Het binnenste buiten

Liber amicorum ter gelegenheid van het emeritaat
van prof. dr. Aernout H.J. Schmidt,
hoogleraar Recht en Informatica te Leiden

Het binnenste buiten

Liber amicorum ter gelegenheid van het emiritaat van prof. dr. Aernout H.J. Schmidt, hoogleraar Recht en Informatica te Leiden

Redactie:
Laurens Mommers
Hans Franken
Jaap van den Herik
Franke van der Klaauw
Gerrit-Jan Zwenne

Lay-out: AlphaZet prepress, Waddinxveen

ISBN-978 90-815196-1-8

Foto: Edwin Walvisch
portfolio: www.walvisch.nl

Inhoudsopgave

Voorwoord

Dit vriendenboek bevat bijdragen van een groot aantal personen met wie Aernout Schmidt in de loop van zijn carrière aan de Universiteit Leiden heeft samengewerkt. Daaronder is ook een flink aantal doctores die hun bul mede kregen uitgereikt dankzij de begeleiding van Aernout. Omdat Aernout nooit voor één gat te vangen is geweest, komt de diversiteit van zijn interesses én van zijn vriendenkring tot uiting in de reikwijdte van de bijdragen.

Bij het classificeren van de bijdragen kwamen we niet verder dan een Wittgensteiniaanse familiegelijkenis: die van het belang het binnenste te kennen en naar buiten te brengen. Het binnenste van de techniek, door Aernout immer met gezond wantrouwen en grote nieuwsgierigheid benaderd. Maar ook het binnenste van de mens, door hem niet altijd begrepen, maar doorgaans 'at face value' geaccepteerd.

Aernout heeft verschillende 'helden' gekend, althans dat veronderstellen wij aan de hand van de boeken die hij ooit las, citeerde en bediscussieerde. Van Hofstadter en Geertz tot Fuller en Lessig, hij stopt nooit bij de grenzen van het recht, vermoedelijk omdat die niet bestaan. Zijn missie lijkt te hebben bestaan uit het 'injecteren' van belangrijke wetenschappelijke denkbeelden in een discipline waar vaak dranghekken worden geplaatst om het positieve recht.

Ver voordat in brede kring het vooruitgangsgeloof in kunstmatige intelligentie gematigd werd, verliet Aernout het pad van de 'harde' rechtsinformatica om het in te ruilen voor datgene waarin de potentiële vooruitgang enorm zou zijn: toepassing van ICT in de juridische beroepen. En toen het adagium 'Wat off-line geldt dient ook on-line te gelden' in brede kring nog voor zoete koek werd geslikt, stond Aernout daar al buitengewoon kritisch tegenover.

Het zal de lezer dan ook niet verbazen dat de bijdragen aan dit boek zich niet licht laten vangen in geheide thema's. Des te toepasselijker is dan ook het feit dat Aernout hartelijk (om niet te zeggen: bulderend) kan lachen om een indeling van dieren uit een boek van de schrijver Borges: dieren die eigendom zijn van de keizer, zwerfhonden, dieren die in deze indeling voorkomen, die juist een kruik gebroken hebben, en die uit de verte op vliegen lijken.[1]

---

1 De complete indeling bestaat uit dieren "a) die de Keizer toebehoren, b) gebalsemde, c) tamme, d) speenvarkens, e) sirenen, f) fabeldieren, g) loslopende honden, h) die in deze indeling voorkomen, i) die in het rond slaan als gekken, j) ontelbare, k) die met een fijn, kameelharen penseeltje getekend zijn, l) et caetera, m) die juist een kruik gebroken hebben, n) die uit de verte op vliegen lijken", J.L. Borges, *Otras inquisiciones (1937-1952*), Buenos Aires, Sur, 1952.

Het lichte onbehagen dat deze absurdistische typologie oproept, nam ook van ons bezit bij pogingen om de bijdragen aan het boek in thema's in te delen. We willen daarom graag benadrukken dat die thema's eigenlijk voornamelijk dienen om de suggestie te wekken dat wij greep hadden op de inhoud van het boek. Anders dan nieuwe media bieden boeken niet echt de mogelijkheid om één bijdrage in meerdere thema's in te delen, iets wat juist in dit geval van bijzonder nut was geweest.

Stoort u zich dan ook vooral niet aan de thema's grensgevallen, informatierecht, methode, praktijk, privacy, transparantie, want zij betekenen in het geheel niets. Zij zijn vooral een manier om – zoals het hoort – dit boek netjes in stukken op te delen.

In het deel Grensgevallen zijn bijdragen te vinden over de werken van Karen Armstrong (Cliteur, Why I had not read Karen Armstrong (but I have now)), overheidsfalen als variant op marktfalen (Dolfsma, Government Failure – 4 types), rechters en (gebrek aan) kennis van statistiek (Gill, Lies, damned lies, and legal truths), het intellectuele modernisme in het Wenen van begin 20e eeuw (Polčák, Quem ad Finem: To the Limits of Modernity), en wetgeving concipiëren conform het model van open-source software (Siewicz, Free Software and the Law; on collaborative law-making and adjudication).

In het deel Informatierecht zijn bijdragen te vinden over de actuele stand van de grondrechtencatalogus in Nederland op het gebied van o.m. uitingsvrijheid (Groothuis, Informatievrijheid en digitalisering. Ontwikkelingen in jurisprudentie en regelgeving), de verhouding tussen publieke en private media en hun diensten op internet (Hins, Publieke media op internet: zorgplicht en concurrentievervalsing), de vergoeding voor privé-kopiëren in internationaalrechtelijk kader (Van der Net, De nabuurrechtelijke aanspraak op een billijke vergoeding voor privé-kopiëren naar internationaal recht), en de moeizame verhouding tussen file sharing en auteursrecht (Siemerink, File sharing bedreigt handhaving auteursrecht).

Het deel Methode bevat een aantal bijdragen over de methode van de (ICT-)rechtsgeleerdheid. Het gaat om een vergelijking van de methode van de rechtsgeleerdheid met enkele andere disciplines (Beunen, De geesteswetenschappen, rechtsgeleerdheid en kunstgeschiedenis vergeleken), de rol van ICT bij het vermijden van schijn (Van Esch, Schijn verdwijnt waar ICT verschijnt), een analyse van de (vermeende) ICT-juridische methode (Hage, Heeft ICT-recht een eigen methode?), informaticamethoden voor informatieuitwisseling en –ranking (Jaap van den Herik, Van registratie naar verwerking) en de vergelijking tussen economische en rechtswetenschap (Wierda, Limits and Dimensions).

Het deel Praktijk gaat in op de rol die ICT speelt in de juridische beroepen en de juridische praktijk. Hierin zijn bijdragen te vinden over de rol van kennismanagement bij de consistentie van straftoemeting (Apistola, Towards a Preliminary Knowledge Management Reasoning System to Improve Consistency of Sentencing), ICT in arbitrageprocedures (Fokker, E-discovery), ICT in de Nederlandse rechtspraktijk (Van den Hoogen, E-Justice: nieuwe

kansen voor onderzoek naar ICT en recht), en de rol van computers in het werk van wetgevingsjuristen (Voermans, Computers kunnen er niks van!).

Het deel Privacy bevat bijdragen op het gebied van onder meer de economische waarde van persoonsgegevens. De bijdragen betreffen de berekening van rendementen op privacybeschermende maatregelen (Borking, Assessing investments mitigating privacy risks), de commodificatie van privacy (Hildebrandt, Recht en markt: met falen en opstaan), de verschuiving van gegevens naar identiteiten als te beschermen object (Prins, Digital Diversity: Protecting Identities Instead of Individual Data), privacybescherming op weg naar singulariteit (Schermer, Privacy and Singularity: little ground for optimism?) en verbetering van de regulering van verwerking van IP-adressen (Zwenne, Over persoonsgegevens en IP-adressen, en de toekomst van privacywetgeving).

Het deel Transparantie, ten slotte, bevat bijdragen op het gebied van rechten op de transparantie van het openbaar bestuur en de toegang tot het recht. De bijdragen gaan over ICT-initiatieven op het gebied van transparantie van het Amerikaanse openbaar bestuur (Adamski, Change We Can Believe In or Politics As Usual?), de vraag hoe het landelijk elektronisch patiëntendossier past in het licht van Aernout's oratie (Franken, Is het elektronisch patiëntendossier een bedreiging voor de rechtsstaat?), de vraag of toegang tot het recht als grondrecht kan worden geconstrueerd (Mommers, Toegang tot juridische informatie als grondrecht), transparantie als grondrecht (Snellen, Towards transparency as a basic human right) en toegankelijkheid van standaarden waarnaar in regelgeving wordt verwezen (Stuurman, Public access to standards: some fundamental issues and recent developments).

Wij wensen in de allereerste plaats de kersverse emeritus veel leesplezier met de artikelen in dit liber amicorum. Dat wensen wij uiteraard ook de andere lezers. En op deze plaats willen wij graag onze dank uitspreken aan de auteurs voor hun geslaagde pogingen het binnenste naar buiten te halen. De redactie was in handen van een aantal collega's van Aernout bij eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij.

Leiden, januari 2010

Laurens Mommers
Hans Franken
Jaap van den Herik
Franke van der Klaauw
Gerrit-Jan Zwenne

DEEL I

GRENSGEVALLEN

Why I had not read Karen Armstrong (but I have now)

Paul Cliteur■

Aernout Schmidt is what I consider to be a 'real professor' and a great academic scholar. The greater part of my academic career at the law faculty of the University of Leiden I worked together with Aernout on the same research project (Social cohesion, multiculturalism and globalization) and in the same department (now: the Institute for the Interdisciplinary Study of the Law). Aernout always struck me as an impressive scholar for two reasons.

First, Aernout was never afraid to start reading very difficult books, apparently without feeling intimidated. I recall Aernout walking around with Douglas Hofstadter's *Gödel, Escher and Bach* (1979) as something he would devour during lunch break.[1] A second reason is that Aernout was not only eager to read difficult books but he was also willing to discuss the content of those books during discussion sessions with other members of the staff and the most gifted students. More than once he also tried to organize those sessions.

I always had a vague excuse not to attend to those sessions, also because the books Aernout selected were too difficult for me or too time-consuming to read. I remember an exhortation by Aernout to read and subsequently discuss Phillip Bobbitt's *The Shield of Achilles: War, Peace and the Course of History* (2002). I bought the book (I have all the books Aernout selected on my bookshelves), noticed that this was more than 900 pages long and did not read it.[2] Another book I bought and subsequently did not read on Aernout's advice was Lawrence Lessig's *Code: and some other laws of cyberspace* (1999). (This time there was not a reasonable excuse; the book is 250 pages long).

As far as I remember there was one book we actually did read together with a small and rapidly dwindling group: the English translation of Ferdinand Tönnies's *Gemeinschaft und Gesellschaft* (1887). All things considered this is not a very impressive record in the light of Aernout's expectations of his direct scholarly ambiance.

Yet on the threshold I hope to rehabilitate myself a bit. I will try to do this by making some remarks on a book that I did not read either at the time this was suggested by Aernout, but which I have read afterwards. That book is Karen Armstrong's *The Battle for God: Fundamentalism in Judaism, Christianity*

■ Paul Cliteur is full professor at the Leiden Law Faculty.

1 Hofstadter 1979.

2 Bobbitt 2002.

and Islam (2000).[3] This time my reluctance to read the book was not inspired by ordinary laziness but a kind of ideological resistance. I 'knew' (without having read the book) that this book would be a bad book. Now that I have read the book I know why. Here are my reasons.

All religions equally beautiful

Karen Armstrong (1944-) is one of the most widely read authors on religion nowadays. She rose to prominence 1993 with *A History of God*, a study in comparative religion and the key figures that have shaped the different religions.[4] Armstrong's central thesis is that all religions are equally beautiful and that it is only fundamentalist approaches (equally dispersed over all religions) that are responsible for the violence connected with religion.[5] Armstrong is also convinced that all religions basically teach the same.[6] They all subscribe to the Golden Rule: do unto others what you would have others do unto you.

This view of religion is all very well, of course, as a profession of faith, but this approach leaves much to be desired as a scholarly orientation because it cannot explain violence. Are there really no moorings for violence in the religious traditions themselves? Is violence something that comes from outside the traditions and is it completely alien to those traditions themselves? Why does it occur more often in some traditions than in others? Why more under some historical conditions than in others?

Armstrong's books affirm people in their most sacred beliefs but are, from a scholarly point of view, more problematic. In particular after the September 11, 2001 attacks she was much in demand on the lecture circuit where she pleas for inter-faith dialogue. The contradictions between religion and modern life are explained by focusing on the misguided interpretations that fundamentalists give to their religious tradition. This attitude is clearly manifested in her book on the interpretation of the Bible: *The Bible* (2007).

Her starting point in *The Bible* is sacred books, Holy Writ or Scripture. In nearly all the major faiths, she says, people have regarded certain texts as sacred and ontologically different from other documents. "They have invested those writings with the weight of their highest aspirations, most extravagant hopes and deepest fears, and mysteriously the texts have given them something in return."[7]

Yet Armstrong has also noticed that scriptural authority has acquired a dubious flavour. "Today scripture has a bad name", she writes. "Terrorists

3 Armstrong 2000.
4 Armstrong 1993.
5 Armstrong 2000.
6 See on this: Antes 2007, who contends that the thesis that all religions say the same cannot be maintained empirically.
7 Armstrong 2007, p. 2.

use the Qur'an to justify atrocities, and some argue that violence of their scripture makes Muslims chronically aggressive. Christians campaign against the teaching of evolutionary theory because it contradicts the biblical creation story. Jews argue that because God promised Canaan (modern Israel) to the descendants of Abraham, oppressive policies against the Palestinians are legitimate."[8] There has been a scriptural revival that has intruded into public life, Armstrong concludes. And especially against those political manifestations of religion is secularist criticism directed. "Secularist opponents of religion claim that scripture breeds violence, sectarianism and intolerance; that it prevents people from thinking for themselves, and encourages delusion. If religion preaches compassion, why is there so much hatred in sacred texts?"[9]

That is a good question indeed. And it makes readers undoubtedly curious about her answer. Alas, that answer is not very satisfying. Basically, her answer boils down to the contention that it is all a matter of interpretation. What she tries to do in her book on the Bible is to make two claims. First, she makes an analytical point. This is that allegorical reading of scripture is perfectly legitimate. Second, there is a historical claim. Armstrong argues that an exclusively literal interpretation of the Bible is a "recent phenomenon". Armstrong thinks, for instance, that until the 19th century very few people imagined that the first chapter of Genesis was a factual account of the origins of life. For centuries, Jews and Christians relished "highly allegorical and inventive exegesis, insisting that a wholly literal reading of the Bible was neither possible nor desirable."[10]

I think both claims are dubious but for different reasons. As a historical argument it would be wrong to claim that literalist interpretations were completely unknown in the past and literalism is an invention of modern fundamentalists.[11] The tendency to take Scripture as literally true was much more widely dispersed in earlier times than in our time. Historical research can point this out. But that is not the point I want to focus on. I want to concentrate on the analytical claim. What is more important is that Armstrong also seems to be an adherent of semantic relativism. And how she reconciles this with her claim of the sacredness of the texts remains unclear. All the same, the reason why she believes this is crystal clear: we do not have to take the

8 *Idem.*

9 *Ibid.*, p. 3.

10 *Ibid.*, p. 3.

11 See: White 1896, p. 305: "The Reformers, having cast off the authority of the Pope and of the universal Church, fell back all the more upon the infallibility of the sacred books. The attitude of Luther toward this great subject was characteristic. As a rule, he adhered tenaciously to the literal interpretation of the Scriptures." See also the Cambridge theologian: Raven 1952, p. 10 who says: "The earliest Reformers alike in science and in religion were not liberals but conservatives, bent upon recalling mankind to an earlier and truer wisdom rather than upon exploring uncharted seas. Hence comes their reverence for the written word, their insistence upon the infallibility of their authorities." For another testimony according to these lines, see Huxley 1892, p. 98.

problematic passages in Scripture seriously, because we can simply focus on what we like. "Interpretation" always provides the way out. What Armstrong wants to demonstrate in her book is that from the first, biblical authors felt free to "revise texts they had inherited and give them entirely different meaning".[12] Later exegetes held up the Bible as the template for the problems of their time. This somewhat relaxed way of dealing with Scripture seems very attractive to Armstrong. About the attitude of those "exegetes" with regard to Scripture she writes:

Sometimes they allowed it to shape their world-view but they also felt free to change it and make it speak to contemporary conditions. They were not usually interested in discovering the original meaning of a biblical passage. The Bible "proved" that it was holy because people continually discovered fresh ways to interpret it and found that this difficult, ancient set of documents cast light on situations that their authors could never have imagined. Revelation was an ongoing process; it has not been confined to a distant theophany on Mount Sinai; exegetes continued to make the Word of God audible in each generation.[13]

This is a revealing passage that sums it all up. But there are some pertinent questions to be posed with regard to this approach. Let us look more closely at the passage quoted before.

Those exegetes that Armstrong admires for their relaxed attitude towards Scripture "sometimes" allowed it to shape their world-view but "they also felt free to change it" and "make it speak to contemporary conditions".

An obvious question then is: "In what situations did those exegetes choose to let their world-view be changed by Scripture and in what situations did they resist and decide *vice versa* to change Scripture?" The dilemma seems to be this: either we are changed by Scripture or Scripture is changed by us. The traditional approach seems to be that we have to be changed by Scripture, but according to Armstrong and the liberal exegetes from the past she admires so much, it is also perfectly legitimate to change Scripture. But how do those "exegetes from the past" decide one way or the other? Armstrong does not give us an answer to that pertinent question, at least not explicitly.

A second question that can be posed with regard to the passage quoted from Armstrong's book is: what exactly were those liberal exegetes doing? One thing is sure, according to Armstrong "they were not usually interested in discovering the original meaning of a biblical passage". But if that was not the focus of their interest, what was exactly? From the traditional perspective is it clear what the meaning of Scripture is. Scripture informs us about the divine. It tells us what a personal, omnipotent and perfectly good God wants us to do. In Scripture God "reveals" his will ("Thy will be done, as in heaven, so on earth." Matt. 6:10).

12 Armstrong 2007, p. 4.
13 *Ibid.*, p. 5.

A respectful intercourse with the divine would suppose, so it seems, that the exegete scrupulously tries to ascertain what the meaning of Scripture is, in order to know what God has in mind for mankind. But apparently the exegetes that Armstrong favours are not interested in this type of question. But what is *their* focus of interest?

Is Scripture "sacred"?

Armstrong also introduces a completely new, and we may say revolutionary, way to look at the "sacredness" of Scripture. In the traditional view Scripture is sacred because it informs us about the eternal plans God has for the world. "In its specifically theological usage, the term (Scripture) serves to identify the written and authoritative word of God rather than any specific textual content."[14] Scripture presents us with moral values and rules that have eternal significance. The Bible was held in high esteem, because there we were provided with the moral injunctions that are not the whims of fashion, the human, all too human, ideas about right and wrong, but absolute and universal guidelines. The whole idea of texts that are sacred and, in the words of Armstrong, "ontologically different", is based on this presumption.

But what does Armstrong do? She tells us that the Bible "proved" that it was holy because people could continually discover "fresh ways to interpret it". So what makes the Bible holy is not its fixed meaning, but exactly the opposite: it has no meaning at all because meaning constantly changes over time. It is merely logical that from here she continues with another disconcerting vision, *viz.* that in this conception of scripture "revelation was an ongoing process". So what has been revealed today as higher wisdom can be obsolete tomorrow. The Ten Commandments revealed on Mount Sinai and one of the most authoritative parts of the Bible, because written or at least dictated by God himself,[15] can in the future be abolished by new insights and this should not convince us of the relative character of the text of the Bible but of its sacredness. The sacredness of the text is exactly that everything is possible. Or, to put it somewhat more instrumentally, Scripture is sacred because it can be used by the exegete for all he or she wishes.

Armstrong is very supportive of the exegesis by the rabbis called *midrash.* This is derived from the verb *darash* meaning "to investigate" or "to seek".[16] The meaning of a text is not "self-evident", so Armstrong tells us. "The exegete had to go in search of it, because every time a Jew confronted the Word of God in scripture, it signified something different. Scripture was inexhaustible."[17]

14 McBrien 1995, p. 1171.
15 See on this: Lewis 1946.
16 Armstrong 2007, p. 81.
17 *Ibid.*, p. 81.

These are revealing words. That the meaning of a text is not self-evident is not very surprising, to be sure, but that *every time* a text is read there exists a new meaning is nothing short of magic. This would make – if it were true – all human communication impossible.

Also the pretension that Scripture is "inexhaustible" is a bit strange. How does Armstrong know? History is still not at an end, so theoretically there may be a point in time where Scripture is really "exhausted". Or is the "inexhaustibility of Scripture" all that the religion of Armstrong and the rabbis she quotes amounts to? I mean: they apparently do not believe in an eternal God who reveals his ideas to mankind but in a kind of magic phenomenon called "Scripture" that makes it possible for them to "get revealed" to them exactly what they want to hear each time this "Scripture" is consulted by them. Is the essence of their faith perhaps a kind of *fetishism:* they believe that one specific book that has in the past sent out new messages to different people all the time will continue to do so till the end of times? If that's the case, fine, but people who believe such a thing would be the creators of a whole new religion, so it seems.

Ordinary books and sacred books

What Armstrong seems to do, is equate the Bible with what we call a classic work. This already appeared in her first book that gained a worldwide audience: *A History of God* (1993). It is here that she writes about the founder of Islam and states: "It is not surprising that Muhammad found the revelations such an enormous strain: not only was he working through an entirely new political solution for his people, but he was composing one of the great spiritual and literary classics of all time."[18] As one commentator has rightly remarked: "This is high praise for a fellow composer perhaps, but nonetheless reductionist in its familiar repetition of the old cornerstone of Jewish and Christian excising God from the authorship of the Holy Qur'an."[19] Philosopher John Haldane (1954-) refers to some modern liberal theologians and adds that if the first Christians had taken their view it is hard to believe that Christianity would have survived the lifetimes of the apostles.[20] That remark is relevant for the work of Armstrong as well, so it seems.

