamminen–Dahlman, Anne: Julkisuus ja tietosuoja opetustoimessa. Opas koulujen ja oppilaitosten käyttöön. 4. uudistettu painos. Opetushallitus, Oppaat ja käsikirjat 2013:7. Tampere 2013. Saatavilla http://www.oph.fi/download/152370_julkisuus_ja_tietosuoja_opetustoimessa.pdf. Viitattu 28.10.2013.
386. Opinion of Advocate General Bot delivered on 23 September 2015, Case C‑362/14 Maximillian Schrems v Data Protection Commissioner, http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=326249 (access September 2015)
387. Opinion of the European Data Protection Supervisor on the "Open Data Package", http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12–04–18_Open_data_EN.pdf.
388. Originally Suomen Laki was a joint project with the Ministry of Justice and Finnish Lawyers Association. Nowadays Ministry of Justice is cooperating with Edilex company. That state owned company is also publishing a commercial law collection.
389. Pääministeri Juha Sipilän hallituksen strateginen ohjelma 29.5.2015. Hallituksen julkaisusarja 10/2015 (Saatavilla: http://valtioneuvosto.fi/sipilan–hallitus/hallitusohjelma, 11.11.2015).
390. Pääministeri Jyrki Kataisen hallituksen ohjelma 22.6.2011, s. 51 (Saatavilla: http://valtioneuvosto.fi/documents/10184/147449/Kataisen+hallituksen+ohjelma/81f1c20f–e353–47a8–8b8f–52ead83e5f1a, 11.11.2015).
391. Päätökset – Korkeimman hallinto–oikeuden päätökset – Korkeimman hallinto–oikeuden päätös ns. pikavippiasiassa. Saatavilla http://www.tietosuoja.fi/fi/index/ratkaisut/korkeimmanhallinto–oikeudenpaatosns.pikavippiasiassa.html. Viitattu 9.5.2014.
392. Päätökset – Korkeimman hallinto–oikeuden päätökset. Saatavilla http://www.tietosuoja.fi/fi/index/ratkaisut/korkeimmanhallinto–oikeudenpaatokset.html. Viitattu 9.5.2014.
393. Päätökset. Saatavilla http://www.tietosuoja.fi/fi/index/ratkaisut.html. Viitattu 9.5.2014.
394. Pahlman: Asiakirjajulkisuus sosiaali– ja terveydenhuollossa (2007) s. 61
395. Panofsky, Erwin 1972 (1939): Studies in Iconology: Humanistic Themes in the Art of the Renaissance. New York: Harper & Row.

396. Password reuse opens doors for cyber criminals, InfoWorld, julkaistu 15.12.2013 (Saatavilla: http://www.infoworld.com/d/security–central/password–reuse–opens–doors–cyber–criminals–457, 16.11.2015).
397. Patrick McLeod (2014), 'Taxing and Regulating Bitcoin: The Government's Game of Catch Up', Journal of Communications Law and Technology Policy, Vol. 22 No. 2.
398. Pellonpää – Gullans – Pölönen – Tapanila: Euroopan ihmisoikeussopimus (2012)
399. Pellonpää – Gullans – Pölönen – Tapanila: Euroopan ihmisoikeussopimus (2012) s. 526–531 ja 583
400. Pellonpää – Gullans – Pölönen – Tapanila: Euroopan ihmisoikeussopimus (2012) s. 751
401. Pellonpää, Matti. Henkilökohtainen koskemattomuus. Teoksesta: Perusoikeudet. Muut kirjoittajat: P. Hallberg, H. Karapuu, Tuomas Ojanen, M. Scheinin, K. Tuori & V–P. Viljanen. Päivitetty sähköinen versio. WSOYPro. Helsinki 2011. s. 283–286.
402. Periaatepäätös kansallisesta tietoturvastrategiasta 4.12.2008 (Saatavilla: http://www.lvm.fi/c/document_library/get_file?folderId=142524&name=DLFE–4935.pdf&title=Periaatep%C3%A4%C3%A4t%C3%B6s%20kansallisesta%20tietoturvastrategiasta%204.12.2008, 16.11.2015).
403. Perkins Coie LLP (2014), Virtual Currencies: International Actions and Regulations, seen on: http://www.perkinscoie.com/virtual–currencies–international–actions–and–regulations/#United Kingdomon
404. Peruginelli – Ragona (eds) Law via the Internet. Free Access, Quality of Information, Effectiveness of Rights (2009).
405. perustaminen (KOM(2012) 140 lopullinen) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:FI:PDF, 16.11.2015).
406. PeVL 11/2000 vp Hallituksen esitys Euroopan unionin ydinaseettomien jäsenvaltioiden, Euroopan atomienergiayhteisön ja Kansainvälisen atomienergiajärjestön välisen ydinaseiden leviämisen estämistä koskevan sopimuksen III artiklan 1 ja 4 kohdan täytäntöönpanosta tehtyyn sopimukseen liittyvän lisäpöytäkirjan eräiden määräysten hyväksymisestä sekä laiksi ydinenergialain muuttamisesta.
407. PeVL 12/2000 vp Hallituksen esitys laiksi merilain 9 luvun muuttamisesta sekä merioikeudellisia vaateita koskevan vastuun rajoittamisesta tehdyn vuoden 1976 yleissopimuksen muuttamisesta tehdyn vuoden 1996 pöytäkirjan eräiden määräysten hyväksymisestä.