What do we understand by a "classic"?[21] Or, as Armstrong says: "a great spiritual and literary classic"? The word "classic" refers to a specific quality of a book, play or work of art that does not antiquate. Common examples are the plays of Shakespeare or the *Iliad* and *Odyssey* of Homer.[22] Every new generation can read those books or see those plays performed on stage and

18 Armstrong 1993, p. 164.
19 Mason 1995, p. 481.
20 Haldane 2003, p. 28.
21 See on this: Young 2000; Henrie 2000.
22 See on Shakespeare: Bloom 1998.

see new things in it, discover new shades of meaning. That makes those plays interesting, but does it make them "holy" or "sacred"?

As can be expected, Armstrong's vision on biblical interpretation is intimately connected with her vision on what religion should be and what she considers a perversion of religion. Religion, so Armstrong tells us, "is a practical discipline that teaches us to discover new capacities of mind and heart".[23] She also calls religion "a skill" that requires perseverance, hard work and discipline. "Some people will be better at it than others, some appallingly inept, and others will miss the point entirely."[24]

It is clear that with such a definition of religion any criticism of religion can easily be discarded as "missing the point" or "appallingly inept". Actually it immunizes religion entirely from any type of critique. Any justified criticism of religion is always criticism of something that aspires to be religion but should be carefully distinguished from religion: fundamentalism. "Fundamentalism" Armstrong sees as the "perversion of religion". It is something that we encounter in all religions. She writes:

The Western media often give the impression that the embattled and occasionally violent form of religiosity known as "fundamentalism" is a purely Islamic phenomenon. This is not the case. Fundamentalism is a global fact and has surfaced in every major faith in response to the problems of our modernity. There is fundamentalist Judaism, fundamentalist Christianity, fundamentalist Hinduism, fundamentalist Buddhism, fundamentalist Sikhism and even fundamentalist Confucianism.[25]

Then the question is: how do we discern true religion from fundamentalism? In her book on fundamentalism she develops an analysis in which fundamentalism is seen as the attempt in various religions to turn *mythos* into *logos.* That means that religion in its pristine state is, according to Armstrong, *mythos*.[26] But what serious believer could go along with that? This definition of "fundamentalism" would make the overwhelming majority of serious believers "fundamentalists". Only those who, like Armstrong, would be prepared to let their religious convictions evaporate into myths would be considered believers in the positive sense of the word – the rest are all dubbed "fundamentalists".

This view, often presented as "moderate", is in fact extreme and something no serious believer could subscribe to. But also from a non-religious analytical or scholarly point of view it is not very satisfying. It misses what believers consider important in their religion.

---

23 Armstrong 2009, p. 1.

24 *Ibid.*, p. 4.

25 Armstrong 2002, p. 164.

26 See on this: Thomas 2001. Armstrong's ideas about myths are elaborated in: Armstrong 2005. "Human beings have always been mythmakers" (p. 1), she writes, and this will always remain so, one may understand from her book. She deplores that since the Greeks there was a rift between mythos and logos (p. 102). See also: Armstrong 2009, p. 1.

Liberal believers usually react to criticism along the lines outlined above with an accusation. They say: "You argue just like the fundamentalists. Why shouldn't it be allowed to modernize religious traditions? You want to relegate religious texts to the dustbin of history, don't you?" But these are all *ad hominem* arguments, that is to say: fallacies and evasions of the issue. That someone argues "just like the fundamentalists" is irrelevant. The question is: are the fundamentalists right with regard to the issue that is under consideration? And it may well be that the fundamentalists are *wrong* as far as they are prepared to use violence, *wrong* in that they do not want to discuss their presuppositions, but *right* in the sense that their vision on what distinguishes sacred texts from classic books is much more convincing than the vision expounded by liberal believers. It is also an unfounded allegation that critics of the liberal approach to belief are motivated by the urge not to modernize religious traditions. The issue at stake is: *how* are we going to do that? The critics of religious traditions I have in mind advocate the open acceptance of moral autonomy. The vision on scriptural interpretation of moral secularists is that we accept or reject biblical values and norms on the basis of *moral* criteria, not *religious* criteria. The yardstick with which we measure the moral value of scriptural passages is itself not a principle derived from Scripture. And it is a principle of scholarly and moral integrity to make that clear.

The British philosopher (1902-1996) had some very pertinent advice for the interpreters of Scripture. "To interpret the gospels correctly you must read them with what may be called interpreter's piety, that is, the will to receive into your mind the exact meaning the author intended, however strange or repellent or boring it may turn out to be."[27]

It requires no elaborate argumentation that this is the exact opposite of what Karen Armstrong requires an interpreter to do. What Robinson calls "interpreter's piety" means that you should try to ascertain as objectively as possible what is *in the text* (textualism) and/or what the *intentions* were of the person, group of persons or institution that made the text (intentionalism). Armstrong has no patience for such an exercise. She (and the rabbis she admires so much) are not busy with the text but with *their own* moral ideas. But exactly that, so Robinson would argue, makes them violators of "interpreter's piety". If you want to know what a "Christian ethics" looks like then you have to gauge what Christ said and what he meant, not what you, the interpreter, hope he said. "I urge you to do this, or at least not to use the phrase 'Christian values' until you have done it."[28]

To further illustrate this point let us pay some attention to what Armstrong finds so refreshing in the Jewish tradition of interpreting Scripture. She refers to the tradition of midrash and says: "Above all, midrash must be guided by the principle of compassion."[29] On the basis of this guideline

27 Robinson 1975, p. 142.
28 *Ibid.*, p.142.
29 Armstrong 2007, p. 82.

Armstrong says, referring to the great Jewish religious leader Hillel (*c.* 60 BCE-10 CE): "The essence of Torah was the disciplined refusal to inflict pain on another human being. Everything else in the scriptures was merely 'commentary', a gloss on the Golden Rule."[30] Hillel also had a clear vision on the way the Torah should be studied by the exegetes: "When they studied Torah, rabbis should attempt to reveal the core of compassion that lay at the heart of all the legislation and narratives in the scriptures – even if this meant twisting the original meaning of the text."[31] R. Akiba (*c.* 50-135 CE), the leading sage of the later Yavneh period, declared that the greatest principle of the Torah was the commandment of Leviticus: "Thou shalt love thy neighbor as thyself'" (Leviticus 19:18).

Many people will read this with approval. But the relevant question is: *what* do we like in those words? What we like in those words, so it seems, are the *moral guidelines* that are being proclaimed, but that is crucially different from the *theory of interpretation* that is presented (if we are kind enough to call this a "theory" at all). The moral principles presented here are: (1) Compassion;[32] (2) With as consequence refusal to inflict pain; (3) The golden rule.

The German philosopher Arthur Schopenhauer (1788-1860), who made "compassion" the cornerstone of his ethics, would have been satisfied.[33] And his British colleague Jeremy Bentham (1748-1832) would have been happy with the consequence drawn from this principle: "Never inflict pain". This means the rabbis were true followers of Schopenhauer or (on the basis of the second inference) utilitarians.[34] And finally they were Kantians as well: they advocated the golden rule.[35] So apparently the Torah is a commentary on Schopenhauer, Bentham and Kant.

Now, Hillel knew that there are things in the Torah that do *not* accord with Schopenhauer, Bentham and Kant. What to do with those passages? Well, the rabbis should *attempt* to reveal the core of compassion that lies at the heart of Scripture, according to Armstrong. But what if that appears impossible? In that case "twisting the original meaning of the text" is allowed, Armstrong approvingly remarks.

---

30 *Ibid.*, p. 83. See also: White 1896, p. 293: "It can not be forgotten that Rabbi Hillel formulated the golden rule, which has before him been given to the extreme Orient by Confucius, and which afterward received a yet more beautiful and positive emphasis from Jesus of Nazareth."

31 Armstrong 2007, p. 83.

32 See also *ibid.*, p. 84: "R. Johanan had shown that, as Hillel claimed, charity was indeed central to scripture: it was the exegete's job to elucidate this hidden principle and bring it to light."

33 See: Schopenhauer 1840.

34 See on the ethics of Bentham: Bentham 1789.

35 Kant 1785, p. 51: "Der categorische Imperativ ist also nur ein einziger, und zwar dieser: handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, daß sie ein allgemeines Gesetz werde."

What is the conclusion we have to infer from this "theory" of interpretation? The only conclusion seems to be that in case of conflict between some passages of the Torah on the one hand and Schopenhauer, Bentham and Kant on the other, it is those philosophers who have the final word. The value of compassion, the principle never to inflict pain and the golden rule have the final word, not Scripture. Scripture is moulded according to those values and principles; the principles are not derived from Scripture and neither can they be abolished on the basis of Scripture.[36]

Richard Dawkins makes this point when he summarizes his treatment of this issue with the words:

My main purpose here has not been to show that we *shouldn't* get our morals from scripture (although that is my opinion). My purpose has been to demonstrate that we (and that includes most religious people) as a matter of fact *don't* get our morals from scripture.[37]

Does Armstrong agree with Dawkins?

There are some, although only a few, passages where it seems to dawn upon Armstrong that this "theory" is no theory at all. On the liberal interpretation of the rabbis so much admired by her she tells us: "To a modern scholar, this seems to violate the integrity of the text, and seeks meaning at the expense of the original".[38] But that conscientious objection (reminiscent to Robinson's "interpreter's piety") is silenced immediately in the sentence following upon the passage just quoted: "But the rabbis believed that because scripture was the word of God, it was infinite. Any meaning that they discovered in a text had been intended by God if it yielded fresh insight and benefited the community."[39]

This is a kind of wordplay with the word "infinity". Because God is "infinite" his Scripture is presupposed to be "infinite" in meaning as well. Subsequently we are being informed what this "infinity" in meaning implies: it gives a free license to the caste of interpreters to project into the text whatever benefits the community (or rather what *they think* benefits the community). But if Scripture is always interpreted against the background of the three principles mentioned before (show compassion; never inflict pain; apply the golden rule) it is far from "infinite". It is highly restricted. If Scripture com-

36 Richard Dawkins comes to a similar conclusion when he writes in Dawkins 2006, p. 275: "we pick and choose among the scriptures for the nice bits and reject the nasty. But then we must have some independent criterion for deciding which are the moral bits: a criterion which, wherever it comes from, cannot come from scripture itself and is presumably available to all of us whether we are religious or not."

37 *Ibid.*, p. 283. See also *ibid.*, p. 298: "the holy books do not supply any rules for distinguishing the good principles from the bad".

38 Armstrong 2007, p. 86.

39 *Ibid*.

mands the destruction of another people (see for instance Numbers 31) the enlightened interpreters will tell us that this could not be the intention of the maker of the text. This is all fine, but it proves that the range of interpretations is restricted.

There is another conclusion we have to draw from the passages quoted from Armstrong. That is that not only the *rabbis* are a combination of utilitarians, Kantians and followers of Schopenhauer but that *God himself* is as well. If Armstrong or the rabbis read something in Holy Scripture that contradicts the principles expounded by the philosophers mentioned, this will not be accepted as "divine". So not a free divine will is authoritative for the liberal believers, but "the benefit of the community" is the real guiding line for interpretation. There is nothing against this, of course, but at the same time it is nothing special.

References

Antes 2007
Antes, Peter, "Sagen alle Religionen dasselbe?", in: *Marburg Journal of Religion,* Volume 12, No. 1, (May 2007), pp. 2-10.

Armstrong 1993
Armstrong, Karen, *A History of God: From Abraham to the Present: the 4000-Year Quest for God,* Heinemann, London 1993.

Armstrong 2000
Armstrong, Karen, *The Battle for God: Fundamentalism in Judaism, Christianity and Islam,* HarperCollins, London 2000.

Armstrong 2002
Armstrong, Karen, *Islam: A Short History,* Random House, Toronto 2002, p. 164.

Armstrong 2005
Armstrong, Karen, *A Short History of Myth,* Canongate, Edinburgh, New York, Melbourne 2005.

Armstrong 2007
Armstrong, Karen, *The Bible: The Biography,* Atlantic Books, London 2007.

Armstrong 2009
Armstrong, *The Case for God: What Religion Really Means*, The Bodley Head, London 2009.

Bentham 1789
Bentham, Jeremy, *An Introduction to the Principles of Morals and Legislation,* Edited by J.H. Burns and H.L.A. Hart, Methuen, London/New York 1982 (1789).

Bloom 1998
Bloom, Harold, *Shakespeare: The Invention of the Human,* Riverhead Books, New York 1998.

Bobbitt 2002
Bobbitt, Philip, *The Shield of Achilles: War, Peace and the Course of History,* Penguin Books, London 2002.

Dawkins 2006
Dawkins, Richard, *The God Delusion,* Paperback edition, Black Swan, Transworld Publishers, London 2006.

Haldane 2003
Haldane, John, *An Intelligent Person's Guide to Religion,* Duckworth Overlook, London, New York, Woodstock 2003, p. 28.

Henrie 2000
Henrie, Mark C., *A Student's Guide to the Core Curriculum,* ISI Books, Wilmington, Delaware 2000.

Hofstadter 1979
Hofstadter, Douglas, *Gödel, Escher, Bach: an eternal golden braid,* Basic Books, New York 1979.

Huxley 1892
Huxley, Thomas Henry, "Naturalism and Supernaturalism", 1892, in: Thomas Henry Huxley, *Agnosticism and Christianity.* And other Essays, Prometheus Books, Buffalo, New York 1992, pp. 92-118.

Kant 1785
Kant, Immanuel, *Grundlegung zur Metaphysik der Sitten,* (1785), in: *Werkausgabe,* Band VII, Hrsg. W. Weischedel, Suhrkamp, Frankfurt am Main 1981, pp. 11-102.

Lewis 1946
Lewis, Joseph, *The Ten Commandments: An Investigation into the Origin and Meaning of the Decalogue and an Analysis of its Ethical and Moral Value as a Code of Conduct in Modern Society,* Freethought Press Association, New York, NY 1946.

Mason 1995
Mason, Herbert, "Review of A History of God by Karen Armstrong", in: *The American Historical Review,* Vol. 100, No. 2 (Apr., 1995), pp. 481-482.

McBrien 1995
McBrien, Richard P., *The HarperCollins Encyclopedia of Catholicism,* HarperCollins Publishers, New York, NY 1995.

Raven 1952
Raven, Charles E., "Religion & Science: A Diagnosis", L.T. Hobhouse Memorial Trust Lecture, No. 16, delivered on 1 may 1946, in: *Hobhouse Memorial Lectures 1941-1950,* Oxford University Press, London 1952, pp. 3-16.

Robinson 1975
Robinson, Richard, *An Atheist's Values*, Blackwell 1975.

Schopenhauer 1840
Schopenhauer, Arthur, *Über die Grundlage der Moral,* in: *Sämtliche Werke,* Band III, Cotta-Verlag/Insel-Verlag, Stuttgart/Frankfurt am Main 1976 (1840), pp. 631-815.

Thomas 2001
Thomas, Scott M., "Review of The Battle for God: fundamentalism in Judaism, Christianity and Islam", in: *International Affairs,* Vol. 77, No. 1, (Jan., 2001), pp. 194-196.

White 1896
White, A.D., *A History of the Warfare of Science with Theology in Christendom,* Volume 2, Dover Publications, New York 1960 (1896).

Young 2000
Young, R.V., *A Student's Guide to Literature,* ISI Books, Wilmington, Delaware 2000.

Government Failure – 4 types

Wilfred Dolfsma[■]

> *"1. We regard the state as an agency whose positive assistance is one of the indispensible conditions of human progress."*[1]

Introduction

The way in which economists have looked at the state and its effects on the economy has fluctuated substantially over time.[2] Nowadays, economists tend to see the market as a default option for social order, and a role for government only when markets fail. In contrast to what is the first substantial article in the first constitution of the American Economic Association – the most influential among associations of economists – governments are largely seen as affecting the workings of an economy negatively if and when they do more than a 'Nightwatch state' would.

Markets are typically believed to fail under circumstances of (excessive) externalities that are either positive or negative, in cases when public goods are traded, in case of increasing returns or a natural monopoly creating market imperfections, or, possibly, according to some, to correct unequal distribution of wealth or income. Social and institutional economic thinking has been much more amenable to a role for government in the economy. Its role, when explicitly investigated, is seen as benevolent in principle. Institutional economics recognizes that markets cannot function if not embedded in a broader set of interrelated institutions.

Developing a convincing analysis of the role of government in economic processes, however, needs to start by considering government failure. Government failure is not the flip-side of the coin of market failure: there is no theory of 'non-market failure' as of yet.[3] Drawing on insights from law, the

---

■ Wilfred Dolfsma is full professor at the University of Groningen, specializing in innovation. University of Groningen, School of Economics and Business, PO Box 800, 9700 AV Groningen, Netherlands, ph. +31-50 363 3453, fax. +31-50 363 7110, w.a.dolfsma@rug.nl.

1 From: Article III (Statement of Principles) of the Constitution By-Laws and Resolutions of the American Economic Association, *Publications of the American Economic Association* 1(1) (March 1886), pp. 35-46, at p. 35.

2 Medema 2003.

3 Cf. Wolf 1997. Wolf (p. 64 ff), however, perceives of non-market failure as circumstances that lead to a rise in the price of the services it offers. He thus seems to follow the logic of determining market failures – externalities, public goods, increasing returns, and possibility merit goods – that are also apparent by their effect on what would otherwise be a 'natural' price.

philosophy of law and law & economics, I will develop some ideas to understand government failure. To see what exactly the role of government can be in an economy, one can approach from the opposite direction, asking 'When will a government fail?' I propose a framework for understanding government failure from a social and institutional perspective. I thus identify and develop 4 different types of government failure. Government can set rules[4] for economic processes and actors that are (1) too specific, (2) too broad, (3) arbitrary, or (4) that conflict with other rules it has set out to address other, related issues (possibly primarily non-economic). This possibly non-exhaustive list of government failures gives rise to different kinds of problems for the economy, which I will elaborate upon in the paper in the context of Intellectual Property Right (IPR) and Anti-trust laws in particular.

Rules in the Economy

By now the importance of rules to understand the economy and economic developments has become pretty clear to most economists. Even hard core neoclassical economists, who have a deep-seated antipathy against any role for government in the economy, acknowledge this. Some of these maintain that an orderly and thus rule-governed economy can do without rules issued and maintained by a government,[5] but most acknowledge that a government is necessary or even a prerequisite for most modern economic activities.[6] A role for the government is mostly acknowledged addressing issues related to property rights, including intellectual property rights, and also in relation to contract law. Even when a national government is absent or weak, players with authority and legitimacy underpinning a set of rules make economic development and prosperity more likely. Sometimes this has been an non-government authority such as the Catholic Church, especially during the Middle Ages.[7]

Even within an otherwise connected economic and legal sphere, such as the United States in the early decades of its existence, rules set out by a (local) government can profoundly affect the direction in which economic development is headed as well as overall levels of income or income distribution.[8] The basis for contract law in Massachusetts has been the will theory, whereas the basis in Virginia was the fairness doctrine from the common law tradition. While the latter allows a judge to annul a contract after it has been agreed upon by the parties, the former does not. Trade and investment are more likely to render benefits in the former.

4 I will use the terms laws, rules, and standards interchangeably and as an institutional economist discuss them as (formal) institutions (cf. Dolfsma 2004, 2009).
5 Ellickson 1991.
6 Glaeser & Shleifer 2002; Greif 2006.
7 Ekelund *et al*. 1996.
8 Kim 2009.

This strongly suggest that, for a number of possible reasons, the rules that a government sets out are less than fully plastic.[9] If at all economists in the neoclassical tradition acknowledge a role for government, the often implicit assumption is that the rules it sets and even the kind of government in existence are fully plastic such that optimal outcomes can always be attained by tweaking them.[10] Social and institutional economics are more likely to acknowledge the path dependence of (government) rules than many other lines of thought within economics,[11] being prone to the unavoidability of incomplete laws either as an unavoidable necessity but also as something purposefully sought.[12]

Government Failure

The proper role of the government is an issue of ideological discussion that goes to the heart of people's convictions of a politico-philosophical nature. At the extremes are the idea that government should be a night watch-state focusing on the issuing of a minimum of rules related to commerce and (national) safety, on the one hand, and the idea that the state should be concerned with the proper functioning of the economic system on the other hand. The extreme position among the latter is associated with communist ideas. In the current economic situation of economic crisis[13] far less far-reaching ideas most prominently advocated with John Maynard Keynes have gained quite a bit of currency once again. The proper functioning of the economy is then seen to relate to issues of addressing *systemic* risks to the economy that are to be expected when the banking system or the automobile industry fail as a whole.

Whatever one's views, scholars will recognize that government[14] must formulate rules for the functioning of society. In a Marshallian tradition, government failure is discussed in terms of the *effects* of any particular set of rules formulated by the government. When rules of a government lead to a concentration of (political) power in the hands of a few, when they lead to overly bureaucratic administration, or when they give rise to a government which is unaccountable, government may be said to have failed.

In my discussion here, I conceive of a government failure in four different ways, inspired by insights from the philosophy of law. I thus do not address the effects of government rule-setting activity, but I take a look at the

9 Acemoglu *et al*. 2001; Acemoglu et al 2005.
10 Cf. Niskanen 2003.
11 Wunder & Kemp 2008.
12 Fon & Parisi 2007.
13 Dolfsma & McCarthy 2009.
14 In this short paper I will discuss government as if it is a homogenous actor that is capable to formulate a well-functioning preference ordering and act upon it by formulating rules.

nature of the rules. Government failure then in no way is the inverse of market failure as discussed by economists. When discussing the possibilities and kinds of government failures, I will not assume a rules-free State of Nature or situation behind a Veil of Ignorance. I will rather discuss possible government failure in the face of any particular set of existing set of rules.[15] The failure will thus be in a context of a government changing, adding or taking away rules, which may turn out to cost some, or even all members of society and benefit others. In addition to the considerations of a consequentionalist kind about the greatest good for the greatest number, there there may be distributional issues that affect parties' deontological claims. Rather than merely addressing this from a consequentionalist perspective, as Fon and Parisi (2007) do, my approach is more of a deontological one.

The non-exhaustive list of four different ways in which government can fail will draw mostly on scholarly work in philosophy of law. When formulating rules, then, government can be (1) too specific, (2) too broad, (3) arbitrary, or (4) setting out rules that conflict other rules it has set out to address other, related (possibly primarily non-economic) issues.

Obviously these categories relate to Sullivan's (1992) distinction between rules and standards along a 'continuum of discretion'. Rules, as Sullivan refers to them, offer less discretion than do standards since they "bind the decision maker to respond in a determinate way to the presence of delimited triggering facts".[16] Standards suggest decision makers to refer back to background principles. The discussion of a government setting out more or less general rules seems to be alluding to what is known as a Roman law tradition, rather than a case law tradition. In Anglo-Saxon case law, jurisprudence proceeds as verdicts are expressed and explained in courts about particular cases with reference to cases that have been decided upon previously. In the Roman law tradition that prevails in other parts of the world, the legislative part of government sets out general rules that civilians follow. The executive part of government sees to it that the rules are followed, whereas the third part of the *trias politica* or separation of powers, the judiciary part may further elaborate on the rules set out.

Too specific rules

Ehrlich & Posner argue that "a perfectly detailed and comprehensive set of rules brings society nearer to its desired allocation of resources by discouraging socially undesirable activities and encouraging socially desirable ones."[17] In their view, rules cannot be too specific. Specific rules reduce uncertainty by making a ruling in a dispute more predictable as decision makers are led to act more consistently by being involved in a more transparent process. The cost of the legal process is also reduced as the speed with which a final

15 Cf. Hamilton 1932; Dolfsma 2009.
16 Sullivan 1992, p. 58; cf. Ehrlich & Posner 1974.
17 Ehrlich & Posner 1974, p. 262.

judicial resolution is reached. Yet, the many attempts at deregulation by a number of governments in recent years may be perceived as an attempt to reduce the specificity of rules and in doing so correct an undesirable situation. A rule being too specific is then seen as one kind of government failure.

Overly specific rules require that a government has to consider vast amounts of information of very diverse kinds. Rules formulated by the government that are very specific will soon become obsolete as circumstances change and need re-formulation.[18] Not only will this be costly in itself for the rule-maker, but uncertainty to society is increased. Overly specific rules, even when addressing a specific set of phenomena that is limited in number, will, however, relate necessarily and intimately with a other rules. Such interrelatedness will make changing a rule difficult and costly, even if no conflict between rules is involved. Changes to a rule may necessitate re-considering the other, related rules. Changing other rules too will hurt agents, who will need to be compensated if a government is not to become an unpredictable bully making arbitrary decisions. Such arbitrariness may affect the principle of equality before the law and the legal security that has been shown to foster commerce.[19] This applies perhaps in particular to rules related to property, bankruptcy, labour contracts, and enterprise.[20]

Too broad rules

A government (the legislative) that formulates rules in very broad terms, without giving guidance about their interpretation or without an authority that may provide such interpretation may be said to fail. In an attempt to have subjects behave in accordance to the spirit of the rules rather than consider anything that is not forbidden by specific rules fair game. (Specific) rules do produce rascals.[21] If rules are too broad, however, the 'rules' of the jungle apply. The weaker party – economic actors such as consumers, employees, and SMEs – may be hurt.

Broad rules may prevent over-inclusion or under-inclusion of situations in a category of events to which a rule applies as very specific rules may 'suppress relevant similarities and differences (Sullivan 1992, 66). Broad rules (or standards, such as 'reasonableness' or 'efficiency') are open-ended and allow for more discretion and flexibility but are possibly more costly to *apply* as a substantial amount of information needs to be gathered and processed for each case at hand. Specific rules, on the other hand, remove from consideration specific kinds of circumstances, thus allowing for (more) direct application. Yet, specific rules are costly to promulgate, as a government setting such a rule needs to consider *a priori* what kinds of circumstances are to be ignored

18 Ehrlich & Posner 1974.
19 Greif 2006.
20 Kim 2009.
21 Cf. LeGrand 2003.

and what the consequences of such ignorance will be for the decisions made, and allow for less flexibility. In particular when events to be regulated are rather heterogeneous or change rapidly, broader rules may be preferred. Decision makers will feel more compelled to explain their judicial decisions.

Arbitrary rules
A government that sets out rules for society and the economy of an arbitrary kind is what Margalit calls a government that rules an indecent society.[22] It is a society that humiliates its citizens (burghers) but that also stifles commerce, which is exactly what the Magna Carta of the year 1215 was to curb. Arbitrary rules increase uncertainty in the economic realm as well. The likelihood that returns on an investment can actually be enjoyed is reduced as rules set by government are more arbitrary. Investment levels will be lower.

Conflicting rules
Any practice[23] in society is likely to have multiple dimensions and may then be affected by rules set out by government promulgated to address specific issues relevant for parts or elements of that practice. What behaviour may be deemed desirable as stipulated by one set of rules may be behaviour that is undesirable from the perspective of another set of rules. If and when the behaviours in practice are inseparable, the actors involved in the practice may find themselves in a bind. Uncertainty is increased the sharper the conflict between rules.

The four ways in which governments may fail can, in actual fact, relate to each other, of course, and will come out best in analyzing a situation where two sets of rules conflict.

Policy: Innovation & Competition

The relation between innovation and competition is unclear empirically (see Table 1).[24] Government policy is involved in setting out rules that affect both these sides of the equation, however. Competition is stimulated most pertinently by anti-trust laws, while one pertinent set of rules meant to stimulate innovation is intellectual property rights (IPRs). Anti-trust laws seek to limit the extent to which a single firm may control a particular market and thus set monopoly prices, or at least prices substantially higher than what would otherwise be the case. IPRs give right holders the exclusive right to exploit commercially the material they can claim property rights over. While this may not in fact be a monopoly, it could give right holders the possibility to

22 Margalit 1996.
23 See Dolfsma 2009, chapter 4 for a discussion of the concept of practice.
24 Dolfsma & Van der Panne 2009.

charge higher prices and recoup investments in both R&D efforts and production capacity. The extent to which this is motive for having a system of IPRs actually makes sense empirically is disputed.[25] At the same time, of course, IPRs are to stimulate diffusion of newly developed knowledge by requiring publication of knowledge if it is to receive protection.

Table 1: Competition and Innovation Related – Findings from selected studies

Aghion & Howitt (1992)	Innovation intensity decreases as competition intensity rises
Aghion *et a*l. (2005)	Inverted-U
Blundell *et.al*. (1995)	Competition stimulates innovation
Boone (2000)	Increased competition will not lead to both product and process innovation
Caballero & Jaffe (1993)	Innovation intensity decreases as competition intensity rises
Cohen & Levin (1989)	Relation market structure & innovation fragile
Geroski (1990)	Monopoly market structure does not stimulate innovation
Kamien & Schwartz (1975)	Unclear relation between competition and innovation
Symeonidis (2001)	No evidence that price competition benefits innovation

Source: Dolfsma & Van der Panne (2009).

The extent to which these two sets of rules conflict has changed over time. In the past, anti-trust laws in Europe, for instance, have been promulgated with a view to protect incumbent firms rather than protect or even stimulate small firms and entrants into a sector.[26] IPR rules have also changed over time.[27] The general direction that these have moved into has produced a situation in which tensions between them have increased. The possibility of government failure then looms large.

There are, to wit, several ways in which (the potential for) anti-competitive behaviour can be detected. One is the *Small but Significant Non-transitory Increase in Price* (SNIPP) test, also called the *Hypothetical Monopolist Test*. Given a proper definition of the relevant market – no small feat – the effects of a hypothetical increase in the price of one good offered in a market by some 5 to 10 percent is determined. If a player can do so permanently without seeing its customers move to a competitor, that player is a monopolist or has such powers to a degree. At issue are what value price and cross-price elasticities exist for a good that one agent offers on the market. This test takes the demand side of a market into consideration, focusing only on price competition between relatively homogenous goods. An industry's history as a monopoly where higher than usual prices are charged already cannot be indicated with the SNIPP test: only (hypothetical) changes to the current sit-

25 See Dolfsma 2005, 2008 for a discussion.
26 Pace 2007.
27 Cf. Dolfsma 2005.

uation are considered. In addition, the industry may face *potential* entry and thus be contestable without being actually contested.[28] It is unclear if and how the contestability of a market will show in a SNIPP test.

Agents in an industry that behave in the way in which a monopolist with market power would may show other behaviours than the ones detected by the SNIPP test. Firms can, for instance, employ limit-pricing as a strategy to both keep prices higher than would be the case while at the same time stifling competition as the price set is lower than an entrant could possibly hope to charge given the lower economies of scale (and thus higher average costs per product) that an entrant can expect in the first phase after entry. Such behaviours can have real, negative effects on both consumers and (potential) competitors, and may thus be deemed undesirable. If rules in the domain of anti-trust law were to be too specific so as to only use the SNIPP test to detect anti-competitive behaviour, such behaviours would not be seen or found undesirable.

Being too strict in ruling out such behaviour by promulgating rules that specifically aim to prevent this may be an instance of government failure. Take the example of newspapers made available free of charge. The price they charge – €0 – may be deemed a limit price to deter entry. Doing so would, however, ignore the nature of this market as a two-sided market.[29] Firms in this industry offer goods on a market that actually cater to two markets at the same time. Readers are interested in them to consume both news and possibly product information advertised. Advertisers are interested in getting attention for their products. The lower the price charged by the producer of a newspaper, the larger the number of consumers will be and thus the audience for the advertisers. The income for the producers of free newspapers comes from one side of the market only. Conceiving of the €0 price as a limit price would in this case be unreasonable.

A broad measure of possible anti-competitive behaviour, such as the so-called Lerner index that simply tries to fathom directly the extent to which a firm in an industry is able to charge a price well in excess of marginal costs,[30] may be problematic too. Such a test would pinpoint as undesirable a kind of behaviour that might well be entirely fair, such as bundling or rebates.[31] A broad rule to detect anti-competitive behaviour such as one based on the Lerner index might in particular point to unbecoming behaviour that is allowed by IPR as a consequence of a firm's innovative efforts that have led to patentable knowledge. If and when such knowledge is used in producing goods and services for which there is a market, the price asked in that market might be substantially higher than marginal cost. Which set of rules is to apply? Will the application of any of the two not be arbitrary? Will players

28 Baumol 1982.
29 Dolfsma & Nahuis 2006; Rysman 2009.
30 Cf. Boone 2000.
31 See Anonymous 2009.

involved not be left in uncertainty? Is the correct conclusion to develop more concrete rules to address situations where rules conflict, and might these become overly specific? Or, rather, should broad rules apply that provide guidance but do not reduce uncertainty?

Conclusion

In this brief contribution to the *Liber Amicorum* for Aernout Schmidt, as he retires as professor of IT and Law from eLaw@Leiden, I have endeavored as an economist (and philosopher) to venture into the field of law. The field of law, for an economist, is fascinating as much as it is foreign. The logic applied and the material deemed relevant can be very different from that trained into as an economist. Nevertheless, or perhaps rather because of this, I have found discussing and working with Aernout very stimulating and a profound learning experience.

It is in grappling with the logic of legal scholars that I have come to look at the role of government as a rules-setting agent differently from how an (institutional) economist, however much one may be aware of the inescapable presence of rules in an economy, would be looking at it. This has led me to suggest that, in promulgating rules, there are four ways in which a government can fail. The rules a government imposes on society and the economy can be (1) too specific, (2) too broad, (3) arbitrary, or they can (4) conflict. When a government fails in such a way, the cost to economic actors is real as a discussion of the realms of anti-trust and intellectual property right laws may suggest.

References

Acemoglu, Johnson & Robinson 2001
D. Acemoglu, S. Johnson & J.A. Robinson (2001) "The Colonial Origins of Comparative Development: An Empirical Investigation." *American Economic Review 91*(5): 1369–1401.

Acemoglu 2005
D. Acemoglu (2005), 'Institutions as the Fundamental Cause of Long-Run Growth', in: Ph. Aghion & S. Durlauf (eds.) *Handbook of Economic Growth*. Elsevier, North Holland, p. 385-472.

Anonymous 2009
Anonymous (2009), 'The Unkindest Cuts', in: *The Economist*, August 20, p. 62.

Baumol 1982
W.J. Baumol (1982), 'Contestable Markets: An Uprising in the Theory of Industry Structure', in: *American Economic Review* 72(1), p. 1-15.

Boone 2000
J. Boone (2000), 'Competitive Pressure: The Effects on Investments in Product and Process Innovation', *RAND Journal of Economics* 31(3), p. 549-569.

Dolfsma 2004
W. Dolfsma (2004), *Institutional Economics and the Formation of Preferences*, Cheltenham: Edward Elgar.

Dolfsma 2005
W. Dolfsma (2005), 'Towards a Dynamic (Schumpeterian) Welfare Economics', *Research Policy* 34(1), p. 69-82.

Dolfsma 2008
W. Dolfsma (2008), *Knowledge Economies*, London & New York: Routledge.

Dolfsma 2009
W. Dolfsma (2009), *Institutions, Communication and Values*, Houndsmills: Palgrave Macmillan.

Dolfsma & Van der Panne 2009
W. Dolfsma and G. van der Panne (2009), *Innovation, Industry Structure and Industry Dynamics*, Mimeo.

Dolfsma & Nahuis 2006
W. Dolfsma and R. Nahuis (2006) 'Media & Economics: Uneasy Bedfellows?' *The Economist* 154(1), p. 107-124.

Dolfsma & McCarthy 2009
W. Dolfsma and K.J. McCarthy (2009) 'What's in a name? Understanding the language of the credit crunch', in: *Journal of Economic Issues* 38(2).

Ehrlich & Posner 1974
I. Ehrlich and R.A. Posner (1974), 'An Economic Analysis of Legal Rulemaking: An Economic Analysis of Legal Rulemaking', in: *Journal of Legal Studies* 3(1), p. 257-286.

Ekelund et al. 1996
R.B. Ekelund Jr, R.F. Hébert, R.D. Tollison, G.M. Anderson and A.B. Davidson (1996), *Sacred Trust: The Medieval Church as an Economic Actor*, New York: Oxford UP.

Ellickson 1991
Ellickson, R. (1991), *Order without Law: How neighbors settle disputes*, Cambridge, MA: Harvard UP.

Fon & Parisi 2007
V. Fon and F. Parisi (2007), 'On the optimal specificity of legal rules', in: *Journal of Institutional Economics* 3(2), p. 147-164.

Glaeser & Shleifer 2002
E. Glaeser and A. Shleifer (2002), 'Legal Origins', in: *Quarterly Journal of Economics* 117, p. 1193-1230.

Greif 2006
A. Greif (2006), *Institutions and the Path to the Modern Economy*, Cambridge UP.

Hamilton 1932
W. Hamilton (1932), 'Institutions', in: *Encyclopedia of the Social Sciences*, eds. E.R.A. Seligman & A. Johnson, vol. 8, New York: MacMillan, p. 84-89.

Kim 2009
S. Kim (2009), 'Institutions and US regional development: a study of Massachussets and Virginia', in: *Journal of Institutional Economics* 5(2), p. 181-205.

Le Grand 2003
J. Le Grand (2003), *Motivation, Agency and Public Policy: Of Knights and Knaves, Pawns and Queens*, New York: Oxford UP.

Margalit 1996
A. Margalit (1996), *The Decent Society*, Cambridge, MA: Harvard University Press.

Medema 2003
S.G. Medema (2003), 'The Economic Role of Government in the History of Economic Thought', in: J. Biddle, W. Samuels and J.B. Davis (eds.), *A Companion to the History of Economic Thought*, Blackwell, p. 428-444.

Niskanen 2003
W.A. Niskanen (2003), *Autocratic, Democratic and Optimal Government. Fiscal Choices and Economic Outcomes*, Cheltenham: Edward Elgar.

Pace 2007
L.P. Pace (2007), *European Antitrust Law Prohibitions, Merger Control and Procedures*, Cheltenham: Edward Elgar.

Rysman 2009
M. Rysman (2009), 'The Economics of Two-Sided Markets', in: *Journal of Economic Perspectives* 23(3), p. 125-143.

Schmidt, Dolfsma & Keuvelaar 2007
A.H.J. Schmidt, W. Dolfsma and W. Keuvelaar (eds., 2007), *Fighting the War on File Sharing*, Cambridge/The Hague: Cambridge UP / TMC Asser Press.

Sullivan 1992
K.M. Sullivan (1992), 'The Justices of Rules and Standards', in: *Harvard Law Review* 106, p. 22-123.

Wolf 1997
Ch. Wolf Jr. (1997 [1988]), *Markets or Governments – Choosing between imperfect alternatives*, Cambridge, MA: MIT Press.

Wunder & Kemp 2008
T.A. Wunder and T. Kemp (2008), 'Institutionalism and the State: Founding Views Reexamined', in: *Forum for Social Economics* 37, p. 27-42.

Lies, damned lies, and legal truths

Richard Gill[■]

Introduction

My acquaintance with Aernout Schmidt began when we were asked to be one another's opponent in a Leiden science-café debate on the celebrated case of the Dutch nurse Lucia de Berk, who at the time was serving a life sentence for seven murders and three attempted murders of her patients: children at a special children's hospital, and terminally ill old people in an ordinary hospital ward where she had earlier worked. The case was sparked when, on the early hours of 4 September 2001, for the so-many'th time (as it appeared) a young child died during one of her shifts. The statistical question of whether Lucia's repeated presence at a series of deaths and near-deaths could merely have been a coincidence was answered first for hospital authorities, then for police investigators, and finally in court (in 2003; answer: no, it could not have been chance).

Aernout is a specialist on law and information technology, and in this capacity he has even taught statistics to lawyers. I am a statistician, but infamous in some Dutch legal circles for my part in inciting some kind of mass movement to get Lucia a re-trial, even though the verdict had been confirmed first on appeal (2004) and finally on "cassation" at the Supreme Court (2006). For instance, G. van Manen, and later P. J. van Koppen (the latter a law-psychologist and eloquent criticaster of our judicial system), accused me in Nederlandse Juristenblad, The Journal of Dutch Lawyers, 2008, of deliberately playing to the gut-feelings of an international scientific rabble by feeding them with misinformation and lies (shades of the lynching of the brothers de Witt).

A retrial is presently (2009) underway following identification of new facts in a medical investigation commissioned by the Procurator-General to the Supreme Court (2008).

Unfortunately for the heat of the science-café debate, it turned out that Aernout and I got on very well together, and in particular tended to agree on almost everything. Still it was a lively and exciting evening and promised well for future collaboration. We quickly converted our debate into a short paper in the new Dutch journal "Expertise and Law" (2008) and I was hoping for more collaboration in the future, only to be shocked by the inform

---

■ Richard Gill is full professor at the Mathematical Institute, Leiden University; cf. http://www.math.leidenuniv.nl/~gill. He specializes in mathematical statistics.

tion that Aernout was so much older than he seems that his friends were writing him a Liber Amicorum on the occasion of his retirement. Being asked to contribute I eagerly sieze the opportunity to settle one niggling difference with Aernout, and to fulfil one wish of the editors of "Expertise and Law", which we did not do in the paper.

This paper will discuss in essay form (more precisely, a Joycean stream of consciousness) my difference with Aernout, and intertwined with that, supply the "missing" passages of our paper. The two topics are indeed in my opinion strongly linked.

Our difference of opinion concerned the question of whether statistics still plays any role in the Lucia case after the 2004 appeal, at the conclusion of which the judges explicitly wrote that their verdict (Lucia is guilty of seven murders and three attempted murders) is reached without any use of statistics.

The (deliberately) missing passages of our paper concerns the question what kind of statistics, if any, ought to be used in criminal court procedings: Classical/Frequentistic; Full Bayesian; or according to the latest fashion: the Likelihood Ratio. We only briefly mentioned the first two statistical flavours, and totally ignored the new *flavour of the month*.

Was Lucia convicted by statistics?

So, is statistics still present and still important in Lucia's case, after the appeal? My opinion is that despite the judges' words (well – that depends on how one reads them), the written argument for their verdict is statistical through and through: however, unfortunately, based on *wrong* statistics, *wrongly* analysed, and *wrongly* interpreted. You may not agree with me, as Aernout also did not agree (though he agreed he should study the verdict first in detail); but it also became clear that he does not understand the word statistics as I do.

I have to admit that my claim also depends on information in the dossier but not in the written verdict. If you wish to check my claims you will be forced to trust the information about it which can be found in Ton Derksen's splendid (2006) book: *Lucia de B: Reconstruction of a Miscarriage of Justice* (unfortunately still not translated in its entirety into English, though some sections and summaries have appeared as separate papers).

The important point I want to make is that there is *no* clear boundary-line between statistics as an advanced and complex science, and common sense interpretation of "statistical data". More subtly, when does the interpretation of statistical data concerning medical events belong to statistics, and when does it belong to medicine? This leads to dangerous situations from the point of view of *determining the true facts of the matter*, which is the task of the judges in Dutch criminal proceedings. Of course, judges often take recourse to the interpretation by experts of "hard facts", when the implications of those hard facts are difficult or impossible for a layperson to see.

But what if the court is not aware that certain hard facts do need expert interpretation, because a lay person's interpretation can be easily wrong, though at face value it might seem convincing?

I am not going to propose a solution to this problem, and probably from a legal point of view it does not exist. The law is the law, judges act on it. However if the problem is associated with recurring miscarriages of justice, then there is a long term problem for justice and for society, as well as the damage done in the short term to people's lives.