408. PeVL 18/2014 vp. Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle duskunnalle tietoyhteiskun takaareksi sekä laeiksi maankäyttö– ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta (HE 221/2013 vp). Helsinki 2014.
409. PeVL 9/2004 vp. Hallituksen esitys sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.
410. Pihlajamäki, Antti. Tietojenkäsittelyrauhan rikosoikeudellinen suoja – Datarikoksia koskeva sääntely Suomen rikoslaissa. Suomalaisen lakimiesyhdistyksen julkaisuja A–sarja N:o 258, 2004
411. Pilvipalveluiden turvallisuus – Mitä organisaatioiden tulisi huomioida pilvipalveluja, Viestintäviraston julkaisu (Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf, 16.11.2015).
412. Pitkänen, Olli – Tiilikka, Päivi – Warma, Eija: Henkilötietojen suoja. Talentum, Helsinki 2013.
413. Poikola, Kuikkaniemi & Kuittinen. My Data – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen. Liikenne– ja viestintäministeriö. Helsinki 2014 (Saatavilla: http://www.lvm.fi/asiakirjat_ja_muut_julkaisut, 15.11.2015).
414. Poliisin valmiuksia parannetaan nykybudjetin raameissa, mutta se ei riitä, 19.03.2015 (Saatavilla: https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/poliisin_valmiuksia_parannetaan_nykybudjetin_raameissa_mutta_se_ei_riita_28088, 11.11.2015).
415. Population Register Centre: Population Information System. Available at <http://www.vrk.fi/default.aspx?id=39> [20.5.2014].
416. Porvari, Paavo. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöidentoiminnassa. Aalto yliopisto. Helsinki 2012.
417. Pöysti Information Government in Practise: Functional Gains and Legal Perils in Scandinavia Studies in Law (2010)
418. Pöysti, Tuomas. Tarkoitus ja metodi. Teoksesta: Tietoturvallisuus ja laki. Saarenpää, A (toim.), Pöysti T (toim.), Sarja M, Still V, Balboa–Alcoreza, R. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, Valtiovarainministeriö Hallinnon kehittämisosasto, Lapin yliopisto, 1997.
419. Pöysti, Tuomas. Uhka, riski ja turvallisuus. Teoksesta: Tietoturvallisuus ja laki. Saarenpää, A (toim.), Pöysti T (toim.), Sarja M, Still V, Balboa–Alcoreza, R.

Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, Valtiovarainministeriö Hallinnon kehittämisosasto, Lapin yliopisto, 1997b.

420. PRESS RELEASE EDPS/08/12, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS–2012–08_Open_Data_EN.pdf.
421. Price of Bitcoin Surges Past $1,000, up 8,000% in One Year (2013) seen on: http://www.techvibes.com/blog/price–of–bitcoin–surges–2013–11–27
422. Prins, R.: Biometric technology law, making our body identify for us: legal implications of biometric technologies. Computer Law & Security Report, 14(3), p.159–165.
423. Prodi käynnistää eEurope–aloitteen nopeuttaakseen Euroopan kehittymistä tietoyhteiskunnaksi
424. Proposal for a Directive of the European Parliament and of the Council Amending Directive 2003/98/EC on re–use of public sector information, http://ec.europa.eu/information_society/policy/psi/docs/pdfs/opendata2012/revision_of_PSI_Directive/proposal_directive_EN.pdf.
425. Proposed Codes, Rules and Regulations, NY State, Dept. of Financial Services seen on: http://www.dfs.ny.gov/about/press2014/pr1407171–vc.pdf.
426. R. Carnap, Y. Bar–Hillel, An outline of the theory of Semantic information. Research Laboratory of Electronic, Massachusetts Institute of Technology, Report No. 247, 1952.
427. Raitio, Juha. Eurooppaoikeus ja sisämarkkinat. Talentum Oy. Helsinki 2010.
428. Raj Samani, François Paget, Matthew Hart (2013), McAffe White Paper – 'Digital Laundry – An analysis of online currencies and their use in cybercrime', (McAffe Inc., Santa Clara, CA).
429. Råman, Jari. Tietoturvallisuus on myös perusoikeus. Lakimies 5/2006.
430. Rampini, Corrado 2002: Die nachträgliche Leistungserschwerung. Dissertation. Universität St. Gallen, Hochschule für Wirtschafts–, Rechts– und Sozialwissenschaften (HSG). Genehmigt auf Antrag der Herren Dr. Alfred Koller und Dr. Ivo Schwander. Dissertation Nr. 2596. Eschen.
431. Rantalankila, Leena: Tietosuojalautakunnan toimivalta täsmentyi. Tietosuoja 2/1999.
432. Read more about the Open Definition at: http://opendefinition.org/od/
433. Reding, Viviane: Privacy Implications of Biometrics. Foreword in Emilio Mordini and Dimitrios Tzovaras (eds.), Second Generation Biometrics: The Ethical, Legal and Social Context. Springer. 2012.

434. Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, OJ L 345/1.
435. Regulation (EC) No 910/2014 of the European Parliament and of the Council of 23 July 2014on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257.
436. Regulation of Bitcoin in Selected Jurisdictions (2014) seen on: http://www.loc.gov/law/help/bitcoin–survey/
437. Reuben Grinberg (2012),' Bitcoin: An Innovative Alternative Digital Currency', Hastings Science & Technology Law Journal, No. 158.
438. Review of recent studies on PSI re–use and related market developments, G. Vickery, August 2011.
439. Rifkind, M., Porter, H., Henry Porter v Malcolm Rifkind: surveillance and the free society, http://www.theguardian.com/commentisfree/2013/aug/24/rifkind–porter–debate–miranda–surveillance/ (access September 2015),
440. Rikosilmiöitä, poliisin www–sivut: Tietorikoksia (Saatavilla: https://www.poliisi.fi/rikokset/rikosilmioita/tietorikoksia, 11.11.2015).
441. Robinson N, Valeri L, Cave J & Starkey T (RAND Europe), Graux H (time.lex), Creese S, Hopkins P (University of Warwick). The Cloud: Understanding the Security, Privacy and Trust Challenges, Final Report. Prepared for Unit F.5, Directorate–General Information Society and Media, European Commission. 30 November 2010. (Saatavilla: http://cordis.europa.eu/fp7/ict/security/docs/the–cloud–understanding–security–privacy–trust–challenges–2010_en.pdf, 16.11.2015).
442. Rowland, D., Kohl, U., Charlesworth, A., Information Technology Law, Fourth Edition, Routledge 2002,
443. Saako henkilötietoja lähettää sähköpostilla salaamattomana? Tietosuojavaltuutetun www–sivut, 2008 (Saatavilla: http://www.tietosuoja.fi/fi/index/ratkaisut/saakohenkilotietojalahettaasahkopostilla.html 14.11.2015).
444. Saarenpää Oikeudellista tilastointia, Oikeus 3/1973.
445. Saarenpää, A (toim.), Pöysti T (toim.), Sarja M, Still V, Balboa–Alcoreza, R. Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, Valtiovarainministeriö Hallinnon kehittämisosasto, Lapin yliopisto, 1997.
446. Saarenpää, A. (ed.), Legal privacy, Zaragoza 2008,

447. Saarenpää, A: Tietosuoja ja tietoturva, identiteetin näkökulma in Tietoturvallisuus ja laki. Ajankohtaista asiaa tietoturvasta. Lapland University Press. Rovaniemi, Finland 2002.
448. Saarenpää, Ahti 1998: Oikeusinformatiikka. Teoksessa: Kangas, Urpo (toim.): Oikeustiede Suomessa 1900–2000: 211–220. Helsinki: WSOY.
449. Saarenpää, Ahti, THE NETWORK SOCIETY AND LEGAL INFORMATION. Some observations from the Nordic point of view. LAW via Internet 2011 papers in www.hklii.hk/eng/Free_Access_to_Law(eng).pdf
450. Saarenpää, Ahti. Henkilö– ja persoonallisuusoikeus. Teoksesta: Tammilehto Timo
451. Saarenpää, Ahti. Oikeusinformatiikka. Teoksesta: Tammilehto Timo (toim.) Oikeusjärjestys, osa 1. Rovaniemi: Lapin yliopisto 2012b.
452. Saarenpää, Ahti: 'Data protection in the network society – the exceptional becomes the natural'. In Galindo, Fernando (ed.): El derecho de la sociedad en red. LEFIS series 14. Prensas de la Universidad de Zaragoza: Zaragoza 2013.
453. Saarenpää, Ahti: 'Finland'. In Blume, Peter (ed.): Nordic Data Protection. Kauppakaari: Helsinki 2001.
454. Saarenpää, Ahti: Data protection in the network society – the exceptional becomes the natural. Teoksessa Galindo, Fernando (ed.): El derecho de la sociedad en red. LEFIS series 14. Prensas de la Universidad de Zaragoza, Zaragoza 2013.
455. Saarenpää, Ahti: Finland. Teoksessa Blume, Peter (toim.): Nordic Data Protection Law. Iustus Förlag, Uppsala 2001.
456. Saarenpää, Ahti: Henkilö– ja persoonallisuusoikeus. Teoksessa Tammilehto, Timo (toim.): Oikeusjärjestys. Osa 1. 8. täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja C 59. Lapin yliopisto, Rovaniemi 2012.
457. Sama vaatimus koskee myös Yhdysvaltain pörssissä listattuja suomalaisyrityksiä. Ks. esim. Kinnunen, Niina (2015). Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen. Vaasa: Vaasan yliopisto.
458. Sandra S. Benson (2009), 'Recognizing the Red Flags of a Ponzi Scheme', The CPA Journal , Vol. 79, No. 6.
459. SANS:n (SysAdmin, Audit, Networking and Security) www–sivut: www.sans.org, about & reading room, 2015. (Saatavilla: http://www.sans.org/about/ & http://www.sans.org/reading–room/, 10.11.2015).
460. Saraviita: Perustuslaki (2011).
461. Sartor G., Human rights in the information society in