The close to 100 page verdict after the appeal proceedings (I suppose the longest in Dutch criminal law history) starts in its preamble with the statement that "a statistical probability calculation plays no role at all in our deliberations". Moreover, "every single one of the deaths (and other incidents) has been indisputibly proven by medical-scientific evidence to be unnatural". These are powerful claims and from their prominent position in the preamble to the "arrest" they seem to be aimed at the world at large, in particular at the media and at the scientific community, in which a great debate had raged over the question of whether or not statistics could be used to prove that someone is a murderer; the debate further muddied by strident fundamentalists shouting which kind of statistics should be used (frequentist or Bayesian). From that verdict onwards, whenever a statistician like myself said something in public about the case, the retort was "but statistics no longer plays any role in the case, so you should keep your mouth shut".

My claim is that statistics was almost the only evidence against Lucia. By the device of converting statistical arguments either into common sense arguments of lawyers, or into medical arguments of medical doctors, the statistics of a coincidence was/were disguised as indisputible medical-scientific facts of unnatural deaths.

Naturally there is a grey area where one person's scientific expertise becomes another person's common sense. This is partly a question of demarkation and ownership of concepts and knowledge. From a scientific point of view, demarkation is merely a matter of convenience and culture; ownership does not exist. For many lawyers however, for whom (to people like me) form often appears to take priority over content, demarcation and ownership are crucial. Obviously, only a statistician is qualified to make statistical probability calculations concerning exactly how unlikely it is that one particular nurse is present at each and every one of the only 9 deaths and reanimations on her ward in a particular year; but a coincidence like this remains (appearing to be) an extraordinary coincidence, and it remains shouting to be given an explanation. When a medical doctor tells you that these events took place on a ward where normally there were no deaths at all (and supports this by showing the numbers of zero deaths in each of the two preceding years), and reminds you that this was a medium-care ward where all the patients were all expected to shortly go back home! – well, who needs a statistician?

Especially, who needs a statistician, when statisticians clearly disagree on what the probability is, because of incomprehensible disagreements con-

cerning the right "model" and the right "paradigma" (these are different issues; the latter refers to the frequentist/Bayesian debate). Indeed, the defence introduced a probabilist with a philosophical bent, and an expert on artificial intelligence and logic, to argue that were many different probabilities depending on your model, so that the question asked by the court "how likely is it that the coincidence is just due to chance" *could not be answered*. The defence got its way. In its verdict, the court scrupulously avoiding any probability calculations, and even any use of words like statistics.

I will briefly expose and analyse the hidden statistical arguments of the court, and (briefly) contrast them with what I believe are sound statistical arguments. Common sense is not always right in matters of probability and statistics; medical arguments about statistics are very often flawed; and as for legal arguments about statistics ... it is not for nothing that the two most famous misinterpretations of conditional probabilities are called the *prosecutor's fallacy* and the *defence attorney's fallacy* respectively. Please note: I do not want to argue that Lucia was unjustly convicted. The judges were totally convinced of her guilt, and whether or not their written legal argument holds scientific water might be a subsidiary issue for some; especially now that new facts (seem to) have made it redundant. No: the point is that there will be a problem in legal proceedings when common sense and scientific expertise have a large overlap; an even greater problem when several expertises overlap with one another and with common sense. In the Lucia case I certainly believe that "law" abused "statistics" in an appalling way. But the blame can be placed just as firmly on the statistical community for being such a shadowy presence in modern Dutch society that the legal community hardly knows that "we" exist, and certainly only has the vaguest idea of what we are about. The incompatibility between the statistical mind and the medical mind is well known to all who work in the arena where those disciplines overlap. Probably the incompatibility between legal and statistical minds is even greater.

I think that the Lucia case has stirred scientific opinion in the Netherlands so strongly, that for some time to come, scientists will be taking more interest in law. This cannot but serve both justice (in its human or social sense) and the legal system. It's an ill wind which blows no-one any good.

Statistical evidence

Statistical evidence is not in principle different from any other kind of technical or forensic or scientific evidence. By definition, scientific evidence in the legal setting is evidence which an average person or an average lawyer cannot safely interpret on their own, but for which they have to rely on the expertise of a specialist. Statistical evidence *is* scientific evidence. However, whereas the average lawyer probably realises that she is no expert on ballistics, or accountancy, or toxicology, and will readily acknowledge that there do exist reliable and highly-trained persons who can help them out in these fields, the

average lawyer, just like the average human being, is a biological machine whose survival and evolution revolves around recognising and interpreting coincidences (what else is statistics?) and, incidentally, around recognising and interpreting motives and personalities (what else is psychology?). Thus a huge part of the evidence evaluated and sifted by police investigators, lawyers, and judges, is in a very strong sense statistical evidence and/or psychological evidence. In many situations, one can make do with the statistics and psychology "of the man in the street". A verdict of a criminal court ought to convince any reasonably intelligent and well-thinking person. How to trust statistical conclusions which only a statistician can obtain?

The statistics of the Lucia case are complicated and subtle and still not understood; in fact, largely because of the refusal of the hospital authorities to let any outsider get any look at all at original data. To this day, not a single professional statistician has ever been officially involved in any of the trials and retrials. (If you are familiar with this case, and you are a Dutch lawyer, this statement is meant to tell you that my definition of "statistician" is different from yours). By the way, similarly, to this day, no-one with a broad generalistic medical knowledge has looked at the medical aspects of the whole case in depth, except for the chief paediatrician (or chef de clinique) of the Juliana Kinderziekenhuis, who was a key player in the initial chain of events triggering the police investigation, and her sister-in-law medical doctor Metta de Noo-Derksen (specialist in gerontology and nursing), a key player in the extra-legal investigations which finally led to Ton Derksen's book, and from there by further steps presently irrelevent to my story, to a re-trial.

In my opinion, statistics (and psychology) drove the case, from start to end: Lucia's conviction for serial murder, and even the "the proof" that there were any murders at all – let alone by whom – were almost entirely based on wrong statistical data, wrongly analysed, and wrongly interpreted; by amateurs.

I summarize my "hard evidence" for this at the end of the paper.

Which statistical paradigma?

The second issue discussed in this paper is the sticky question of which statistical paradigma might be appropriate to the Lucia case in particular, and to legal proceedings in general. Aernout and I briefly discussed the opposition between classical frequentist statistics (p-values, hypotheses tests, significance and power…) and those magically appealing Bayesian statistics (so simple: posterior odds equals prior odds times likelihood ratio). The reviewers of our paper were highly disappointed that we did not pay any attention to a very modern alternative; I think they were referring to the new dogma that all a statistician must do is compute the likelihood ratio. I deliberately did not want to discuss competing schools of statistics in the context of our debate, nor of our paper, for the following reason: in my opinion, it was totally irrelevant.

It should not be a surprise that there are different ways to formally model the processes of learning from uncertain data, decision making in the face of uncertainty, statistical inference, and so on. There are so many different kinds of ways in which we need to draw conclusions from "statistical data", in the sense of data which has been produced by some random mechanism (I mean, the output of the mechanism is random), and could easily have been different (our task being to draw conclusions about the nature of the mechanism). For instance, when one spins (rather than tosses) a coin, it turns out that coins have a preference to fall on one particular side. This is because coins are struck from a flat sheet of metal, with, say, heads on top, tails below; this procedure makes coins in the shape of a thin slice from of a very long tapering cone. Küchenhoff (2008) reports 501 tails in 800 spins of recent German 2 Euro coins (16 students each spinning a coin 50 times). He noted that there is a significant difference between the students (or their coins, or the tables on which the coins spun, or whatever...).

Is the aim merely to report some kind of fair summary of the data which anyone could use for their own ends? Or should one take account of the use which the consumer is going to make of your statistics? For instance, send someone to jail for counterfeiting coins of the Euro-realm? Should we make use of other information and if so, what and how? Results of spinning 1 Euro coins? Or of Dutch 2 Euro coins? Complex phenomena need to be simplified before they are amenable to mathematical analysis. The different schools of statistical inference correspond to different idealisations; different simplifications. Each one can be extremely appropriate or can be extremely *inappropriate* in any particular situation – it depends on whether one has focussed on essential or on peripheral issues; whether one has neglected essential aspects of the problem and concentrated on peripheral. It depends on how seriously one should take the various kinds of information which are available. And of course, if we are talking about chances, it depends on which chance you are talking about. A chance of 1 in a 100 means 1 in a hundred somethings, and those somethings need to be extremely carefully specified. The same event has any probability between 0% and 100% you like, as one considers it relative to different "classes of hypothetical repetitions".

The debate which raged between Bayesians and frequentists concerning the Lucia case, and which probably put the court off making any serious use of statistics, was largely irrelevant since the crucial thing was not the 1) style of inference, but 2) the model assumptions and 3) the data. Point 2) concerns the question *what are the conceptual repetitions*? What structure can be assumed about those repetitions? This is a very difficult task: we are talking about a conceptual or counter-factual situation in which we rerun a year in the life of a hospital ward again and again, with some things kept the same, other things allowed to vary naturally. Which should be thought to be kept fixed, which are allowed to vary? How will they vary, then? What is *natural variation* in a year in the life of a hospital ward?

What statistical model?

If we want to know if Lucia's presence at so many incidents was due to chance, we need to understand how shifts of nurses, and incidents in the medical care of patients, get fixed in time, in the *natural situation* that no killer is at work; it is just business as usual. The statistician whose advice to the court made a great deal of impact in the original trial thought of the normal situation as being as follows: first of all, we fix the shifts of all the nurses. Think of a duty-roster being drawn up on the 1st of January, and then being followed scrupulously throughout the year. Three shifts a day, the year round, 365 days; somewhat more than 1000 shifts altogether. During the year patients are admitted to the ward and discharged from the ward. Occasionally there is an *incident* – a life-threatening, and sometimes life-terminating, medical emergency. These incidents were supposed to occur *completely (or uniformly) at random*, in the very strong sense that each and every one of those 1000+ shifts has the *same* chance to have an incident occur in it; and the occurrence or non-occurrence of incidents in any particular set of shifts, has no effect whatever on the chances of incidents in the other shifts.

I think it should surprise no-one that this model turned out to be obviously false. To begin with, the statistics were only being done because a nurse had already noticed that Lucia had been often present at incidents.

What statistical data?

I will come back to the model later, and say a little more about the data now. An extraordinary fact is that no "statistician" officially involved in the case so far went back to the sources (ward log books, personnel records, patients medical records, and the memory of nurses and doctors) but all assumed that it was valid. I have consulted with statisticians with large experience of similar cases in the UK and in the USA and in Norway. The first thing you do is ask for the formal definition of "incident" and the formal definition of "the shift in which the incident occurred". You check that the criteria can be verified, for every shift, without having to know which nurses were on duty when. Similarly you ask for the formal definition of "who's on a shift" and you check that the criteria can be verified without knowing what happened during the shift, for every shift.

Another fact is that the tabulation of this data was done largely by an internal team of medical personnel at the hospital where the events took place. I have consulted with senior nursing experts in Canada, the US, and the UK, and the first thing that happens when suspicion is raised in this kind of case is that an outside team of medical investigators is called in, and a careful and independent investigation is made. This happens *before* the police is called in, and certainly *before* press releases are put out, alluding to activities of a serial killer.

We now know for sure that the coincidence was not due to chance because incidents were to an important extent *made to happen* during Lucia's shifts, by definition. Whether or not an event was an unexplained serious medical incident depended on whether or not Lucia was (thought to be) present. More subtly, when an incident was supposed to occur, depended on when Lucia was on duty. A full-time nurse has one of the three shifts of the day, for a number of days in a row; every incident on those days is either in or next to one of her shifts. This gives a lot of latitude for fudging the data; latitude which certainly was taken advantage of, though probably subconsciously. The investigators never specified an objective, or at least inter-subjective definition of what is an incident, nor when it is thought to occur. The court statisticians never asked to see the protocol.

An attempt to locate known incidents in shifts in a self-consistent way, without reference to who is on duty, results in several less coincidences. The original 9 incidents in a year, all in Lucia's shifts, changes on the basis of a careful investigation to 7 incidents in her shifts, 4 out of them. Since she has about one sixth of all the shifts, one would rather expect something like 1 or 2 or 3 in her shifts, 10 or 9 or 8 out... But this is no longer that stunning "nine out of nine".

Back to paradigmas

Even if we accept the data, I will not say that a frequentist analysis is correct and a Bayesian wrong, or vice-versa. They are different, and indeed, a huge difference in numerical results, is very, very informative. Garbage in, garbage out… in this case, what you get out depends in an extraordinarily sensitive way on what you put in; it becomes clear by comparing different models and different paradigmas that the data does not tell us a very great deal at all.

Enough has been written elsewhere about *classical frequentist* versus *Bayesian* statistical inference (sometimes characterized as *objective* versus *subjective*). In my opinion neither of these paradigmas is really suitable for use "in court". I fear that neither judges nor juries are ever going to understand what is a significance level and what is a p-value (that disposes of classical statistics). I have sympathy for a so-called *empirical Bayesian analysis* but great distrust of the "true" or "fundamentalist" Bayesian use of purely subjective probabilities; especially of prior, subjective probabilities of innocence and guilt. Whose subjective probabilities? I hope that the defence will object, and their objection will be carried.

The modern alternative is the Likelihood Ratio. Actually it is an ingredient in either traditional schools' calculations; the novelty of the likelihood ratio approach is that we do not commit ourselves to what is to be done with the Likelihood Ratio. We just inform the court what it is, possibly converting numerical values (e.g., a likelihood ratio of larger than a million), into a verbal description (e.g., the data overwhelmingly supports the one hypothesis over the other).

The likelihood ratio is simply the ratio of the probability of the observed data (the evidence), under the scenario or model adhered to by the prosecution, to the probability of the same, observed data (evidence), under the scenario adhered to by the defence. However, this is easier said than done. No-one has yet done a decent "likelihood ratio" analysis of the Lucia data, for a very good reason: no-one has any idea of what a good probabilistic description is of events on a hospital award in a natural situation, with no killer at work, let alone in the situation supposed by the prosecution to be the case, that a certain person was trying to kill some of the patients. As I remarked above, so far everyone who has discussed the statistics of the Lucia case has taken the model of independent, uniformly random events for granted as a starting point. However, we know that 7 (=2+2+3) of the incidents concerned only 3 babies, in other words, we have sub-sequences of very similar medical emergencies occuring for the same child. We also know now that there are large fluctuations in the numbers of incidents per year over longer periods of time (a year or two before the time Lucia worked at JKZ, and again, a few years after she was removed from the scene, there were similar large numbers of incidents, to that one year whose apotheosis was a criminal investigation).

The basic empirical research into the existence and meaning of this kind of fluctuations has simply never been done, neither at those hospitals in the Hague where Lucia worked, nor in general. What we do know is that variation in the rates of events, and dependence between events, coupled with a non-uniform allocation of personnel to shifts, automatically inflates the variability in the numbers of events experienced by different nurses. Hidden confounders leads to over-dispersion. Some nurses experience what seems like much too many, some experience what seems like much too few.

It seems that the likelihood ratio approach cannot even leave the ground. If we could get over the first difficulties, new difficulties come up; this paper is too short (and the new difficulties require more technical statistical knowledge), so I will leave it at that.

Hidden statistics

I now return to my other main theme, the persistence of statistics in the verdict of the appeal court. Here I will just summarize a number of observations made by Ton Derksen in his book and in his submission to the judicial review committee CEAS.

The court finds it significant that "all the incidents took place in a short time period and during the shifts of Lucia", when "normally there were no incidents on that ward". I think that the court here is drawing statistical conclusions (there are too many incidents, and Lucia is involved with them) from statistical data; though I have argued above that a) the data is wrong and b) the inference is incorrect, since the normal situation is one of clusters of events which then tend to "hit" one or two nurses. Of course, these obser-

vations were made by medical personel; does this make that evidence *medical*, rather than *statistical*? Actually, I don't care what we *call* it (think of Romeo's rose Juliet); the fact is that a professional statistician (I repeat: the court's experts were not professional statisticians, nor were the experts put forward by the defence) could well have persuasively argued that the cluster of events doesn't have to mean anything, nor does Lucia's presence at so many mean very much on its own, especially after we have taken care to remove *selection bias* and also taken account of the *post hoc* problem, which essentially forces us to an *empirical Bayes approach*. However, as I said before, the necessary basic *empirical* research has still never been done!

Somewhat more pernicious is the following. The court learnt from their "statisticians" that a statistical correlation does not imply causation. It learnt that the coincidence was not due to chance and that Lucia had to explain why she was repeatedly present at those incidents. The statisticians did offer a number (to be precise: four) alternative explanations of the coincidence, *by way of example.* Amazingly, deep in the "arrest" we find the judge asking Lucia, example by example, whether any of these explanations (and only these explanations) were applicable. "Mrs de B., were you a bad nurse?" "No your honour, my colleagues and superiors always had high regard for my work" [since a bad nurse would experience more incidents because the quality of her care is low, this doesn't make her a murderer], "Mrs de B., did you have to care for more difficult cases/get more difficult shifts than your colleagues?" "No your, honour, we shared the work fairly...".

My statistical colleagues and I are deeply shocked by this. The court has adopted statistical reasoning, though applying it incorrectly, and applying it to bad data; the numbers and calculations are gone, but the verbal argument of their own statistical advisors remains standing. Aernout objected.

Finally, very pernicious (in my statistician's opinion), but depending on knowledge of the underlying dossiers, is the following. For each of the deaths and critical situations considered by the court, a large number of medical experts was consulted. In every single case a majority of experts thought that the event was not unnatural, but always some experts could be found who could say that they thought that the event had some rather strange, inexplicable features. In two cases, in which Lucia was indeed convicted for murder or attempted murder, only one expert considered the event in question inexplicable (a different expert each time). One might hope that those medical experts had strong medical arguments why these events were medically inexplicable. However, the experts said "this event appears natural, but because Lucia was present, as she was at so many other events, I believe it was an unnatural event".

This incontrovertible scientific-medical proof of inexplicable deaths or incidents is actually medical doctors' amateur statistical reasoning, based on data which we now know to be highly unreliable.

Conclusions

The fuzzy border between statistical expertise and medical or legal common sense can be used, whether accidentally or deliberately, to hide bad statistical data and bad statistical inferences away from the eyes of the world. On the other hand, the fact that in the Lucia case neither the court nor the defence worked with professional statistical experts says something negative about the visibility of the statistical profession in the Netherlands. Apparently, society at large (in this country) has little idea what statistics is about, little idea what statisticians do.

The technical problems of modelling the kind of data collected in the Lucia case are illustrative of the enormous challenges facing forensic statistics at the moment. *More research needs to be done*. I am convinced that advanced modern statistics can play an increasingly important role in criminal investigation and prosecution, and that the legal context requires the development of new paradigma's and new methodologies. We statisticians are really only just starting to tackle this job.

As criminal investigation uses more and more advanced science and technology, the legal profession is finding itself more and more challenged. This is a world-wide phenomenon. One may look for remedies in the training of lawyers, or in court procedures. More and more, forensic research is going to be multidisciplinary; more and more, scientists are going to disagree about the conclusions, and not because one is better than the other, but largely because they have different information, or are making different assumptions, or talking different languages. In science we search for differences and resolve them in open dialogue; sometimes we discover that *right now we don't know, more research needs to be done*. In the Dutch criminal court, the judges decide what information to give to one expert, ask some questions, get some answers, then repeat this procedure with another expert. From the scientific point of view, it is as if the judge is the leader of a multidisciplinary scientific investigation, where the members of his team are not allowed to communicate with one another, and one person only is responsible for the decisions concerning flow of information, and translation of information between disciplines.

I understand very well the good reasons for the existing *procedures*. However, I fear that the judge is taking over the job of a police investigation team; perhaps only attempting this because the case put by the prosecution is too weak! If the situation is such that the procedure is not likely to succeed, there is no point in going through the motions. The results are arbitrary.

References

Derksen 2006
A.A. Derksen (2006), *Lucia de B.: Reconstructie van een Gerechtelijke Dwaling*, Veen Magazines, Diemen.

Küchendoff 2008
H. Küchenhoff (2008), 'Coin Tossing and Spinning – Useful Classroom Experiments for Teaching Statistics', pp. 417-426 in: *Recent Advances in Linear Models and Related Areas*. Essays in Honour of Helge Toutenburg. S. and C. Heumann (eds), Physica-Verlag HD.

Quem ad Finem: To the Limits of Modernity

Radim Polčák■

No place like Vienna

Throughout 19th century, the Austrian Empire was truly an exceptional European power. Compared to other similarly powerful contemporary European states, Austria covered a much broader scope of nations and cultures. The coexistence of various, often substantially different, national entities, was, of course, not idyllic at all. Most nationalities, probably except the dominant Austrians and Hungarians, suffered from inequalities, suppression or bureaucracy. However, the fact that all nationalities of the Austrian empire (in total more than 10 dominant nationalities and dozens of minor ones) coexisted within one state, i.e. they could or even had to interact with each other, brought remarkable artistic, cultural and scientific achievements.[1]

All these political, social, cultural and scientific developments had a common geographical centre: Vienna. Accumulated wealth, the glamour and the attention of imperial family attracted literally the best personal substrate of all kinds, from craftsmen to philosophers. Moreover, this came at the right time – great scientific achievements made people able to understand and use physical forces as well as to get closer to understanding the nature of life. At the same time, new means of transport enabled people to freely travel across the world[2] so it became possible for various intellectual giants not just to exchange letters, but to meet in person and discuss matters in the legendary cafés of Vienna.[3]

It is not a wonder that taking the best of dozens of cultures and melting it with technological progress and the omnipresent spirit of modernity accidentally created an environment incomparable to anything before and very likely also to anything after. The typical life of a *fin de siècle* European intel-

---

■ Radim Polčák is head of the Workgroup of Law and ICT, Faculty of Law, Masaryk University.

1 Comprehensive and picturesque view on contemporary Vienna can be found for example in Schorske 1981.

2 However, travelling was not comfortable enough, preventing people from travelling constantly (as we do now). We might then think that objective possibility of travelling together with its contemporary constraints made people on one hand to travel but on the other hand to stay longer.

3 Cafés were not only places of refreshment, rest or entertainment. They also acted as main meeting points of various formal or informal societies. They were also offering readings, mostly newspapers and later also magazines, that were normally available only to the upper class (subscriptions were in those days extremely expensive).

lectual started somewhere in the Austrian countryside (in Moravia, Slovenia, Romania or so), continued in some of the local centers that prepared him or her (mostly him) for the lights of the Big City and then reached its peak at Café Bräunerhof, Kaffee Alt Wien or simply somewhere around there.

As mentioned above, all intellectual life of the second half of the nineteenth and the beginning of the twentieth century was dominated by the spirit of modernity. Universal belief in the power of the reason had put aside metaphysics and brought forward analytical disciplines and methods which finally led to the development of forms of positivism.

If we were to choose an icon of Viennese positivism, it would probably be Ludwig Wittgenstein. His life is not entirely matching the typical life story of then-contemporary Viennese intellectuals as mentioned above, as he was in fact born in Vienna and his intellectual career reached its peak partly on the battlegrounds of the Great War and in Cambridge. In any case, his thoughts have shaped a multitude of contemporary Viennese intellectual societies. In the only monograph that was issued during his life, the Logisch-Philosophische Abhandlung (later renamed as Tractatus Logico-Philosophicus), he puts forward with striking shortness some of very basic ideas of positivism starting with the facts:[4]

> "1.1 The world is the totality of facts, not of things.
> 1.11 The world is determined by the facts and by their being all the facts.
> 1.12 For the totality of the facts determines what is the case, and also whatever is not the case.
> 1.13 The facts in the logical space are the world."

The last point shows Wittgenstein's unshakable belief in abilities of reason on the one hand and his refusal of metaphysics on the other.[5] In his view, our inability of reasonable understanding of facts cannot be caused by natural limits of the reason, but either by individual limitations or by methodological insufficiencies.

That belief in the power of the reason is, of course, not a product of the end of nineteenth century. It reportedly originates in ancient philosophy and reappears in different shapes and intensity periodically since then. Wittgenstein and his teachers, namely Russell and Frege, did not return primarily to the works of ancient philosophers, but to the roots of modernist rationalism at the end of the seventeenth century. Most of all, they considered themselves as successors of Gottfried Wilhelm Freiherr von Leibniz.

Although it might seem that Viennese positivism was a coherent movement, there were strong tensions between two of its main streams; empiricism and intuitive positivism. The original (empirical) positivism was not

4 See Wittgenstein 2004, p. 62.

5 The refusal of metaphysics and inclination to pure reason is to be seen as a general tendency of late modernity. It is comprehensively mapped for example in Sullivan 1933, p. 238.

just based on the assumption that human reason is able to comprehend the world, but also on the call for empirical proofs of rational theses. Empirical positivists, such as Ernst Mach,[6] required not just rational investigations and logical explanations of facts, but also proofs by empirical means. They believed, being inspired mainly by Newton,[7] that empirical experience is the only source of knowledge.

The most well-known Viennese intellectual center that was originally based on machism[8] was the Vienna Circle (der Wiener Kreis). It was a highly respected and honourable scientific society that gathered around German philosopher Moritz Schlick. Although the circle was originally grounded on the thoughts of Ernst Mach, there can be seen a shift from empirical to logical positivism. Schlick and other members of the Circle believed, similarly to Mach, that logic was just another name of rationality. However, they were not that rigorous in asking for empirical proofs.

In any case, Schlick and the rest of Vienna Circle (except Gödel – see below) followed Mach by strictly denying the role of the intuition. In his response to contemporary attempts of including the intuition among relevant scientific methods,[9] Schlick wrote:[10]

> "Intuition, as we continue to find, is the very opposite of knowledge. In pure intuition, raw contemplation, everything is utterly individual, for itself, compared with nothing. (-) If again, there is so large a crop nowadays of gifted and ardent spirits who oppose the philosophic to the scientific method, who find no satisfaction in a science which is for every merely ordering, elaborating, establishing relations, which makes no effort to create anything new, but actually sees it as its task to rediscover in everything the most that it can of what is old and familiar – well, these people may betake themselves to intuition, but they should not declare it to be philosophy, nor proclaim experiences to be knowledge; let them admit that it is artistic, not intellectual, satisfaction, which they seek and enjoy."

---

6 Unlike Wittgenstein, Mach is very good example of a contemporary intellectual – he was born in Chrlice (nowadays a part of Brno), studied at catholic Gymnasium (high school) in Kromeriz and then moved to Vienna. He is well known namely for his work in physics, where his name is nowadays used for measuring the speed of sound. He – among others – believed that physics (and not metaphysics) is methodologically able to handle all the facts (including humanities); see for example Mach 1960, pp. 446-481.

7 Newton explains the difference between intuition and reason by comparing science and alchemy – while alchemy depends on intuitive belief, science has clear language and tangible proofs; see for example Westfall 1983, p. 23.

8 This later term indicating empirical positivism was used mainly by Mach's critics – see for example Illenkov 1982, p. 3. The term also reflects Mach's strong will for defending the empirical element in positivism. His fierce attacks were aimed at those who pleaded concurrent approaches reportedly led to a number of unfortunate consequences out of which the most tragic was the suicide of another great physicist, Ludwig Boltzmann; see Yourgrau 2007, p. 38.

9 These attempts had, however, very solid grounds in Kant and were even sponsored by contemporary theoretic inventions made in quantum mechanics. Especially the latter is something that Schlick was never able to respond to satisfactorily (see Schlick 1979, pp. 153-189).

10 See Schlick 1979, pp. 150-151.

Despite of all unfortunate historical and political happenings, the Viennese spirit of logical positivism was flourishing even throughout the first third of the twentieth century and gave birth to the concepts that have steered the development of mankind until now. The 'Vienna syndrome',[11] was so strong that it kept together the contemporary elite even despite of the Great War, dissolution of the Austrian Empire and the consequent economical crisis. It is then a paradox that such a strong movement was destroyed in just a couple of months by something that it silently helped to emerge,[12] but that was not based on rationality or logic, but on intuitive ideology: Nazism.

Albert Einstein later commented on the role of modernity in the development of ideologies of envy saying that[13] "[o]ur age is proud of the progress it has made in man's intellectual development. The search and striving for truth and knowledge is one of the highest of man's qualities – though often the pride is most loudly voiced by those who strive the least. And certainly we should take care not to make the intellect our god; it has, of course, powerful muscles, but no personality. It cannot lead, it can only serve; and it is not fastidious in its choice of leader. This characteristic is reflected in the qualities of its priests, the intellectuals. The intellect has a sharp eye for methods and tools, but is blind to ends and values. So it is no wonder that this fatal blindness is handed on from old to young and today involves a whole generation."

Coding: Yes, we can

One of the key aspects of logical positivism is the positivity, or objective cognizability, of knowledge. As all knowledge has to be obtained rationally, positivists believe that it should also be possible to present it to the ratio of someone else and to eventually make it an object of logical review. This, of course, requires having a proper language that is able to serve the purpose of objectively (re)viewable monotonous and perfect transfer of knowledge from one to another.

To shortly illustrate this positivist call, we can use again the sharp and uncompromised words of Ludwig Wittgenstein, whose statement is so simple that it could be used as a heading and at the same time as the content of the last chapter of his *Tractatus*: "What we cannot speak about, we must pass over in silence."

---

11 This term is used by Palle Yourgrau for extraordinarily strong identification of the intellectual community with the place arising of the fact that its members felt the uniqueness of the situation and did not want the spirit to vanish that, as proved later, never returned in any other place in the world. See Yourgrau 2007, pp. 77-89.

12 There is a reason to think that general focusing on logic and neglecting metaphysics (or morality) in fact enabled the development of Nazism – for an interesting discussion, see for example Strong & Sposito 1995, p. 263-287.

13 See Einstein 2006, p. 238.

The claim for the positivity of knowledge has, of course, not emerged in the era of late modernism. Much earlier, we can see very strong efforts to create a language capable of serving the above requirements in the work of the 'last real philosopher' Gottfried Wilhelm Freiherr von Leibniz.[14]

The efforts of Leibniz towards creating a monotonous and logically perfect language were definitely not aiming easy goals. In fact, he started working on a language that would be universally applicable on any kind of knowledge and that would be able to keep its structure forever just with marginal amendments to its terminology.[15] Despite of Leibniz's geniality, the project of universal *calculus philosophicus* was not successful.[16]

Despite of the fact that Leibniz has failed, the modernist and later positivist call for perfect language prevailed and became even more urgent at the end of nineteenth century. The experience with *calculus philosophicus* just led to reconsideration of the primary task. It was obvious that creating universal perfect language goes beyond human capabilities and so it became clear that the way to at least partial success might be attained only through mitigating basic requirements.

Consequently, the first more or less successful attempt of getting close to *calculus philosophicus* was not aimed to become universal language at all, but to serve only as a simple representation of basic logical formulas. Although it might seem as just marginal achievement compared to Leibniz's challenge, Frege's *Begriffsschrift*[17] meant in fact a revolution in many areas of knowledge, namely in philosophy, mathematics and logic. To put it in brief, Frege had simply shown that finding perfect language for particular tasks, i.e. coding, might be possible.

Frege's work inspired many other philosophers and mathematicians and brought even more modernist optimism into a society already highly optimistic of knowledge. His formal convention became a widely accepted tool for expressing various mathematical and logical concepts as well as for articulating logical findings of empirical disciplines.

That great achievement was, besides of its impact on mathematics and logic, also acknowledged by moral philosophers. The only problem in applying Frege's logical code on ethical rules was that empirically-based positivist

---

14 Leibniz got the label of the 'last real philosopher' from one of his great admirers, Norbert Wiener, who noticed the fact that he was able to have under control nearly all the contemporary knowledge (i.e. the knowledge of all existing and relevant scientific disciplines); see Wiener 1948, p. 2.

15 Leibniz even believed that any (true) scientific discovery has to be followed by an amendment of the language in order to express it and vice versa that an absence of new terminology makes it impossible to engage in scientific research (as it is impossible to express its results); see Rutherford 1995, p. 234.

16 The attempt of creating *calculus philosophicus* is mapped in detail in Oxford compendium dedicated to Leibniz; see Rutherford 1995, pp. 224-269.

17 For an English-written explanation of the aim and role of this language, see for example Lee 1997, p. 25.

expressions operated with basic categories of 'true/false' while ethics works mainly with another binary category of 'valid/invalid'.

Probably the first philosopher who used Frege's 'code' in order to express rules instead of facts was Austrian Ernst Mally[18]. He engaged in a number of tasks that were later (in some cases even by a decade) tackled by his famous followers Von Wright and Jorgensen[19].

Coding the morality aimed at bringing moral philosophy closer to the 'real' sciences by giving it an opportunity of logical expression, assessment and provability of its statements. Moreover, one of the side effects of the development of deontic logics (i.e. logics based on deontic operators), let us to pass in silence for a moment whether desirable or non-desirable, was also the deemed possibility of precise coding of legal rules. In other words, while Frege showed that precise coding is possible, Mally demonstrated that precise coding might be used also in the area of legal (or any other) rules.

The limits of coding

When Russell issued together with Whitehead their *Principia Mathematica*,[20] it was considered as a complex and complete compendium of contemporary mathematics. Frege's new code made Russell and Whitehead able to express their system, statements and implications with a level of perfection that could have never been reached before. Moreover, it seemed that similar achievements in methods of coding of moral philosophy were sooner or later to lead to the development of a more or less complete system of logical symbols that would be able to handle also the tasks of ethics and the law. In those days, achieving these extremely attractive feats of human reason seemed just like a matter of time. However, they simply looked too good to be true.

At the same time when optimistic modernism was at its full strength, a person is born at the suburbs of Brno whose destiny was to change the very grounds of mathematics, logic and overall philosophy of science: Kurt Gödel. After he moved to Vienna, his exceptional talent and diligence lifted him soon to most prestigious scientific saloons including Schlick's circle. Unlike other members of this prestigious society, Gödel was reported as very

18 Mally's work is not very well know, probably because of his highly problematic political positions and opinions. If he had not been such a strong German nationalist and later fascist, his achievements would probably receive much broader attention (see Mally 1926).

19 One of the questions put forward and being solved by Mally were conditional deontic operators that were re-invented and used by Von Wright almost twenty years later.

20 This opus magna concluded Russell's work on the concepts of mathematics and was planned as a complete and perfect system of mathematics and the ground for any future mathematical research. Despite of its imperfections (see below), it is still being used as one of the greatest pieces of classical mathematics; see for example its reprint Russell 1997.

rarely speaking or arguing, but rather making notes and thinking silently.[21] As his rhetoric skills and even body constitution were relatively weak, he took the courage to speak out his theses only in situations where he had them backed by precise and undoubted arguments.[22]

When this genius mathematician started to analyze Russel's *Principia Mathematica*, his original intent was totally different from what was about to come out. He engaged in the analysis of Russel's work using the same positive logic methodology, but he found out that diligent application of that method showed inconsistencies and unverifiable elements. Upon these findings, Gödel formulated and proved his general and special theorems of incompleteness.[23] In particular, he found out that

1. positive axiomatic logical systems cannot be complete and internally consistent at the same time

2. the axioms of such systems cannot be proved within their structure (i.e. they have to be proved by measures standing outside of the system)

It took mathematics, logic and other affected disciplines a while before they recognized the true relevance and impact of the above theorems.[24] In fact, they were not applicable just on Russel's *Principia Mathematica*, but equally on any other complex logical systems based on axioms. Consequently, Gödel's theorems of incompleteness have once and forever proved that any attempt of coding of rational knowledge inevitably leads to imperfections. In other words, Gödel proved that any complex expression of the human reason has to be either incomplete or internally defective.

If we combine the outcomes of two of the greatest minds of twentieth century, Wittgenstein and Gödel, we come to quite frustrating conclusions. While Wittgenstein claims that we should speak only when we are able to precisely express our knowledge (i.e. in a logically provable manner), Gödel states that we will never be able to formulate (code) our complex knowledge in such a way. The only logical conclusion of these strong and precisely argued top statements of logical positivism is obvious: scientists should either forget about their ambitions and elaborate only on particular (not complex) tasks, or they should keep silent.

---

21 Palle Yourgraou gives a comprehensive and picturesque view on Gödels personality in Yourgrau 2007, pp. 21-28.

22 This is also considered as one of the reasons why just very little has been published by Gödel upon his friendly discussions with Einstein; see Yourgrau 2007, p. 150.

23 See Gödel 1931. The English translation of his article is available in numerous collections. The most complete is up until now a three-books series issued by Oxford Publishing; see Gödel & Feferman 1986.

24 For the genesis of acceptance and implementation of Gödel's theorems, see for example Smullyan 1992.

As Gödel formulated his theorems at a very young age, their recognition and acceptance by the discipline that they targeted in the first place, i.e. mathematical logic, occurred relatively slowly. Their reception went in stages from ignorance through refusal to (unsuccessful) attempts of proving otherwise. In any case, Gödel did not really care about any broader impact of his discovery – the only thing that was really able to attract his attention were sporadic attempts to raise and argue particular counterarguments.

At the end of the process of recognition of what Gödel did primarily to Russell and Whitehead and consequently to all modernists, there was no other option than to take the theorems of incompleteness simply as factual limits of human reason. To a certain extent, the theorems of incompleteness were – as to their philosophical impact – comparable to Einstein's findings on the absoluteness of the speed of light, as they have clearly outlined the limits of human efforts.

Both Ludwig Wittgenstein and his teacher and supporter Bertrand Russell did not physically take part in Viennese café life. That might be one of the causes for the fact that Russell hardly recognized what happened to his *opus magnus* and to other modernist attempts in the light of Gödel's theorems of incompleteness. Consequently, Russell's rational optimism managed to continue to enlighten his pupils in such a way that even later recognition of objective limits of reason laid down by Gödel could not change their interests and engagements. Thus, while the philosophical circles of Vienna started to recognize the upcoming end of pure modernity, another contemporary center of rational thinking, Cambridge, continued to inspire the next generation of scientists by partially false but beautiful and motivating belief in rational perfection that has resonated the college walls till today.

The limits of freedom

Although Russell and his pupils, including the founder of cybernetics, Norbert Wiener, considered themselves as followers of earlier modernist thinkers like Kopernik, Kepler and Leibniz, substantial differences between original and peak modernity can be observed. Early modernists understood the permanent quest for knowledge as an attempt of getting close to the divine.[25] Therefore, their works take metaphysical (spiritual) elements as points of reference for rational knowledge. In their works, coding is focused on describing the creations of God and is inevitably understood as naturally faulty, while perfection is not a sign of humanity but of divinity.

Contrary to that, peak modernists like Russell or Wittgenstein see the divinity and its consequences tackled by the metaphysics just as a kind of construct that is hard or impossible to be reasoned by rational arguments. Having problematic personal experience with confessions and with church-

25 See for example Mercer, Sleigh 1995, pp. 67-123.

es (in the case of Russell it was the Anglican Church, in the case of Wittgenstein it was the Catholic Church), they saw the divine not as a point of reference, but rather as a constraint limiting the freedom of the human mind. Similar were their views on other metaphysical concepts, such as morality.

Speaking with the words of Michael Oakshott,[26] the peak modernists considered the reason as the key of positive development of the platform of understanding that serves as the basis of human freedom.[27] They believed that this platform has a purely rational nature and the broader it is developed, the wider are the limits of our freedom. Consequently, they saw the ratio as the main source of human freedom, whereas metaphysical concepts are only limiting its reach.[28]

What Gödel did in that respect was proving that the platform of understanding can be limited also by absolute limitations of the rational mind. In other words, if we take the ratio as the only developing factor of the platform of understanding, the reach of the platform of understanding is naturally limited and these limits are quite clear – simultaneous completeness and perfection.

The levels of coding

In his later publications, Aernout Schmidt speaks about the distinction between a more or less abstract concept of law and its operational mode.[29] While the law represents the objectively indefinable complex, its operation, i.e. the activity undertaken within the system of law, is much more particular and understandable. While we are unable to completely and precisely describe, neither in statutes nor in doctrinal publications, the nature, structure or content of law, we are relatively well able to cognize how the law works, i.e. what is the regime of legal procedures, what rights arise out of particular actions etc. In other words, while the level of the perfection of coding the law is relatively lower, the level of understanding and coding its operations can be quite high.

---

26 Oakshott distinguishes between theoretical and practical knowledge. The first of those two can be compared with the first level of coding discussed below and the latter with the second level of coding; see Oakshott 1975, p. 13.

27 The platform of understanding represents in Oakshott's theory individualized source of knowledge that might be determined by a multitude of factors – for an informative explanation of the concept and its comparison with Wittgenstein, see Craig 1998, p. 71.

28 This opinion can be argued through the background of all inventions that could have been, or more often in fact were, later abused for irrational purposes. Ethical contemplation of those who brought these inventions forward undoubtedly slowed down or sometimes even stopped the process of discovery. For an example, see Einstein 2006, pp. 122-124.

29 This distinction is made in Schmidt 2009 and has been announced as a core thesis for a paper to be presented at Cyberspace 2009.

It is then obvious that it is more important and attractive for legal practice to work with codifications of the operational mode of the law rather than with the codifications of law itself. Thus, legal practitioners work with commented statutes, rendered case-law collections or particular legal opinions rather than with contemplative legal theoretic books analyzing the nature of the law or its grounds. It is not just because the codifications of legal operations give more particular answers on practical legal questions such as how to file a lawsuit or how to write a contract, but also because the operational mode of law is understandable to a very large extent by the ratio. On the contrary, codifications of mere law, regardless of whether they are contained in statutes (namely in constitutions) or in great works of legal philosophers, are too far from rational understandability and operability for legal practice.

Coding of cyberspace also works in two layers. Unlike in the case of law, the first layer, i.e. code in Lessig's sense,[30] is without any dispute purely developed by human mind.[31] Obviously, it is extremely difficult to codify natural laws of cyberspace to be complex and perfect at the same time,[32] so Lessig's code is and will always remain incomplete and internally faulty, probably even more so than the law. However, the operational mode of Lessig's code can be rationally understood up to very high level of perfection and consequently codified into the form of technical specifications, user manuals etc.

The parallel between second level understanding and coding of law and second level understanding and coding of Lessig's code can be demonstrated through the role of those who professionally engage in these, namely practicing lawyers and hackers.[33] In both cases, their main task is to develop the understanding of the second level of coding, i.e. of the operational mode. In other words, their job is to understand how the law or the internet works.

Taking into account that the law is inevitably incomplete and faulty, lawyers might develop their rational understanding of its operational mode to such an extent that they might be able to reveal its internal errors and contradictions. Similar to that, hackers might develop their knowledge about the operational mode of the internet to the extent in which they are able to understand problematic parts and gaps of the code. Thus, it is in both cases

30 Lawrence Lessig formulated a thesis that the (computer) code is the law of the cyberspace – unlikely the (state) law, it rather acts as natural laws not motivating but determining human behaviour. See Lessig 2006.

31 Purist positivists believe in objective law being also developed only by rational acts of legitimate humans (the Lawmaker). However, this belief turned to be at least partially false as proved by multiple examples of law being positively developed and formally perfect but basically faulty just like in the case of fascist or communist law.

32 By perfection we mean code's ability to define cyberspace as a space suitable for the development of artificial counterparts of life.

33 We use this term in its more formal meaning – nowadays, it is rather used to indicate computer criminals, while in the past, it indicated people who were skilled enough to dispose with the computer network according to their will; see Raymond & Steele 2000.

possible to rationally develop perfect operational knowledge about imperfections of the respective systems, i.e. of the law and of the internet, in the same way as Gödel rationally developed his knowledge about the imperfections of Russell's *Principia Mathematica*.