papers.ssrn.com/sol3/papers.cfm?abstract_id=1707724
462. Schartum, D. W. (ed), Overvåking in en Rettsstat, Fagbokforlaget 2010,
463. Schweighofer – Kümmer – Hötzendorfer (eds.) Tranparenz. IRIS 2014.
464. Schweighofer – Saarenpää – Böszörmenyi (eds.), KnowRight 2012 and
465. Schweighofer, E., Kummer, F., Hötzendorfer, W. (ed.), Transparency, Proceedings of the 17th International Legal Informatics Symposium IRIS 2014, Salzburg 2014,
466. Sethi, I: "Biometrics. Overview and applications" in Katherine J. Strandberg and Daniela Stan Raicu (eds), Privacy and Technologies of Identity. A Cross–Disciplinary Conversation. Springer Science + Business Media, Inc. 2006.
467. SFS–käsikirja, standardit ja standardointi 2013, s. 7 (Saatavilla: http://www.sfs.fi/files/83/KK_1_2015_muokattu.pdf, 16.11.2015).
468. Simon Barber, Xavier Boyen, Elaine Shi, Ersin Uzun (2012), 'Bitter to Better – How to Make Bitcoin a Better Currency', Lecture Notes in Computer Science , Vol. 7397.
469. Sinisalo, Kari – Immonen, Heikki – Leistén, Martti – Pöyhönen, Juhani – Savolainen, Matti – Tulkki, Hannu – Virtanen, Ilpo: Henkilörekisterityöryhmän väliraportti. Oikeusministeriön lainvalmisteluosaston julkaisu 10/1978. Helsinki 1977.
470. So You Know Nothing About Bitcoins? Here's 50 Things That'll Make You Sound Like An Expert (2014) seen on: http://www.bluntbit.com/news–bits/know–nothing–bitcoins–heres–50–things–thatll–make–sound–like–expert/#.U_imvrySwng
471. Söderlindh, Åsa: Personlig integritet som informationspolitik. Debatt och diskussion i samband med tillkomsten av Datalag (1973:289). Skrifter från VALFRID, nr 38. Högskolan i Borås, Institutionen Biblioteks– och informationsvetenskap: Borås 2009.
472. Söderlindh, Åsa: Personlig integritet som informationspolitik. Debatt och diskussion i samband med tillkomsten av Datalag (1973:289). Skrifter från VALFRID, nr 38. Högskolan i Borås, Institutionen Biblioteks– och informationsvetenskap, Borås 2009.
473. Solove, D. J., Schwartz, P. M., Information Privacy Law, Fourth Edition, New York 2011,
474. Statistics Finland: Kuluttajahintaindeksi. Rahanarvokerroin 1860 – 2012. Available at <http://www.stat.fi/til/khi/2012/khi_2012_2013–01–15_tau_001.html> [3.4.2014].
475. Still, Viveca. Euroopan unioni. Teoksesta: Tietoturvallisuus ja laki. Saarenpää, A (toim.), Pöysti T (toim.), Sarja M, Still V, Balboa–Alcoreza, R. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, Valtiovarainministeriö Hallinnon kehittämisosasto, Lapin yliopisto, 1997.
476. Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity

Theft (2012), seen on: http://ec.europa.eu/dgs/home–affairs/e–library/documents/policies/organized–crime–and–human–trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf.
477. Study on 'Pricing of Public Sector Information', Deloitte consulting and others, June 2011.
478. Suomen kyberturvallisuusstrategia – mitä tehdään ja miksi? Turvallisuuskomitean esitys 26.11.2013 (Saatavilla: http://www.cgi.fi/sites/default/files/files_fi/events/2013–11–26_cgi–kyberseminaari_1.virtanen–vesa.pdf, 16.11.2015).
479. Suomen kyberturvallisuusstrategia (VNp 24.1.2013) (http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit/doc_download/50–suomen–kyberturvallisuusstrategia–ja–taustamuistio, 11.11.2015),.
480. Suomen virallinen tilasto (SVT): Kuluttajahintaindeksi [verkkojulkaisu]. Rahanarvokerroin 1860 – 2012. Tilastokeskus, Helsinki 2012. Saatavilla http://www.stat.fi/til/khi/2012/khi_2012_2013–01–15_tau_001.html. Viitattu 10.9.2013.
481. Suomen virallinen tilasto (SVT): Syytetyt, tuomitut ja rangaistukset [verkkojulkaisu]. Tilastokeskus, Helsinki 2012. Saatavilla http://www.stat.fi/til/syyttr/index.html. Viitattu 24.1.2014.
482. Suomesta tietoturvan turvasatama? TTL ry, julkaistu 30.09.2013 (Saatavilla: https://ssl.ttlry.fi/news/201309/suomesta–tietoturvan–turvasatama, 14.11.2015).
483. Supreme Administrative Court of Finland
484. Svantesson, D., Greenstein, S. (ed.), Nordic Yearbook of Law and Informatics 2010–2012. Internationalisation of Law in the Digital Information Society, Copenhagen 2013,
485. T. Berners–Lee, J. Hendler, Ora Lassila (May 17, 2001),"The Semantic Web". Scientific American Magazine. Retrieved March 26, 2008.
486. Tala, Jyrki. Lainsäädäntö, ajankohtaisia kehityspiirteitä. Teoksesta: Oikeusolot 2000. Katsaus oikeudellisten instituutioiden toimintaan ja oikeusongelmiin. OPTL:n julkaisu 173. Julkisuuteen 30.8.2000.
487. Tala, Jyrki. Lainvalmistelu ja sääntelyn vaihtoehdot. Hakapaino Oy. Helsinki 2012. (Saatavilla: http://optula.om.fi/material/attachments/optula/julkaisut/tutkimustiedonantoja–sarja/3tlC4mLLD/TTA_115_Tala_2012.pdf, 16.11.2015).
488. Tala, Jyrki. Lakien laadinta ja vaikutukset. Edita Prima Oy. Helsinki 2005.
489. Tala, Jyrki. Selvitys vaihtoehtojen hyödyntämisestä erityisesti yrityksiin vaikuttavan

lainsäädännön valmistelussa. Turun yliopisto. 11.12.2007. (Saatavilla: https://www.tem.fi/files/25910/Tala_vaihtoehtoselvitys_2007_lopullinen.pdf, 16.11.2015).