It is a paradox that our ability of perfect second level coding – including our ability to reveal inconsistencies in first level code[34] – in fact partially proves the modernist idea of rational perfection. However, such perfection can be reached only when the object is rational code (regardless whether we speak about the code of mathematics, of the internet or of law).

In any case, we see that it is objectively, although ideally, possible to reach perfect knowledge of legal practice as well as it is objectively possible to reach perfect knowledge of functioning of the internet. Moreover, this rational knowledge really constitutes the platform of understanding of respective experts and defines the limits of their freedom. If a lawyer develops perfect knowledge of the operational mode of the law including its inevitable inconsistencies, it extends his abilities to such an extent that she might then decide whether she will obey the primary code or not. Similar to that, if a hacker learns perfectly about the code governing the internet including its inevitable gaps, it makes her able to decide whether her activities will be determined by the code or whether she will simply omit the code and act contrary to it.

Russell would surely be pleased to learn about professions that can acquire complete and perfect rational knowledge and where the level of rational knowledge determines their freedom to decide. In these cases, it is also true that any metaphysics might not extend the platform of understanding of above mentioned professionals, but rather limit it. If, for example, a hacker starts to morally contemplate over a planned attempt to break into some information system, it might not lead to extending her abilities but rather to omitting or mitigating possible actions. Similarly to that, any result of a lawyer's dilemma over the extent to which she is going to defend herself against a ticket might only lead to the limitation of the use of her true abilities.

The above-mentioned is, however, valid only if we speak about the second level of coding (understanding and expressing). On the contrary, the first level of coding, i.e. trying to understand and speak about the nature, morality or law, is affected by the inevitable imperfections described by Gödel. In this case, we might formulate even an opinion that is almost completely opposite to our observations regarding the coding of the second level, i.e. that first level coding is not just inevitably incomplete and faulty, but also depending on various kinds of intuition rather than on the ratio.

34 This can be illustrated also by a very simple practical example – it is much more difficult to write the text of some normative instrument like a statute than to analyze and criticize it after it is issued.

It is relatively difficult to logically argue the thesis that the success in primary coding, i.e. in primary understanding, describing or prescribing, depends not just on ratio but also on moral, aesthetical or other intuition. When the outcome, the code, is of a rational nature, just as in the case of law or Lessig's computer code, it would not make entirely sense that its source should be based on anything else than again on ratio.

On the other hand, many of the greatest thoughts (primary codes) including those cited in this article, although created upon hard work and genius mind, must surely have been achieved not as simple causal consequence of logical thinking, but rather provoked by spiritual, emotional or other motives. The argument for stating that is simple – they simply seem too good to be mechanically produced by logical thinking.

Personal concluding note for Aernout

Searching for arguments for the above thesis that intuition plays a key role in primary coding, that would be solid enough to persuade even Aernout Schmidt, decided I to visit both past capitals of modernity – Vienna and Cambridge. I was searching there for some kind of metaphysical substance giving these places the power to motivate their inhabitants to tirelessly search for the limits of human rationality. Unfortunately, neither the palaces of Vienna nor the colleges of Cambridge provided me with a satisfactory answer.

It is true that, as noted at the beginning of this text, Vienna as well as Cambridge had enormous economical and consequently also intellectual gravity. However, it could not be the luxury, the glamour or privileges of walking on the grass and eating (although English food) in magnificent halls, that in fact motivated the brightest minds of their times to repeatedly undergo exhausting quests to the limits of human intellect.

It is therefore a bit ironic, that while I have travelled to explore the very places that according to my belief motivated Newton, Russel, Gödel, Wittgenstein, Frege, Carnap, Wiener, Mach, Schlick and dozens of others to search for perfection, the answer was still laying down on my table. I accidentally found it when checking for the deadline for delivering my contribution to this book (of course, I terribly missed it). All that time, it was contained in the title of an e-mail from Laurens Mommers: "*Liber Amicorum*…"

At that point, I found out that such books are not just made in order to pay a tribute to good friends and fellow scientists, but also to professionally express our gratitude for the friendships that extend our platforms of understanding for primary coding and free us from limits of our basic rationality. Thus, I would like to thank first for Aernout's kindness, openness and benevolence that made it possible for me to call myself a friend of his. Secondly, I would like to express my gratitude for our friendship that made me work harder, think deeper and, most of all, to be freer.

References

Craig 1998
E. Craig, *Routlege Encyclopedia of Philosophy*, vol. 7, New York: Routlege, 1998.

Einstein 2006
A. Einstein, *The Einstein Reader*. New York: Kensington Publishing, 2006.

Gödel 1931
K. Gödel, Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, *I. Monatshefte für Mathematik und Physik*, vol. 38, 1931.

Gödel & Feferman 1986
K. Gödel, S. Feferman, *Kurt Gödel Collected Works I*, Oxford: Oxford University Press, 1986.

Ilyenkov 1982
E. Ilyenkov, *Leninist Dialectics and the Metaphysics of Positivism*. London: New Park Publications, 1982.

Lee 1997
B. Lee, *Talking heads: language, metalanguage, and the semiotics of subjectivity*. Durham: Duke University Press, 1997.

Lessig 2006
L. Lessig, *Code V.2*, New York: Basic Books, 2006.

Mach 1960
E. Mach, *The Science of Mechanics*, Chicago, Open Court Publishing, 1960.

Mally 1926
E. Mally, *Gurndgesetz des Sollens. Elemente der Logik des Willens*. Graz: Leuschner & Leubensky, 1926.

Mercer & Sleigh 1995
C. Mercer, R. C. Sleigh jr. Metaphysics: The Early Period to the Discourse on Metaphysics, in Jolley, N. (ed.) *The Cambridge Companion to Leibniz*, Cambridge: Cambridge University Press, 1995, pp. 67-123.

Oakshott 1975
M. Oakshott, *On Human Conduct*. Oxford: Oxford University Press, 1975.

Raymond & Steele 2000
E. S. Raymond, G. L. Steele (eds.), *Jargon File*, Project Gutenberg (www.gutenberg.org), 2000.

Rutherford 1995
D. Rutherford, The Philosophy and Language in Leibniz, in Jolley, N. (ed.) *The Cambridge Companion to Leibniz*, Cambridge: Cambridge University Press, 1995, pp. 224-269.

Schmidt 2009
A. Schmidt, Radbruch in Cyberspace: About Law-System Quality and ICT Innovation, forthcoming, *Masaryk University Journal of Law and Technology*, vol. 3(2), 2009.

Schlick 1979
M. Schlick, *Philosophical papers*, ed. Henrik L. Mulder and Barbara F. B. van de Velde-Schlick. Springer, 1979.

Smullyan 1992
R. Smullyan, *Gödel's incompleteness theorems*, Oxford: Oxford University Press, 1992.

Strong & Sposito 1995
T. B. Strong, F. A. Sposito, Habermas' Significant Other, in Stephen K. White (ed.) *The Cambridge Companion to Habermas*. Cambridge University Press, 1995.

Sullivan 1933
J.W.N. Sullivan, *The Limitations of Science*, New York: The Viking Press, 1933.

Whitehead & Russell 1997
A.N. Whitehead, B. Russell, *Principia Mathematica*. New York: Cambridge University Press, 1997.

Westfall 1983
R. S. Westfall, *Never at rest: a biography of Isaac Newton*, Cambridge: Cambridge University Press, 1983.

Wiener 1948
N. Wiener, *Cybernetics: or, Control and communication in the animal and the machine*. Cambridge: MIT Press, 1948.

Wittgenstein 2004
L. Wittgenstein, *Tractatus Logico-Philosophicus*. Whitefish: Kessinger Publishing, 2004.

Yourgrau 2007
P. Yourgrau, *A World Without Time – The Forgotten Legacy of Gödel and Einstein*, New York: Penguin Books, 2007.

Free Software and the Law

On collaborative law-making and adjudication

Krzysztof Siewicz■

Introduction

In February 2009, during his occasional speech to investors, Steve Ballmer (Microsoft CEO) talked a bit about the company's competitors in the market for operating systems.[1] He mentioned three of them as most important ones. First, there are those who trade in unauthorized (unlicensed) copies of Microsoft Windows, the so-called *pirates*. Second, there is Linux. Third, there is Apple. The term *Linux*, as used by Mr. Ballmer in his speech, denotes a whole family of operating systems.[2] These operating systems consist mainly of Free Software programs. A Free Software program is a computer program that can be developed, distributed, and used by anybody. Many individuals, companies, NGOs, and government agencies contribute to Free Software without direct compensation. So, when Microsoft CEO calls *Linux* a competitor, it means that they seriously consider that by allowing anyone to develop, distribute, and use software, one can manage to deliver a product that can become a substitute for the in-house developed Windows. The same Windows, in which the company invests millions of dollars every year, and for which it pays an army of employees to work at.

This idea may seem a fallacy. Indeed, at first glance it appears naive to believe that it would be possible to manufacture a good quality product by allowing anyone to participate in the production, and by allowing anyone to offer that product in the market after it is developed. It immediately brings to mind *The Tragedy of the Commons*[3]. Nevertheless, a growing number of individuals, companies, and government agencies develop, distribute, and use Free Software. Also, although not all Free Software programs are of good quality, some of them are. More importantly, many of them are of sufficient quality to constitute substitutes for such proprietary software as Microsoft Windows. So, we may state that the idea is not a fallacy, at least not a complete fallacy. Indeed, the practice shows that Free Software has made a substantial success.

■ Krzysztof Siewicz is writing a Ph.D. thesis on legal issues of open source software, at the Leiden Law Faculty.

1 AppleWatch, *Microsoft CEO Scoffs at Mac Share Gains*, at: http://blogs.eweek.com/applewatch/content/macbook/microsoft_ceo_scoffs_at_mac_share_gains.html.

2 Precisely speaking, 'Linux' is the name of an operating system kernel only.

3 Hardin 1968.

The success of Free Software has stimulated the emergence of many initiatives that in one way or another copy, mimic, or at least borrow from the approach that has been applied in the development of Free Software. Many such initiatives have succeeded extraordinarily, such as Wikipedia. However, I do not wish to argue that in the future all computer programs will be Free Software, or that everything should be organized in the way the development of Free Software is organized. Nevertheless, I find it intriguing to investigate whether it would be possible to organize the law in such a way. I will use 'the law' in a broad sense. I will use the term to cover both (1) lawmaking (production of *positive law*), and (2) application of the positive law (adjudication).

So, I would like to provide an answer to the following question: *Is it possible to organize the law (in the above sense) in the way the development of Free Software is organized?* In order to answer this question, I will first briefly present what Free Software is. Then, I will identify the essential elements of its development. Afterwards, I will search for these identified elements in the current law. If they are not present, I will perform a preliminary analysis of whether and how to implement them. Finally, I will conclude this small research project, by summarizing the findings about similarities between the law and Free Software, about the reasons for organizing the law in the way the development of Free Software is organized, and about ways to set up such an organization. This conclusion will constitute an answer to the above question.

What is Free Software?

Free Software is software that is available to any interested party together with the rights to control the functioning of the software. In order to allow for an effective control, the rights to Free Software encompass source codes, not only the binaries. To put it in a nutshell, a source code is a human-readable expression of a program. When presented with a source code, a person skilled in the art of programming can study the program, understand it, identify existing flaws ('bugs'), and design corrections of the bugs or any other desired improvements. Generally, for the purpose of using a program the source code has to be translated into a machine-readable object code (also referred to as a "binary"). Binaries are impracticable to study and modify; this makes access to source code necessary for the purpose of modification.

But mere access to source code is insufficient for a program to constitute Free Software. An additional necessary condition is that users of the program are allowed to undertake a set of activities with the program. A list of this activities has been proposed by Richard M. Stallman and the following quote from his *Free Software Definition* is relevant here.

"Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it means that the program's users have the four essential freedoms:

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and change it to make it do what you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help your neighbor (freedom 2).
- The freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits (freedom 3). Access to the source code is a precondition for this."[4]

As a default legal rule, these freedoms do not exist. Some (narrow) exceptions notwithstanding, all activities mentioned in the above quote are reserved exclusively to the copyright holder of the program in question, and users may undertake them if only the copyright holder agrees. But there are quite many copyright holders that do agree. The consent comes in the form of a copyright license. Since the usual practice is to use model (adhesive) licenses and to publish programs licensed in such a way in the Internet, the result is that every user of a Free Software program is granted with the above four freedoms. Simply speaking, almost everyone is allowed to do almost everything with Free Software.

However, even though the freedoms are so broad and even though they apply to a large number of persons, the development of Free Software is far from anarchy. More precisely, it has been observed that an important part of the development is performed by communities. By a 'community' I mean a group of users that collaborate in the development of a Free Software project and who may also distribute the project to other users, as well as to those who provide guidance on its use. Communities consist of individuals, but they may also include firms, NGOs, and government agencies. Communities gather around single programs or collections of programs, organized in a functional whole (hence, 'projects').

Depending on the size and nature of the project, the number of contributors, its development stage, *etc*., the organization of communities takes various forms. In small projects there is usually one person that supervises the maintenance of the whole project, while other contributors restrict themselves to submitting contributions only. In bigger communities the authority and responsibility for the project is distributed. The social structure of an average software community gathered around a medium or large Free Software project usually consists of (1) a few leaders who decide about the devel-

4 R.M. Stallman, *Free Software Definition*, at: http://www.gnu.org/philosophy/free-sw.html.

opment of the project and (2) a number of contributors who follow the leaders. We shall refer to the leaders as *project owners*.

According to Eric S. Raymond "[t]he owner of a software project is the person who has the exclusive right, recognized by the community at large, to distribute modified versions."[5] More precisely, project owners serve as a source of *official versions* of the project. Unofficial versions are usually understood as versions maintained individually by users outside of the community. Actually, even inside the communities it is every user's right to modify Free Software for their own use, and to distribute such modifications in some 'closed user or development group'.[6] In fact, no project owner can legally prevent any user (including community participants) from releasing competing versions of the project on their own. Also, project owners may not legally bind other community members to produce a particular contribution. Straightforwardly speaking, project owners merely accept or reject contributions that flow to the project, and a rejection does not prevent from including the contribution in an unofficial version. In order to exercise this limited authority, project owners gather and manage resources necessary to control the quality of the contributions (both technical and legal), and to integrate the contributions in the official version. The project owners assign these activities between themselves and recruit additional project owners from the community if there is such a need.

Essential elements of Free Software development

After this brief presentation, I am now ready to identify the essential elements of Free Software development. These are: (1) access to source codes of computer programs under the terms that allow all users to undertake all freedoms as defined by Stallman, and (2) existence of software communities, wherein some users subject themselves to the authority of project owners who organize the development of official versions of the programs. This is a very simplified statement, but it is sufficiently fair and accurate for the purposes of this article.

---

5 Eric S. Raymond, *Homesteading the Noosphere*, at: http://www.catb.org/~esr/writings/cathedral-bazaar/homesteading/. Project ownership understood as a kind of exclusivity over the maintenance of the project may seem a paradox, as above we extensively explained that under the Free Software licenses every user is allowed to maintain Free Software on their own. In fact, there is no paradox, as long as we read Raymond carefully and note the distinction between (1) the legal right, which is indeed available to everyone as provided for in the licenses, and (2) the right "recognized by the community", which is granted to certain individuals only. Indeed, project ownership may not be mistaken for any kind of legal title in software, in particular the copyright to the project, although it may accompany such a title. See also: Guibault et al. 2006.

6 Eric S. Raymond, *Homesteading the Noosphere*, at: http://www.catb.org/~esr/writings/cathedral-bazaar/homesteading/.

Free Software elements currently present in the law

The above statement of the essential elements of Free Software development consists of terms specific to software and not to the law. These are 'computer programs', 'source codes', 'freedoms as defined by Stallman', 'software communities', 'project owners'. So, at first glance it appears that it would be hard to identify these elements in the law. But let me look more into the nature of the designates of these terms, before calling it a day. Let me start with the notion of a 'computer program' and then gradually move to other terms.

Lawyers tend to seek for definitions of terms in the provisions of law instead of looking for them in encyclopedias or other relevant literature. I will eagerly follow this approach, which would save me a discussion about technical peculiarities. There is no such definition of a 'computer program' in the EC and member states' legislation that I am aware of. Allow me then to turn to the US Copyright Act Sec. 101 and the definition included therein, which states that a computer program is a "set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result." Please note that if we removed references to a computer from that definition, it could be expressed in the following way: "set of statements or instructions[, of which the purpose is] to bring about a certain result."

This reformulation boils down to omitting the fact that computer programs are to be used in computers. Also, instead of mentioning this fact, it stresses that programs are 'statements or instructions' aimed at obtaining 'certain results'. When we realize that this is the important part of the nature of computer programs, we have to admit that there are quite many similarities between the programs and the law. Namely, positive law is indeed a set of statements or instructions, aimed at obtaining certain result. The intended result of the law is a regulation of human behaviour. We could even attempt to argue that the law is a "set of statements or instructions to be used directly or indirectly in (addressed to) a human being in order to bring about a certain result."[7] In other words, I emphasize that both computer programs and the law are essentially sets of statements or instructions aiming at some results. In this article I would like to proceed as if the only difference between the two were to whom they are addressed.[8]

Having such an understanding, it is much easier to identify the equivalent of the notion of 'source codes' in the law. If a computer source code is an expression of a program understandable and capable of being manipulated by a human, than the 'legal source code' must be an equivalent expression of the law (positive law). Precisely speaking I refer here to texts of statutes or execu-

7 Here, I would like to refer the reader to Botler 1984, who elaborates on what I have just committed – application of a description and understanding of the currently dominating technology to an (directly) unrelated concept.

8 And this could change in the future, for example if computers are allowed to adjudicate. Then, we will require a positive law addressed to computer judges (both material and procedural law).

tive orders.[9] It has been an established (or at least proposed) practice since the dawn of the rule of law, to present positive law in acts published in a language understandable to society. A further analogy to computer source codes can be performed. Namely, similarly to source code that has to be translated (compiled) into binaries, positive law often has to be interpreted to construct the actual legal rule that follows from it (*i.e.*, a right or an obligation of a certain party). I will develop this analogy when discussing adjudication later on.

Let me now search for a legal equivalent of the notion of 'freedoms as defined by Stallman'. As I explained above, these freedoms do not exist in computer programs as a default, but they have to be granted to users by the copyright holders. As a default, users are not allowed to manipulate computer programs, even if they are presented with their source codes. Positive law bears much similarities here too. Although texts of legal acts are generally available to everyone, not everyone is allowed to modify the law. Generally, this authority is reserved to selected representatives only – the legislative power. However, the legislative may allow users of the law to perform some degree of modification. This is particularly visible in civil law which contains a lot of *iuris dispositivi*, *i.e.*, default rules that can be modified by parties to a certain degree. Conversely, criminal or administrative law rarely may be affected by the addressees in such a way.

This observation leads us to the identification of equivalents of 'software communities' and 'project owners' in the law. The law is developed by the society in a way similar to how Free Software projects are developed in the communities. According to established theories dating back at least to the Enlightenment, the sovereign (the society) empowers its representatives (such as the members of parliament) to pass laws that regulate each and every member of the society. The law includes also the rules that regulate the manner in which this representation is performed, as well as the manner in which other rules are enforced. So, each society having its laws prepared by the legislative consisting of elected representatives, can be compared to a software community that develops a Free Software project under the authority of project owners.

Certainly, the degree of freedom that every user of such a Free Software project can exercise towards their own copies of programs included in the project is much broader than the degree of freedom that every citizen can exercise towards the law. While software can be easily copied and used in a given computer in isolation from computers of other users, it is not that easy to multiply the law and run its multiple instances in isolation. This requires that the whole society (or a significant part of it) agrees and coordinates their activities. Such attempts, are usually called '*coup d'etat*', 'revolution', *etc*. Notably, these terms have their close Free Software equivalent, which is 'forking', but I will not elaborate on this concept here.

9 Although every practicing lawyer would agree that there are statutes and executive orders that are completely incomprehensible for any human being.

At this moment I can already conclude that there are many Free Software elements currently present in the law. Precisely speaking, when we think about the similarities between the law and software, we realize that positive law is developed by representatives of society in much the same way as Free Software programs are developed by software communities under the authority of project owners. An important difference, however, is that users of Free Software have much more freedom towards their own copies of Free Software as compared to the freedom of individuals from a given society towards the law of this society. But at the beginning of this article, I decided not to focus on (1) the making of the positive law only. I used the term 'the law' to encompass also (2) the application of law (adjudication). Let me now briefly search for Free Software equivalents in this second area of the law.

Roughly speaking, adjudication is done by taking a text of positive law, identifying provisions applicable to the facts of the case, interpreting the relevant rights and obligations from the provisions, ordering the parties to follow these rights and obligations, and (unless the parties obey) performing enforcement actions. This process can be compared to running a program on a certain computer and using the result of the program. Let me explain this far analogy. If the purpose of a program is to sort numbers, the computer will present the numbers in an order when the program is run on it. Similarly, if the purpose of a given provision of law is to make one party pay a price for goods delivered by the other party, a judge will order the infringing party to pay. I envisage that many readers do not see any similarity at all. Fortunately, it is not that important to convince them, since even if there is a similarity, that similarity alone is not sufficient to conclude that there are any Free Software elements in adjudication.

In the search for closer and more relevant similarities it is worthwhile to notice that court decisions are usually published together with reasoning. In some jurisdictions these publications (more precisely: *rationes decidendi*) become a part of the law, while in other ones they are still used in subsequent interpretations of the positive law. Reasoning is for a court decision what source code is for a computer program. Namely, it allows to understand the legal rule in question and to replicate the application of this rule to identical or similar facts. A judge would often be helpless if not allowed to reuse past decisions and reasoning with them when adjudicating current cases. So, there is a close analogy between such a re-use and the re-use allowed for users of Free Software, who may combine an original Free Software program with any modifications to obtain an improved whole. Software communities, similarly to the society, agree that such manipulations should be performed (or at least authorized) by qualified personnel only (the law – judges, Free Software – project owners).