490. Taloudellisia ryhmittymiä, G7/G8, Ulkoasiainministeriön www–sivut, taloudellisia ryhmittymiä (http://www.formin.fi/public/default.aspx?contentid=69275&contentlan=1&culture=fi–FI, viitattu 13.11.2013).
491. Talous– ja sosiaalikomitealle ja Alueiden komitealle, Verkko– ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi (KOM(2001)298 lopullinen) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:FI:PDF, 16.11.2015).
492. Tehtävät – Kansainvälinen yhteistyö – Valvontaelimet. Saatavilla http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/kansainvalineny hteistyo/valvontaelimet_0.html. Viitattu 9.5.2014.
493. Tehtävät – Sidosryhmäyhteistyö – Opetustoimen tietosuojan ohjausryhmä. Saatavilla http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/sidosryhmayhtei styo/opetusalantietosuojanohjausryhma.html. Viitattu 9.5.2014.
494. Tehtävät – Tulosohjaussuunnittelu ja –seuranta. Saatavilla http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/tulosohjaussuun nitteluja–seurantauusin.html. Viitattu 9.5.2014.
495. Terveyden ja hyvinvoinnin laitos: verkkosivut. Aiheet – Tietopaketit – Sosiaalihuollon tiedonhallinta – Aineistot – Tikesos–arkisto. Saatavilla http://www.thl.fi/fi_FI/web/fi/aiheet/tietopaketit/tiedonhallinta/aineistot/tikesosarkisto. Viitattu 28.1.2014.
496. The American Heritage Dictionary, http://www.ahdictionary.com/word/search.html?q=biometrics
497. The Council of the EU: Glossary of Security Documents, Security Features and other related technical terms, available in English at: http://prado.consilium.europa.eu/en/glossarypopup.html
498. The Internet of Things—A survey of topics and trends, Andrew Whitmore, Anurag Agarwal, Li Da Xu, Springer, 2014.
499. The National Bank of Romania, http://www.bnr.ro/National–Bank–of–Romania–1144.aspx
500. The New York Times. ”N.S.A. Able to Foil Basic Safeguards of Privacy on Web”. 5.

syyskuuta 2013. URL: http://www.nytimes.com/2013/09/06/us/nsa–foils–much–internet–encryption.html; The New York Times. ”Unlocking Private Communcations”. 5. syyskuuta 2013. URL: http://www.nytimes.com/interactive/2013/09/05/us/unlocking–private–communications.html?ref=us; sekä Greenwald, Glenn (2014). No Place to Hide. Edward Snow¬den and the USA. Surveillance State. New York: Metropolitan Books.

501. The Open Knowledge Foundation –OFKN, trading as Open Knowledge, is dedicated to promoting the creation, sharing and application of Open Knowledge in the Digital Age. More detail about OFKN can be found at https://okfn.org/about/.
502. The Opinion on Anonymisation Techniques adopted by WP29 is available at: http://ec.europa.eu/justice/data–protection/article–29/documentation/opinion–recommendation/files/2014/wp216_en.pdf
503. The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy, OECD Digital Economy Papers No. 209 (Saatavilla: http://www.oecd–ilibrary.org/docserver/download/5k8zq930xr5j.pdf?expires=1384943537&id=id&accname=guest&checksum=F48E280298BC0D07681B2FFC81C890CC, 16.11.2015).
504. Tietoa OECD:stä, Suomen pysyvä edustusto OECD:ssä ja Unescossa (Saatavilla: http://www.finlandunesco.org/public/default.aspx?nodeid=34689&contentlan=1&culture=fi–FI, 10.11.2015).
505. Tietoa poliisista, organisaatio, poliisin www–sivut: www.poliisi.fi › etusivu › Tietoa poliisista › Organisaatio (Saatavilla: http://www.poliisi.fi/tietoa_poliisista/organisaatio, 11.11.2015).
506. Tietosuojalautakunta: verkkosivut. Saatavilla http://oikeusministerio.fi/fi/index/ministerio/neuvottelu–jalautakunnat/tietosuojalautakunta.html. Viitattu 20.11.2013.
507. Tietosuoja–lehden toimitus: Rekisterinpitäjille säädetty ilmoitusvelvollisuus laajeni. Tietosuoja 2/1999.
508. Tietosuoja–lehti: verkkosivut. Saatavilla http://www.tietosuoja–lehti.fi, viitattu 28.1.2014.
509. Tietosuoja–lehti: Web site. Available at <http://www.tietosuoja–lehti.fi> [8.4.2014].
510. Tietosuojavaltuutetun kannanotto 1.7.2010 dnro 1475/41/2009 (Saatavilla: http://www.tietosuoja.fi/fi/index/ratkaisut/sahkopostinjatekstiviestienkayttaminente.html, 14.11.2015).

511. Tietosuojavaltuutetun toimisto: Henkilörekisteriin tallennettujen tietojen tarkastaminen. Päivitetty 22.8.2014. Helsinki 2014. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/RTLvP7vGp/Henkilorekisteriin_talletettujen_tietojen_tarkastaminen_22.8.2014.pdf. Viitattu 5.11.2014.
512. Tietosuojavaltuutetun toimisto: Henkilörekisteriin tallennetun tiedon oikaiseminen. Päivitetty 27.7.2010. Helsinki 2010. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpmoUoh/Henkilorekisteriin_tallennetun_tiedon_korjaaminen.pdf. Viitattu 5.11.2014.
513. Tietosuojavaltuutetun toimisto: Henkilötietolain mukainen ilmoitusvelvollisuus. Päivitetty 27.7.2010. Helsinki 2010. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfpr4Tsl/Henkilotietolain_mukainen_ilmoitusvelvollisuus.pdf. Viitattu 5.11.2014.
514. Tietosuojavaltuutetun toimisto: Oppilaiden henkilötietojen käsittely kodin ja koulun yhteistyössä. Opas peruskouluille. Päivitetty 18.12.2012. Helsinki 2012. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfq7U6EZ/Oppilaiden_henkilotietojen_kasittely_kodin_ja_koulun_yhteistyossa.pdf. Viitattu 5.11.2014.
515. Tietosuojavaltuutetun toimisto: Rekisteritutkimuksen tietosuojaopas tutkijoille ja tietopyyntöjä käsitteleville viranomaisille. Päivitetty 27.7.2010. Helsinki 2010. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqBT5i3/Rekisteritutkimuksen_tietosuojaopas_tutkijoille_ja_tietopyyntoja_kasitteleville_viranomaisille.pdf. Viitattu 5.11.2014.
516. Tietosuojavaltuutetun toimisto: Sähköpostin käytöstä sosiaalihuollossa. Päivitetty 15.9.2010. Helsinki 2010. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqFHt2y/Sahkopostin_kaytosta_sosiaalihuollossa.pdf. Viitattu 5.11.2014.
517. Tietosuojavaltuutetun toimisto: Tietosuoja ja tieteellinen tutkimus henkilötietolain kannalta. Päivitetty 27.11.2010. Helsinki 2010. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqJGExr/Tietosuoja_ja_tieteellinen_tutkimus_henkilotietolain_kannalta.pd

f. Viitattu 5.11.2014.

518. Tietosuojavaltuutetun toimisto: Toimialakohtaisten käytännesääntöjen laatiminen. Päivitetty 27.7.2010. Helsinki 2010. Saatavilla http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/egqckIFxR/Toimialakohtaisten_kaytannesaantojen_laatiminen.pdf. Viitattu 5.11.2014.
519. Tietosuojavaltuutetun toimisto: Toimintakertomukset 1987–1990 ja 1993–2013. Helsinki. Toimintakertomukset 2004–2013 saatavilla http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/tulosohjaussuunnitteluja–seurantauusin.html, viitattu 9.5.2014. Toimintakertomukset 2001–2003 osittain saatavilla http://www.tietosuoja.fi/1936.htm, http://www.tietosuoja.fi/27192.htm, http://www.tietosuoja.fi/uploads/pm5s162jk.rtf ja http://www.tietosuoja.fi/uploads/dm34trq.rtf, viitattu 19.11.2013.
520. Tietosuojavaltuutetun toimisto: verkkosivut. Saatavilla http://www.tietosuoja.fi. Viitattu 9.5.2014.
521. Tietosuojavaltuutetun toimisto: Vuosikertomukset ja katsaukset toimintaan 2004–2013. Helsinki. Saatavilla http://www.tietosuoja.fi/fi/index/tietosuojavaltuutetuntoimisto/tehtavat/tulosohjaussuunnitteluja–seurantauusin.html. Viitattu 9.5.2014.
522. Tietosuojavaltuutetun toimisto: Web site. Available at <http://www.tietosuoja.fi> [15.5.2014].
523. Tietotekniikkarikollisuus, poliisin www–sivut: Tietotekniikkarikollisuus (Saatavilla: https://www.poliisi.fi/rikokset/tietotekniikkarikollisuus, 11.11.2015).
524. Tietoturva ry:n www–sivut (Saatavilla: www.tietoturva.fi, 14.11.2015).
525. Tietoturvaa välillisesti koskevista säännöksistä esimerkkeinä mainittakoon 5 §:n säännökset terveydentilaa koskevien tietojen käsittelystä ja 13 §:n säännökset henkilö– ja soveltuvuusarviointitesteistä.
526. Tietoturvalliseen yhteiskuntaan, Kansallisen tietoturvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle 14.12.2004 (Saatavilla: http://80.248.162.134/oliver/upl163–Tietoturvastrategia%2014.pdf, 16.11.2015).
527. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007 (Saatavilla: http://vm.fi/dms–portlet/document/371267, viitattu 16.11.2015).
528. Tietoyhteiskuntakaari, Liikenne– ja viestintäministeriön www–sivut: www.lvm.fi,

Tietoyhteiskuntakaari (Saatavilla: http://www.lvm.fi/web/hanke/tietoyhteiskuntakaari, 11.11.2015).