As a side note, I would like to draw the reader's attention to the fact that the publication of court decisions and the presentation of their complete reasoning is an important safeguard to the rule of law, in addition to the publication of positive law. This is so fundamental that I do not even have to provide a reference here, but let me refer you to Fuller and his *Morality of Law* as

an example. Indeed, one could not imagine a democratic state with secret laws and secret court decisions escaping second instance scrutiny because of their obscurity. At the same time, these elements (publication and capability of being reused) are essential elements of Free Software. Conversely, proprietary software is based on the premise that source codes should not be publicly available, and the general public should not be allowed to manipulate them.

Still, an important difference between Free Software and adjudication is as follows. While anyone is free to manipulate own copies of Free Software despite the official versions are handled by project owners, there is generally no possibility that individuals could adjudicate themselves, without resorting to the state-appointed judge. Exceptions, which confirm the above rule, include methods and institutions of ADR, such as the international commercial arbitration. With some reservations, also negotiations between parties to a contract can be seen as a kind of exception. Namely, instead of resorting to a judge, parties often decide to settle matters between themselves. By doing so they essentially agree on what the law is between them. Certainly, there are limits to what parties may agree on, but undoubtedly their agreement within these limits constitutes the law (*inter partes*).

Here, I can conclude that the following Free Software elements are already present in the law. First, the law (positive law) is developed by representatives of society in much the same way as Free Software programs are developed by software communities under the authority of project owners. Second, the adjudication of the law is performed in a way that reuses past decisions in present cases in much the same way as software communities reuse existing Free Software in the development of their projects. Despite these similarities there remain important differences, which generally boil down to barriers of entry. There are generally no barriers an individual has to face before manipulating his own copy of a Free Software program in order to make an unofficial version of it. The barriers increase, if the individual wishes to affect the official version, which is subject to the project owners' consent. But even such barriers are low if compared to the barriers that society places on individuals who wish to manipulate effectively the making of positive law or adjudication. At best, they can do so only *inter partes*.

Proposal for implementing Free Software elements in the law

It follows from the above that although the law already has much in common with Free Software, there is still at least one important difference. The difference is between a high barrier that individuals have to face if they wish to manipulate with the law (change positive law or adjudicate) as compared with the relatively low barrier to the manipulation of Free Software. Why should not society relax the control exercised by its representatives and appointed officers over the law, and give more of it into the hands of every

individual? The success of Free Software shows that such a relaxed control may lead to the development of good quality products that successfully compete with products developed under strict private control. Can the law be better if produced in such a distributed and collaborative manner? There is more than just the economic argument. I do believe that such an experiment is worth a try as a way of bringing us closer to the Bergson's and Popper's ideal of *open society*.[10]

Probably, I should make it explicit that I do not propose to overthrow any government, initiate revolution, or to allow any form of anarchy. I think I have made it quite clear in this article that Free Software has not much to do with anything of this kind. Any attempts to make Free Software and the law alike must take into consideration the fact that the law has to serve the whole society, whereas it is possible that a computer program is run for the purposes of a single user only, without affecting other users. So, instead of simply allowing anyone to change the law or resolve a legal dispute, the proposal should borrow from Free Software in another way. Perhaps a good way to start would be to consider allowing a broader participation of individuals in making law and adjudication, without removing the control over the effects of these activities from representatives and officers appointed by the whole society.

I can already present an example of how this could be done. In September 2007, the government of New Zealand called for public consultations of the draft Police Act. However, instead of following the traditional exchange of paper comments to the draft, a public wiki was launched. The response outgrew expectations, and according to the information on the archived wiki, the draft has been amended using comments that everyone could enter directly on the wiki over the Internet.[11] A similar initiative has been performed by the Polish Ministry of Finance in 2006, when the ministry launched a wiki for collecting proposals for amendments to tax law. Unfortunately, an archive of that wiki is not available and I could not find any information about how it affected the drafting of the proposal that was put before Sejm (the Polish parliament).

Publication of draft laws (even at their early stage of development) and making it possible for individuals to comment or even amend the drafts can lead to a material increase of the participation of the whole society in governance. Clearly, one should not expect that this would lead to any good if such wikis are left unmoderated and uncoordinated. Every project that tries to copy the success of Free Software should take care to adopt organization, which is a necessary condition of its success. Here, I will not present an elaborate proposal of how to do this for two reasons. First, it should not be done

10 For similar ideas see: Kenneth Wong, FOSS Government Policy, at: http://en.wikibooks.org/wiki/FOSS_Government_Policy.

11 Stuff.co.nz, *Police wiki lets you write the law*, at: http://www.stuff.co.nz//47127. For the archive of the wiki itself see: http://policeact.govt.nz/wiki/.

by a lawyer, but rather by a skilled manager. Second, in order to properly design such an open drafting of the law much further research is necessary, that I could not perform while preparing this article.

Instead, let me present one more example, this time related to adjudication. In June 2007, the US Patent and Trademark Office together with the New York Law School has launched the Peer-to-Patent project.[12] Simply speaking, the crux of the project was to invite the general public to examine patent applications for prior art. Normally, it has been an obligation of the examiner employed at the patent office to find prior art (apart from examining other patentability criteria). The project did not remove this obligation from the office, but it provided the office with the help of any interested individuals. Moderation and coordination procedures were put into place, since examiners were not presented with all submissions made by visitors of the web page. The 'project owners' evaluated and selected prior art before communicating it to the examiners (obviously, examiners could browse the public web page in spite of this). Also, a mechanism similar to a wiki was employed to aid users in the examination of patents and make it more easy to submit prior art.

The Peer-to-patent project, although not related to the adjudication as performed by judges, is an example of what can be done in the area of the application of law. Namely, whenever the law has to be applied (and adjudication performed by judges constitutes a subset of this application), exact facts of the case have to be determined. Apart from the facts, an interpretation of the law has to be performed, for which a research of past decisions and all related jurisprudence has to be performed. Traditionally, these activities are performed either by the parties, by special officers (prosecutors), or by the judges themselves (sometimes with the help of clerks). The development of Free Software has shown that many of these activities can be 'outsourced' to the general public, if only the procedure is properly organized. The success of the Peer-to-patent project constitutes evidence that such outsourcing can be performed in the application of the law as well.

Conclusion

I am careful of drawing too broad and general conclusions from the above preliminary analysis. Indeed, the law and Free Software have very much in common. Much more can be borrowed from the organization of Free Software development and introduced in the making of the law and in adjudication. However, my purpose was not to argue that there are no differences between the law and Free Software, or that both of them should be organized in the same way. Rather, I hope that I have stimulated the reader to start asking a question *To what extent can the process of law-making and adjudication*

12 Wong & Kreps 2009, at: http://www.ifosslr.org/ifosslr/article/view/9/6.

be 'open'? I also wanted to make the reader aware of an important limitation. It is caused by the fact that although anyone can run its own copy of a computer program without affecting others, we all have to follow the same law, at least in jurisdictions that recognize the rule of law.

So, I have the following answer to the question posed at the beginning of this article, which was: *Is it possible to organize the law (in the above sense) in the way the development of Free Software is organized?* It is possible to borrow from the organization of the development of Free Software and to introduce it both in the process of making the law, and in the process of adjudication. It will lead to making the law reflect more of the diverse interests existing in the society. If properly organized, it can lead to an increase of the quality of the law and its application. However, given the important differences between the law and Free Software, it is not possible to perform a simple copy of organization patterns. The idea calls for further research.

References

Botler 1984
D.J. Botler, *Turing's Man*, The University of North Carolina Press; 2nd ed. 1984.

Guibault et al. 2006
Lucie Guibault, Ot van Daalen, *Unraveling the Myth around Open Source Licenses. An Analysis from A Dutch and European Law Perspective* (TMC Asser Press 2006) 25 *et seq*.

Hardin 1968
Garrett Hardin, *The Tragedy of the Commons*, Science, Vol. 162, No. 3859 (December 13, 1968), pp. 1243-1248.

Wong & Kreps 2009
C. Wong, J. Kreps, *Collaborative Approach: Peer-to-Patent and the Open Source Movement*. International Free and Open Source Software Law Review (1, may. 2009).

DEEL II

INFORMATIERECHT

Informatievrijheid en digitalisering

Ontwikkelingen in jurisprudentie en regelgeving

Marga Groothuis■

Inleiding

Het internet biedt individuen en groepen vergaande mogelijkheden om hun vrijheid van meningsuiting uit te oefenen. Internet en andere digitale communicatiemiddelen zijn ook belangrijke instrumenten om het democratisch debat te bevorderen. Toegang tot internet betekent toegang tot een wereldwijd netwerk waarin politieke standpunten kunnen worden gepubliceerd en verspreid, maatschappelijke misstanden worden gesignaleerd en publiek debat kan worden gevoerd.

Tegelijkertijd worden samenlevingen in toenemende mate afhankelijk van digitale netwerken. Toegang tot internet is een voorwaarde geworden voor actieve maatschappelijke en politieke participatie. Reeds in 2003, tijdens de UN World Summit on the Information Society, werd het belang van internet als instrument voor de informatievrijheid onderstreept.[1] Twee jaar later stelde het Comité van Ministers van de Raad van Europa vast dat ICT ongeëvenaarde mogelijkheden biedt voor de uitoefening van de vrijheid van meningsuiting.[2] Tevens werd het principe aanvaard dat de vrijheid van meningsuiting zoals vastgelegd in artikel 10 van het Europees Verdrag voor de Rechten van de Mens niet mag worden beperkt op andere gronden dan die genoemd in het tweede lid van die verdragsbepaling, enkel omdat de communicatie plaatsvindt in digitale vorm.[3]

Ook in Nederland is er toenemende aandacht voor de rol van digitale communicatiemiddelen binnen de rechtsstaat. De regering heeft medio 2009 de Staatscommissie Grondwet, in het kader van een herziening van de Grondwet, gevraagd te adviseren over grondrechten in het digitale tijdperk.[4]

■ Marga Groothuis is universitair docent bij het Instituut voor Publiekrecht van de Universiteit Leiden. Zij is tevens verbonden aan eLaw@Leiden, centrum voor recht in de informatiemaatschappij.

1 *Geneva Declaration of Principles*, UN World Summit on the Information Society 10-12 December 2003, WSIS-03/GENEVA/DOC/4-E, http://www.itu.int/wsis/index.html.

2 *Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society*, CM(2005)56 final 13 May 2005, www.coe.int.

3 Artikel 1 van de *Declaration*.

4 Reeds in 2000 heeft de Commissie Grondrechten in het digitale tijdperk (Commissie Franken) het kabinet geadviseerd om de artikelen 7, 10 en 13 Grondwet te wijzigen in verband met de ontwikkelingen op het gebied van de informatie- en communicatietechnologie. Zie over dit advies paragraaf 2 van deze bijdrage.

Ook zijn recent Kamervragen gesteld over toegang tot internet als mensenrecht en de wenselijkheid van regelgeving om mondiale vrijheid van toegang tot het internet te garanderen.[5]

In dit hoofdstuk staat de digitale vrijheid van meningsuiting in Nederland en Europa centraal. Dit thema wordt belicht aan de hand van de volgende drie vragen:

i) Welke met ICT samenhangende ontwikkelingen zijn te onderscheiden in recente wetgevingsinitiatieven en jurisprudentie inzake de vrijheid van meningsuiting in Nederland?

ii) Hoe kunnen deze ontwikkelingen worden geplaatst in een breder internationaal- en Europeesrechtelijk kader?

iii) Welke vraagstukken en concepten kunnen naar verwachting relevant zijn voor een juridisch debat over de vrijheid van meningsuiting en digitalisering in de komende jaren?

De opzet van deze bijdrage is als volgt. Paragraaf 2 belicht de opdracht aan de Staatscommissie Grondwet en plaatst deze in een rechtsvergelijkend perspectief. Vervolgens worden in paragraaf 3 enkele recente ontwikkelingen in de Nederlandse jurisprudentie inzake informatievrijheid en ICT geanalyseerd, waaronder het in de belangenafweging toekennen van gewicht aan 'context', 'impact' en 'de mate van openheid' van een digitaal forum. In paragraaf 4 wordt onderzocht welke concepten centraal staan in de jurisprudentie van het Europese Hof voor de Rechten van de Mens inzake artikel 10 EVRM in een digitale omgeving. In paragraaf 5 ten slotte komt de vraag aan de orde welke vraagstukken en concepten naar verwachting relevant zullen zijn voor een Nederlands en Europees debat over de vrijheid van meningsuiting en digitalisering in de komende jaren.

De opdracht aan de Staatscommissie bezien in rechtsvergelijkend perspectief

Op 8 juli 2009 heeft de regering de *Staatscommissie Grondwet* ingesteld.[6] In de opdrachtverlening verzoekt de regering de Commissie onder meer om te adviseren over "de noodzaak tot wijziging van de Grondwet in verband met

5 Vragen van het Kamerlid Peters (GroenLinks) aan de ministers van Buitenlandse Zaken en van Justitie en de staatssecretaris van Economische Zaken over wetgeving om mondiale vrijheid van toegang tot het internet te garanderen (ingezonden 2 juli 2009), met de daarop door de regering gegeven antwoorden, *Kamerstukken II* 2008-09, Aanhangsel, No. 2652.

6 Besluit van 8 juli 2009 houdende instelling van een staatscommissie voor de herziening van de Grondwet (Instellingsbesluit staatscommissie Grondwet), Staatscourant 9 juli 2009, nr. 10354.

de grondrechten in het digitale tijdperk." Het advies van de Staatscommissie wordt medio 2010 verwacht.[7] In haar toespraak bij de installatie van de Staatscommissie zei minister Ter Horst van Binnenlandse Zaken dat "sommige grondrechten door technologische ontwikkelingen verouderd lijken te raken."[8] Zij noemde daarbij in het bijzonder de artikelen 7 (vrijheid van drukpers) en 13 (brief-, telefoon- en telegraafgeheim) en merkte op dat de *Commissie Grondrechten in het Digitale Tijdperk* zich al eerder over dit onderwerp had gebogen.

Reeds in 1999 heeft die Commissie de regering geadviseerd om artikel 7 Gw te wijzigen "in verband met de ontwikkelingen op het gebied van de informatie- en communicatietechnologie".[9] De Commissie benadrukte in zijn advies het belang van een techniek-neutrale formulering van grondrechten. Ten aanzien van art. 7 stelde zij onder meer: "Essentieel voor het nieuwe artikel is dat voor het uiten van een mening via bijvoorbeeld internet, omroep of films eenzelfde grondwettelijk regime geldt als voor het uiten van een mening via een boek of een krant."[10] Een voorstel tot wijziging van artikel 7 Gw dat conform het advies van de Commissie in techniek-neutrale termen was opgesteld, werd na een kritisch advies van de Raad van State niet ingediend bij de Tweede Kamer.[11] In 2005 heeft de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Tweede Kamer bericht dat, in verband met de technologische ontwikkelingen, een nieuw voorstel tot wijziging van artikel 7 Gw zou worden voorbereid, waarbij recente internationaalrechtelijke ontwikkelingen zouden worden betrokken.[12]

De minister voor Bestuurlijke Vernieuwing wees in dit kader op de *Declaration on Human Rights and the Rule of Law in the Information Society* van het Comité van Ministers van de Raad van Europa van 13 mei 2005.[13] Hierin heeft het Comité van Ministers een aantal richtsnoeren geformuleerd voor de toepassing van mensenrechten in een digitale omgeving. Het doel is richting te geven aan de rechtsontwikkeling inzake de toepassing van mensenrechten in de informatiesamenleving in de lidstaten van de Raad van Europa.

Uitgangspunt in deze Verklaring is dat ICT-toepassingen, zoals het world wide web en e-mail, de drijvende kracht vormen achter de opbouw van de Europese en wereldwijde informatiesamenleving. Zij zijn onmisbare instrumenten geworden in democratische processen en bieden een breed

---

7 In het instellingsbesluit wordt de Staatscommissie verzocht het advies uit te brengen voor 1 oktober 2010.

8 Toespraak minister Ter Horst te Den Haag, 9 juli 2009, gepubliceerd op www.minbzk.nl.

9 Advies 'Grondrechten in het digitale tijdperk', *Kamerstukken II* 2000-01, 27 460 nr. 1, bijlage I.

10 P. 225 van het advies van de Commissie.

11 Zie voor dit wetsvoorstel, het advies van de Raad van State en het nader rapport van de regering: http://www.minbzk.nl/grondwet_en/grondwet/parlementaire/brieven_aan_.

12 Brief van 28 november 2005, *Kamerstukken II* 2005-06, 30 300 VII, nr. 35.

13 Declaration CM(2005)56 final, gepubliceerd op www.coe.int.

scala aan mogelijkheden bij de uitoefening van mensenrechten, in het bijzonder de vrijheid van meningsuiting en de vrijheid van vereniging en vergadering. Geen toegang, of een beperkte toegang, tot deze digitale communicatiemiddelen zal individuen beperken in hun mogelijkheden om hun informatievrijheden uit te oefenen, aldus de Verklaring. Vastgesteld wordt dat ICT-toepassingen niet alleen kansen kunnen bieden, maar ook bedreigingen kunnen vormen voor de uitoefening van de vrijheidsrechten, in het bijzonder door de nieuwe technische mogelijkheden voor staten en andere actoren om informatiestromen te monitoren en te censureren.[14] Een kernbepaling is opgenomen in artikel 1 van de Verklaring:

"Freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the ECHR, simply because communication is carried in digital form."

De Verklaring roept de Lidstaten van de Raad van Europa op om hun (nationale) mensenrechteninstrumenten te herzien en zo nodig aan te passen teneinde mensenrechten te kunnen blijven beschermen in een snel ontwikkelende informatiesamenleving.

In de rechtsvergelijkende studie 'Constitutional Rights and New Technologies', uitgevoerd door de Universiteit Tilburg[15] is in kaart gebracht welke ontwikkelingen hebben plaatsgevonden in Frankrijk, Duitsland, België, Nederland, Zweden, Canada en de Verenigde Staten ten aanzien van grondrechten en nieuwe technologieën in de periode 2000-2007. Voorts is onderzocht welke aanbevelingen voor (grond)wetgevers uit de gevonden ontwikkelingen kunnen worden gedestilleerd.

Op basis van deze studie concluderen de onderzoekers dat in het onderzochte tijdvak in geen van de onderzochte landen vergaande grondwettelijke veranderingen hebben plaatsgevonden in reactie op technologische ontwikkelingen. Zij geven een tweeledige, mijns inziens overtuigende verklaring voor deze bevinding. In de eerste plaats zijn constituties vrijwel steeds rigide van aard: de procedure voor grondwetswijziging is zodanig zwaar dat constituties niet snel of eenvoudig kunnen worden geamendeerd. Dit geldt in het bijzonder voor federale stelsels zoals de Verenigde Staten, Duitsland en België, met een delicaat machtsevenwicht tussen de centrale overheid en de deelstaten. Een tweede verklaring kan worden gevonden in het feit dat de grondrechten in alle onderzochte landen met uitzondering van Nederland, zijn geformuleerd in zodanig brede, techniek-neutrale termen dat nieuwe communicatietechnologieën onder de reikwijdte van de bestaande grondrechten kunnen worden gebracht.

---

14 In dit kader kan ook worden gewezen op de uitspraak EHRM van 1 juli 2008 in de zaak Liberty t. Verenigd Koninkrijk (grootschalig onderscheppen van telefoon- en e-mailverkeer.) *NJCM-Bulletin* 2009-1, pp. 42-53.

15 Leenes, Koops & De Hert 2007. Dit boek is een vervolg op de eerdere rechtsvergelijkende studie die in 1999-2000 werd uitgevoerd onder supervisie van A. Koekkoek: Koekkoek et al. 2000.

Ten aanzien van de vrijheid van meningsuiting wordt in dit rechtsvergelijkend rapport desalniettemin geconcludeerd dat als gevolg van de opkomst van internet verscheidene rechtsvragen zijn gerezen. Een centraal thema in dit verband is de rechtspositie van *bloggers.* Deze vervullen enerzijds een vergelijkbare functie in de democratie als journalisten van de gedrukte pers, door het verzamelen en verspreiden van informatie, het formuleren van standpunten en het uiten van ideeën en opinies, en aldus het leveren van bijdragen aan het publieke debat. Anderzijds kan worden gesteld dat 'iedereen' een blog kan beginnen en zichzelf aldus een journalist kan noemen. Als gevolg van dit spanningsveld is in elk van de onderzochte landen de vraag gerezen of bloggers dezelfde beschermde status als journalisten dienen te krijgen. Die vraag is onder meer actueel in het kader van het verschoningsrecht voor journalisten. In België is het criterium 'een ieder die via een medium informatie onder het publiek verspreidt' bepalend voor de vraag of de zaak onder de reikwijdte van de wet inzake het verschoningsrecht voor journalisten valt. In Canada wordt een brede definitie van journalistiek gehanteerd, ook ten aanzien van nieuwe media. In Zweden wordt, in lijn met jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) inzake de vrijheid van meningsuiting van journalisten, een meer materieelrechtelijk criterium gehanteerd, namelijk de mate waarin de informatie 'een bijdrage levert aan het publieke debat', hetgeen rechters in staat stelt uitingen van bloggers te beoordelen in het licht van de omstandigheden van het individuele geval.[16]

Op basis van deze rechtsvergelijkende studie, bezien in het licht van de uitgangspunten van de bovengenoemde *Declaration on Human Rights and the Rule of Law in the Information Society* van de Raad van Europa, kan worden geconcludeerd dat de grondrechten in de huidige Nederlandse Grondwet, vergeleken met de constituties van de andere onderzochte landen, sterk techniekgekleurd zijn geformuleerd. De vraag rijst in hoeverre dat tot knelpunten leidt bij de toepassing van de grondwetsartikelen, en in het bijzonder artikel 7 Gw, in de rechtspraktijk. Die vraag staat centraal in de nu volgende paragraaf.