529. Tiilikainen, Teija. Perustuslaillisuus integraatiossa. Teoksesta Euroopan perustuslaki. Edita Prima Oy. Helsinki 2005.
530. toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista,
531. Traunmüller (ed.), Electronic Government Third International Conference, EGOV 2004.
532. Tuloksellisuustarkastuskertomus hallituksen lainsäädäntösuunnitelma, valtiontalouden tarkastusviraston tarkastuskertomukset 18/2012, s. 47 (Saatavilla: http://www.vtv.fi/files/3212/Tarkastuskertomus_18_2012_NETTI.pdf, 16.11.2015).
533. Tuori, Kaarlo: Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota. Lakimies 7–8/2004.
534. Turvallisuuskomitean www–sivut (Saatavilla: http://www.turvallisuuskomitea.fi/, 11f.11.201).
535. tutkimusta, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten
536. Tyler Moore, Nicolas Christin (2013), 'Beware the Middleman: Empirical Analysis of Bitcoin–Exchange Risk', Financial Cryptography and Data Security Lecture Notes in Computer Science Vol. 7859.
537. Ulkoasiainministeriö: verkkosivut. EU – EU:n laajentumis– ja naapuruushankkeet – Twinning ja TAIEX – TAIEX – EU–rahoitteista täsmäapua hallinnolta hallinnolle. Saatavilla http://www.formin.fi/public/default.aspx?contentid=201547&contentlan=1&culture=fi–FI. Viitattu 1.4.2014.
538. Uutiset – 2014 – FYROM:n (Macedonia) delegaation opintomatka 3. – 6.3. tietosuojavaltuutetun toimistoon. Saatavilla http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2014/02/fyromnmacedoniadelegaationopintomatka3.–6.3.tietosuojavaltuutetuntoimistoon.html. Viitattu 9.5.2014.
539. Uutiset – 2014 – Pohjoismainen selvitys pankeille. Saatavilla http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2014/01/pohjoismainenselvitys pankeille.html. Viitattu 9.5.2014.
540. VAHTI 2/2010. Valtiovarainministeriö: Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Helsinki 2010. Saatavilla https://www.vahtiohje.fi//web/guest/2/2010–ohje–tietoturvallisuudesta–

valtionhallinnossa–annetun–asetuksen–taytantoonpanosta. Viitattu 29.4.2014.

541. Vahti Ohjaus, Valtiovarainministeriön www–sivut. (Saatavilla: http://vm.fi/ohjaus, 11.11.2015).
542. Valtion ICT–hankintojen tietoturvaohje, VAHTI 3/2011 (Saatavilla: https://www.vahtiohje.fi/web/guest/3/2011–valtion–ict–hankintojen–tietoturvaohje, 16.11.2015).
543. Valtioneuvosto: verkkosivut. Aiemmat hallitukset – Vanhasen hallitus – Tietoyhteiskuntaneuvosto. Saatavilla http://valtioneuvosto.fi/tietoarkisto/aiemmat–hallitukset/vanhanen/tietoyhteiskuntaneuvosto/fi.jsp. Viitattu 19.11.2013.
544. Valtioneuvoston kanslian toiminta. Valtioneuvoston kanslian www–sivut: www.vnk.fi (Saatavilla: http://vnk.fi/, 11.11.2015).
545. Valtionhallinnon etätyön tietoturvallisuusohje, Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003 (Saatavilla: https://www.vahtiohje.fi/web/guest/2/2003–turvallinen–etakaytto–turvattomista–verkoista, 16.11.2015 & https://www.vahtiohje.fi/web/guest/3/2002–valtionhallinnon–etatyon–tietoturvallisuusohje, 16.11.2015).
546. Valtionhallinnon kansainvälisen tietoturvayhteistyön hallintamalli, 2009 (Saatavilla: https://www.vahtiohje.fi/web/guest/valtionhallinnon–kansainvalisen–tietoturvayhteistyon–hallintamalli, 10.11.2015).
547. Valtiovarainministeriö: verkkosivut. Julkisen hallinnon ICT – Tietoturvallisuus – Voimassa olevat tietoturvaohjeet ja –määräykset. Saatavilla http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/. Viitattu 29.4.2014.
548. van der Ploeg, I.: Biometrics and the body as information. Normative issues of the socio–technical coding of the body. In Surveillance as Social Sorting by David Lyon (Ed.). Routledge. 2003.
549. van der Ploeg, I.: Genetics, biometrics and the informatization of the body. Ann Ist Super Sanità. 2007 Vol. 43, No. 1.
550. Van Dijk, J., The Network Society, Sage Publications 2012, 3rd Edition,
551. Vanto, Jarno J. Henkilötietolaki käytännössä. WSOYpro. Helsinki 2011.
552. Viestintäviraston NCSA–toiminnoista. Viestintävirasto ohje 7.5.2015 (Saatavilla: https://www.viestintavirasto.fi/attachments/Viestintaviraston_NCSA–toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf, 11.11.2015).
553. Viestintäviraston Toimalakatsaus 2/2015. S. 25. Julkaistu 31.08.2015. Saatavilla,

https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2015/toimialakatsaus22015.html.

554. Viestintäviraston Toimalakatsaus 3/2015. S. 25. Julkaistu 16.09.2015. Saatavilla, https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2015/toimialakatsaus32015.html.
555. Virtanen, Ilpo: Lausunnot henkilörekisterityöryhmän väliraportista. Tiivistelmä. Oikeusministeriön lainvalmisteluosaston julkaisu 19/1977. Helsinki 1977.
556. Virtual Currency Taxation seen on: http://www.vero.fi/fi–FI/Syventavat_veroohjeet/Henkiloasiakkaan_tuloverotus/Virtuaalivaluuttojen_tuloverotus (28450).
557. Voimassa olevat tietoturvasopimukset. Sisäministeriön www–sivut: http://www.formin.fi, Voimassa olevat tietoturvasopimukset, päivitetty 7.9.2015 (Saatavilla: http://formin.finland.fi/public/default.aspx?nodeid=49295&contentlan=1&culture=fi–FI, 16.11.2015).
558. Voorhees, J., Obama Defends NSA Surveillance: "Nobody Is Listening to Your Telephone Calls.", June 7 2013, http://www.slate.com/blogs/the_slatest/2013/06/07/obama_defends_nsa_surveillance.html/ (access September 2015),
559. Voutilainen, Tomi: ICT–oikeus sähköisessä hallinnossa – ICT–oikeudelliset periaatteet ja sähköinen hallintomenettely. Edita, Helsinki 2009.
560. W3C:n (World Wide Web Consortium) www–sivut (Saatavilla: http://www.w3.org, 10.11.2015).
561. Wadham, J., Human Rights and Privacy – The Balance, speech given at Cambridge (March 2000), http://www.liberty–human–rights.org.uk/mhrp6j.html (access October 2015),
562. Wallin, Anna–Riitta – Nurmi, Pekka: Tietosuojalainsäädäntö. 2. uudistettu painos. Lakimiesliiton kustannus: Helsinki 1991.
563. Wallin, Anna–Riitta – Nurmi, Pekka: Tietosuojalainsäädäntö. 2. uudistettu painos. Lakimiesliiton kustannus, Helsinki 1991.
564. Warren, S. D., Brandeis, L. D., The Right to Privacy, Harvard Law Review, 4(5), 1890,
565. Wayman, J.L.: Fundamentals of Biometric Technologies. Available at: http://www.engr.sjsu.edu/biometrics/publications_tech.html.
566. Webster, F., Theories of the Information Society, 4th Edition, Routledge 2014,

567. Westby, J. R., Project Chair (ed.), International Guide to Privacy. American Bar Association Privacy & Computer Crime Committee Section of Science & Technology Law, ABA Publishing 2004,
568. Wiese Schartum – Bygrave – Berge Bekken (eds.) Jon Bing En hyllest /// A Tribute (2014)
569. Woodward, J.D, Jr – Webb, K – Newton, E – Bradley, M – Rubenson, D: Army Biometric Applications: Identifying and Addressing Sociocultural Concerns, (2001). Available at: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1237.pdf.
570. WoodWard, J.D, Jr: Biometrics – Facing up to Terrorism, Rpt. IP–218 (Rand Publications 2001). Available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP218.pdf.
571. Woodward, J.D, Jr: Super Bowl Surveillance: Facing up to Biometrics, Rpt. IP–209 (Rand Publications, 2001). Available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP209.pdf
572. World's biggest biometric ID scheme forges ahead. BBC News. Available at: http://www.bbc.co.uk/news/world–asia–india–16979875.
573. WP 29: Lausunto 13/2011 älykkäiden mobiililaitteiden paikkatietopalveluista (WP 185). Annettu 16.5.2011. Saatavilla http://ec.europa.eu/justice/data–protection/article–29/documentation/opinion–recommendation/files/2011/wp185_fi.pdf. Viitattu 27.1.2014.
574. WP 29: Lausunto 4/2007 henkilötietojen käsitteestä (WP 136). Annettu 20.6.2007. Saatavilla http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fi.pdf. Viitattu 28.1.2014.
575. WP 29: Press Release. Brussels, 22 October 2013. Saatavilla http://www.tietosuoja.fi/uploads/rz25k5ifyunkt8.pdf. Viitattu 29.10.2013.
576. WP 29: verkkosivut. Saatavilla http://ec.europa.eu/justice/data–protection/article–29/index_en.htm. Viitattu 28.1.2014.
577. WP29 recommend to adopt a case by case approach "in order to strike the balance between the right to privacy and the right to public access" (Opinion 7/2003, wp 83). WP29 (Working Party 29) was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf

578. Wright, Georg Henrik von 1987: Tiede ja ihmisjärki. Keuruu: Otava.
579. Yhteinen tiedonanto euroopan parlamentille, neuvostolle, Euroopan talous– ja sosiaalikomitealle ja alueiden komitealle, Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö (JOIN(2013) 1 final) (Saatavilla: http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:FI:PDF, 16.11.2015).
580. Yhteiskunnan turvallisuusstrategia VNp 16.12.2010 (Saatavilla: http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit/doc_download/24–yhteiskunnan–turvallisuusstrategia, 11.12.2013).
581. YK:n suuntaviivat tietokoneistettujen henkilötietojen sääntelyyn, ENISA:n www–sivut, UN Guidelines (Saatavilla: http://www.enisa.europa.eu/activities/risk–management/current–risk/laws–regulation/data–protection–privacy/un–guidelines, 10.11.2015).
582. YK:n yleiskokous, suuntaviivat tietokoneistettujen henkilötietojen sääntelyyn. UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files. 14 Joulukuuta 1990. (Saatavilla:
583. Ylä–Kotola, Mauri & Arai, Mehdi 2000: Uusmediatieteen perusteet. Helsinki: Edita.
584. Ylä–Kotola, Mauri 1998. Tieteen ykseys, Hermann Friedmann ja transsendentalismi. Teoksessa Inkinen, Sam & Sundgren, Eva & Ylä–Kotola, Mauri (toim).: Mediatieteen kysymyksiä 2. Kirjoituksia modernista ja postmodernista kulttuurista. Mediatieteen julkaisuja C2. Rovaniemi: Lapin yliopisto.
585. Yleistä IT–standardisointityöstä, SFS:n www–sivut: www.sfs.fi (Saatavilla: http://www.sfs.fi/standardien_laadinta/sfs_n_tekniset_komiteat_ja_seurantaryhmat/it–standardisointi/it_–_yleistietoa, 16.11.2015).
586. Ylipartanen, Arto. Tietosuoja terveydenhuollossa, potilaan asema ja oikeudet