Ontwikkelingen in de Nederlandse jurisprudentie

Medio jaren negentig, toen het gebruik van internet in opkomst was, was er onder juristen discussie over de vraag of artikel 7 Grondwet van toepassing

16 In Nederland is in 2008, kort na de afsluiting van de rechtsvergelijkende studie, een voorontwerp voor Wijziging van het Wetboek van Strafvordering tot vastlegging van het recht op bronbescherming bij vrije nieuwsgaring (Wet bronbescherming in strafzaken) gepubliceerd (voorontwerp van 29 oktober 2008, te downloaden op www.jusitie.nl). Dit voorontwerp, dat bij de afsluiting van deze bijdrage (november 2009) nog niet was ingediend bij de Tweede Kamer, biedt mijns inziens geen helder beoordelingskader voor de rechtspositie van bloggers, omdat de voorgestelde wettekst geen materieelrechtelijk criterium bevat om te beoordelen of een persoon onder de reikwijdte van de voorgestelde wet valt.

was op uitingen op internet, en zo ja, welk lid van dat artikel dan van toepassing was.[17] Thans, vijftien jaar later, is er geen twijfel meer over de vraag òf de vrijheid van meningsuiting van toepassing is op internet: die vraag wordt in de jurisprudentie zonder meer bevestigend beantwoord. Welk lid van artikel 7 Grondwet van toepassing is (lid 1 inzake drukpers, lid 2 inzake radio en televisie of lid 3 inzake 'andere middelen') wordt in gerechtelijke uitspraken vrijwel steeds in het midden gelaten: in rechtsoverwegingen inzake artikel 7 Grondwet wordt het artikellid eenvoudigweg niet nader gespecificeerd.[18] Daarnaast is er een tendens in de rechtspraktijk om een beroep op de vrijheid van meningsuiting te beoordelen op basis artikel 10 EVRM en niet (ook) op artikel 7 Grondwet.[19] Een eerste mogelijke verklaring is het ontbreken van een proportionaliteitstoets in artikel 7 Grondwet (en in de andere in hoofdstuk 1 van de Grondwet opgenomen grondrechtsbepalingen), terwijl die toets in de jurisprudentie van het Europese Hof voor de Rechten van de Mens inzake art. 10 EVRM een centrale rol speelt.[20] Een tweede mogelijke verklaring is de techniek-afhankelijke formulering van artikel 7 Gw en de daaruit voortvloeiende rechtsonzekerheid betreffende de toepassing op internet.[21]

Drie elementen hebben in recente jurisprudentie over de vrijheid van meningsuiting op internet (2008-2009) relatief veel aandacht gekregen, namelijk het in het kader van de proportionaliteitstoets van art. 10 EVRM toekennen van gewicht aan *context*, *impact* en de *mate van openheid* van een digitaal forum. In het onderstaande worden deze aspecten belicht.

Casus 1
Een 31-jarige vrouw uit Drenthe had haar ex-partner, en vader van haar vijfjarig zoontje, op haar Hyves-pagina aangeduid als pedofiel. Deze Hyves-

17 Zie in dit verband onder meer de regeringsnota *Wetgeving voor de elektronische snelweg (*1998), *Kamerstukken II* 1997-98, 25 880, nrs. 1-2; Commissie Grondrechten in het Digitale Tijdperk 1999; Studiecommissie VMC 1999, Asscher 1999; Dommering 2000; Schmidt & Wiarda 2000.

18 Zie hierover ook: Koops & Groothuis 2000.

19 Veelzeggend in dit verband is de rechtsoverweging van het Gerechtshof Amsterdam in de beschikking van 21 januari 2009 inzake vervolging van het Tweede Kamer Lid Wilders (art. 12 Sv). Het Hof overwoog "dat de uitleg die door het EHRM aan artikel 10 EVRM is gegeven, de bescherming van de vrije meningsuiting op basis van artikel 7 Gw heeft overvleugeld." Hier staat tegenover dat Artikel 7 van de Nederlandse Grondwet in een aantal opzichten meer bescherming biedt dan artikel 10 EVRM. Het vereiste in het eerste en derde lid dat inhoudelijke beperkingen slechts bij wet in formele zin gesteld mogen worden, is daarvan een voorbeeld.

20 Zie uitgebreid over het ontbreken van een proportionaliteitstoets in het huidige art. 7 Gw en de wenselijkheid van een grondwetswijziging op dit punt: Studiecommissie VMC, 'Preadvies inzake een nieuwe tekst voor de artikelen 7 en 13 van de Grondwet', supra noot 18.

21 Dit punt kwam naar voren in de interviews met rechters en advocaten in het kader van het door de Universiteit Leiden uitgevoerde grondwetsevaluatie-onderzoek 2009: Barkhuysen & Dimitrova 2009.

pagina had een zogeheten 'persoonlijk profiel': de inhoud ervan was alleen zichtbaar voor Hyves-gebruikers die zij had toegevoegd als 'vriend'. Nadat de vrouw over haar ex-partner had geschreven "Ik moet mijn kind meegeven aan een pedo", deed deze aangifte bij de politie. Op 3 augustus 2008 werd de vrouw door de politierechter van de Rechtbank Assen veroordeeld wegens smaad. Zij kreeg een voorwaardelijke werkstraf van 40 uur opgelegd.[22]

De advocaat van de verdachte had betoogd dat de uitspraak niet in het openbaar was gedaan en daarom geen sprake was van smaad. Hij vergeleek het afgeschermde Hyves-profiel met een huiskamer waarin je tegen vrienden mag zeggen wat je wilt. De rechtbank oordeelde anders: omdat iedereen die als vriend was toegevoegd de uitlatingen op de pagina kon lezen, achtte de rechtbank het Hyves-profiel wèl openbaar.

Op 3 november 2009 heeft het Gerechtshof Leeuwarden uitspraak gedaan in hoger beroep.[23] Naar het oordeel van het hof kan de wijze waarop – en de aard van de bewoordingen waarin – verdachte haar gedachten via haar Hyves-pagina met een twintigtal anderen heeft gedeeld niet anders worden opgevat dan het welbewust en derhalve opzettelijk ruchtbaarheid geven aan die uitlatingen. Het Hof overweegt:

> "Het betrof immers niet een beperkt aantal geadresseerden die – zoals de raadsman de vergelijking maakt – in de beslotenheid van de huiskamer vertrouwelijke informatie krijgt toevertrouwd. In het onderhavige geval gaat het om een in potentie ruimere kring van personen, die kennelijk naar eigen inzicht en zonder enige restrictie over de uitlatingen mocht beschikken, waarbij daarnaast een verdere verspreiding van de gewraakte tekst door de oorspronkelijk geadresseerden – gezien de aard van de beschuldiging – voor de verdachte niet alleen in theorie voorzienbaar was maar ook op voorhand feitelijk te verwachten viel."

Het Hof veroordeelt de verdachte tot een voorwaardelijke werkstraf van 40 uur wegens smaad op de Hyves-pagina.

Casus 2

Op de Nederlandse website www.stopkindersex.com staat een weblink naar de Amerikaanse websites www.dutchpedophilesexposed.org en www.dutchpredators.org, waar veroordeelde pedoseksuelen met naam en toenaam en foto staan vermeld. Eiser in deze zaak is wegens ontucht met minderjarigen in 2007 door het Gerechtshof Arnhem strafrechtelijk veroordeeld. Hij eist voor de Voorzieningenrechter van de Rechtbank Rotterdam, op straffe van een dwangsom, dat gedaagde zijn persoonsgegevens en foto' | 's binnen twee dagen verwijdert van www.stopkindersex.com, www.dutchpedophilesexposed.org, www.dutchpredators.org dan wel elke andere website waarop

---

22 Deze samenvatting is gebaseerd op een artikel in *De Volkskrant* van 6 augustus 2008: Sjoukje Budde en Jochem Lybaart, 'Hyves is geen huismaker, zegt rechter'. De uitspraak, waarin alleen zijn opgenomen de personalia van veroordeelde, de pleegdatum, de toegepaste wetsartikelen en de beslissing, is niet gepubliceerd maar opgevraagd door de redactie van *Computerrecht*.

23 Dit arrest gepubliceerd op www.rechtspraak.nl, *LJN* BK1897.

gedaagde enige invloed heeft. Gedaagde voert aan dat zij niet verbonden is aan de beide Amerikaanse websites en derhalve niet verantwoordelijk is voor de inhoud ervan. Ook voert zij aan dat zij de Nederlandse site www.stopkindersex.com voor 1 euro heeft verkocht en sindsdien ook aan die site op geen enkele wijze meer is verbonden.

De Voorzieningenrechter[24] oordeelt dat, hoewel gedaagde heeft verklaard dat zij de Nederlandse site heeft verkocht, voldoende aannemelijk is dat het nog steeds in de macht van gedaagde ligt gegevens op deze site te plaatsen of te verwijderen. Door op de website www.stopkindersex.com een link te plaatsen naar sites waar de persoonsgegevens van eiser staan vermeld, handelt gedaagde naar het oordeel van de Voorzieningenrechter in strijd met de Wet bescherming persoonsgegevens (Wbp). Vervolgens onderzoekt de Voorzieningenrechter of het onrechtmatige karakter aan het plaatsen van voornoemde link kan worden ontnomen omdat het recht op vrijheid van meningsuiting mogelijk zwaarder weegt dan het recht op een persoonlijke levenssfeer. Naar het oordeel van de voorzieningenrechter weegt het recht op vrijheid van meningsuiting in casu niet zwaarder dan het recht op een persoonlijke levenssfeer. In beginsel geldt dat gedaagde haar mening vrijelijk moet kunnen uiten. In een rechtsorde is het echter de kunst binnen de grenzen van het toelaatbare te blijven. Zo wordt eenieder geacht onschuldig te zijn, tot zijn schuld wordt bewezen en is iemand die zijn straf heeft uitgezeten weer een vrij man met alle (grond)rechten van dien. Gedaagde gaat daaraan naar het oordeel van de Voorzieningenrechter voorbij. Gebleken is dat het op internet vermelden van persoonsgegevens van personen die zich strafrechtelijk hebben moeten verantwoorden, eigenrichting in de hand werkt, aldus de Voorzieningenrechter. Die omstandigheden maken dat het recht op vrijheid van meningsuiting in casu niet prevaleert boven het recht op een persoonlijke levenssfeer.

Casus 3

Verdachte in deze zaak heeft zich, onder het pseudoniem Joshadam, op het internetforum www.Polinco.net meermalen beledigend uitgelaten over homoseksuelen, negroïde personen, allochtone vrouwen en Joodse mensen. Daartoe heeft verdachte woorden gebruikt als 'kruipende dieren', 'ratten' en 'schorem'. De verdachte heeft ter zitting aangevoerd dat op het internetforum Polinco een eigen jargon werd gehanteerd en dat hij de gewraakte bewoordingen heeft gebruikt omdat hij dat spannend en ludiek vond. Hij heeft gesteld dat op dit forum geschreven kon worden wat men normaal niet mag of durft te uiten.

De Rechtbank Amsterdam oordeelt op 2 juni 2008[25] dat de teksten een onmiskenbaar homofoob, racistisch, islamofoob en antisemitisch karakter hebben. Belediging van groepen is strafbaar gesteld in artikel 137c Sr. In dit

24 Voorzieningenrechter Rotterdam 24 maart 2009, *LJN* BH7631.
25 *LJN* BD2977.

geval is derhalve voldaan aan het in het tweede lid van artikel 10 EVRM gestelde vereiste dat de (mogelijke) beperking is voorzien bij wet. Ook dient een strafrechtelijke veroordeling een van de in artikel 10 lid 2 EVRM genoemde doelen: de bescherming van de rechten van anderen. Ten aanzien van de vraag of de inbreuk op de vrijheid noodzakelijk is in de democratische samenleving (de proportionaliteitstoets) oordeelt de Rechtbank als volgt. Niet is gebleken dat het internetforum Polinco op actieve wijze de openbaarheid nastreeft. Het forum wordt niet aan mensen via de mail, gemaskeerde links of pop-ups aan internetgebruikers opgedrongen. Ook komt men niet zomaar op het forum terecht. Aannemelijk is "dat verdachte juist door de keuze voor deze website in de veronderstelling verkeerde – en ook de bedoeling had – dat zijn uitlatingen slechts door een klein groepje gelijkgestemden zouden worden gelezen." Zijn opzet was derhalve gericht op een beperkte mate van openbaarheid. Hierin bestaat volgens de Rechtbank een duidelijk verschil met media als televisie of radio, waarbij de kijker en/of luisteraar in veel mindere mate in de hand heeft welke informatie op hem wordt afgestuurd. Nu verdachte een semi-openbare internetsite als forum heeft gekozen, is de rechtbank er niet van overtuigd dat verdachte het opzet had de uitlatingen in volledige openbaarheid te doen. Op deze grond spreekt de Rechtbank verdachte vrij van het telastegelegde.

Het Gerechtshof Amsterdam vernietigt bij arrest van 23 november 2009 in hoger beroep het vonnis van de Rechtbank Amsterdam. Ten aanzien van verdachtes opzet bij de openbaarheid verwijst het Hof naar zijn eerdere arrest van 20 juni 2008 waarin het bepaalde dat "door gebruik te maken van internet welbewust wordt gekozen voor een medium met een groot potentieel publieksbereik".[26] Daaraan doet in het onderhavige geval naar het oordeel van het Hof niet af dat internetgebruikers de Polincowebsite moesten 'aanklikken' en aldus niet ongevraagd met verdachtes uitlatingen in aanraking kwamen. Toegang tot de feitelijke inhoud van de website, in casu de gewraakte teksten, was vrij en werd niet met een wachtwoord beschermd. Bovendien blijkt uit zich in het dossier bevindende teksten dat de verdachte op de Polincowebsite meermalen heeft gewezen op de openbaarheid daarvan. Verdachtes opzet staat derhalve naar het oordeel van het Hof vast. Het Hof veroordeelt verdachte tot een voorwaardelijke boete van 900 euro boete.

Met de bespreking van deze drie casus, die zijn geselecteerd uit een verzameling van 20 uitspraken van Nederlands rechtbanken en gerechtshoven (civiele kamers en strafkamers) betreffende de vrijheid van meningsuiting op internet in het tijdvak 2008-2009, beoog ik te illustreren dat rechters, in het kader van de proportionaliteitstoets van art. 10 EVRM en in het kader van strafrechtelijke en civielrechtelijke normen van Nederlands recht, gewicht toekennen aan *context*, *impact* en de *mate van openheid* van een digitaal forum. Elke zaak is uniek, en de bijzondere omstandigheden zijn bepalend voor het rechterlijk oordeel. Maar bij een vergelijkende analyse van de onderzochte

26 *LJN* BD7024.

uitspraken valt op dat rechters in het tijdvak 2008-2009 nog verschillende criteria hanteren om te bepalen of een digitaal forum open dan wel gesloten is, en in welke mate. Ook hanteren zij verschillende criteria om te bepalen wat, gelet op de aard van het forum en de aard van de uiting, de te verwachten impact van een uiting is. In de onderzochte uitspraken is bovendien niet altijd expliciet gemaakt welke criteria en methoden zijn gehanteerd om de betreffende rechtsvragen te beantwoorden. Uit de onderzochte uitspraken in onderlinge samenhang bezien komt het beeld naar voren van rechters die nog enigszins zoekende waren over de vraag hoe zij uitingen op internet, gelet op de kenmerken van dit medium en de specifieke toepassing daarvan, dienen te interpreteren in het kader van art. 10 EVRM.

In paragraaf 4 wordt onderzocht welke richtsnoeren de jurisprudentie van het Europese Hof voor de Rechten van de Mens op dit punt biedt.

Europeesrechtelijke ontwikkelingen

De volgende twee casus, geselecteerd uit een achttal uitspraken van het EHRM inzake vrijheid van meningsuiting op internet in het tijdvak 2006-2009, bevatten aanwijzingen voor de criteria die het EHRM hanteert bij de proportionaliteitstoets bij uitingen op internet.

Casus 1
Stephane Perrin, een Fransman met woonplaats in het Verenigd Koninkrijk, is door de Britse autoriteiten gearresteerd wegens het plaatsen van drie webpagina's met pornografische inhoud op internet. De webpagina's waren op internet aangetroffen door een officier van de Metropolitan Police. De eerste webpagina was een 'preview' voor de tweede en derde webpagina, die konden worden bekeken na betaling van een som geld per credit card. Perrin bekende tijdens zijn verhoor door de politie dat hij verantwoordelijk was voor de webpublicaties maar stelde dat de betreffende internetsite werd beheerd door een in de Verenigde Staten gevestigd bedrijf dat voldeed aan alle lokale wetten en waarvan hij een meerderheid van de aandelen bezat. Wegens het publiceren van de eerste webpagina (de 'preview page') werd Perrin op grond van de Obscene Publications Act veroordeeld tot 30 maanden detentie. In hoger beroep bij het Court of Appeal werden de veroordeling en straf bevestigd. Vervolgens diende Perrin een klacht in bij het EHRM, stellende dat zijn recht op vrije meningsuiting was geschonden.

Het Hof oordeelt in zijn uitspraak van 18 oktober 2005[27] dat het feit dat de verspreiding van de afbeeldingen in kwestie in andere staten mogelijk legaal zou zijn, nog niet betekent dat het verbieden van een zodanige verspreiding binnen het eigen grondgebied de beoordelingsmarge van het Verenigd Koninkrijk te buiten gaat. Het feit dat de Obscene Publications Act

27 EHRM 18 oktober 2005, Perrin t. Verenigd Koninkrijk, appl. no. 5446.03, *European Human Rights Cases* 2006-2, pp. 112-119.

mogelijk slechts beperkte bescherming aan kwetsbare personen zou bieden is volgens het Hof geen reden voor de verantwoordelijke regering om niet te pogen om hen te beschermen. Het feit dat er mogelijk andere middelen zijn om te beschermen tegen schade maakt het naar het oordeel van het Hof niet disproportioneel om strafrechtelijk te vervolgen, vooral wanneer niet is aangetoond dat andere middelen effectiever zijn. Over Perrins argument, ten slotte, dat websites als deze zelden per ongeluk worden bezocht, overweegt het Hof dat de webpage waarvoor Perrin is veroordeeld vrij te bezoeken was voor een ieder die op internet surfde. Het Hof wijst er ook op dat het betreffende materiaal juist het soort materiaal is dat jonge mensen, die de nationale autoriteiten proberen te beschermen, zouden willen vinden. Het Hof overweegt verder dat het voor de klager mogelijk was geweest om de schade, en daardoor de veroordeling, te vermijden, met voorzetting van zijn 'business', door ervoor te zorgen dat geen van de foto's beschikbaar was op de preview-webpage. Op basis van deze overwegingen verklaart het Hof de klacht van Perrin kennelijk ongegrond (art. 35, derde lid EVRM).

Casus 2

De Engelse krant Times Newspapers Ltd is aangeklaagd en tot in hoogste instantie veroordeeld voor smaad wegens voortdurende publicatie van twee artikelen in zijn digitale archief op internet.[28] De Court of Appeal had geoordeeld dat hiervoor de *internet publication rule* gold: er is een termijn voor het instellen van een actie wegens smaad en voor internetpublicaties start deze termijn elke keer wanneer een artikel in het digitale archief wordt opgevraagd. In de motivering bij dit oordeel was aangegeven dat iedere opvraging van een artikel in het internetarchief door een internetgebruiker werd gekwalificeerd als een nieuwe publicatie. De Times klaagt bij het EHRM op grond van art. 10 EVRM: volgens de krant had deze *internet publication rule* een 'chilling effect' op de vrijheid van meningsuiting.

Het Hof stelt in zijn uitspraak van 10 maart 2009[29] voorop dat internetarchieven een substantiële bijdrage leveren aan het bewaren en beschikbaar stellen van nieuws en informatie. De internetarchieven vallen derhalve onder de reikwijdte van art. 10 EHRM. Het Hof overweegt dat de termijn voor het instellen van acties wegens smaad is bedoeld om kranten te beschermen tegen oude aanklachten. De lengte van die termijn valt binnen de 'margin of appreciation' van de lidstaat. Het Hof geeft aan dat de 'margin of appreciation' voor de staten groter is wanneer het gaat om internetarchieven voor *oude* nieuwsberichten, omdat er dan geen urgentie meer is om door middel van publicatie te rapporteren over publieke misstanden. In casu had de Engelse rechter The Times gelast om bij de twee in geding zijnde krantenartikelen gedurende de gerechtelijke procedure een bericht te plaatsen dat deze artikelen nog waren onderworpen aan een rechterlijk oordeel inzake smaad.

---

28 Zie voor een uitgebreide beschrijving van de feiten *Mediaforum* 2009/03, p. 89.

29 EHRM 10 maart 2009, Times Newspapers. v. Verenigd Koninkrijk, appl. 3002/03 en 23676/03.

Het Hof oordeelt dat een zodanige kennisgeving in casu geen onevenredige inbreuk opleverde met de vrijheid van meningsuiting en dat derhalve geen sprake was van strijd met art. 10 EVRM.

Afsluiting

Op grond van het vorenstaande kan worden geconcludeerd dat het EHRM in het kader van de proportionaliteitstoets bij artikel 10 EVRM gewicht toekent aan de context waarin een digitale uiting wordt voldaan. Tevens blijkt dat het Hof het internet ziet als een open terrein waarin een ieder 'al surfend' informatie en opinies kan tegenkomen. Voorts kan worden geconcludeerd dat het Hof in de twee besproken uitspraken een ruime beoordelingsmarge aan de lidstaat heeft gegeven voor de interpretatie van de in geding zijnde rechtsregels in een digitale omgeving. In beide zaken betrof de uiting *niet* het aan de kaak stellen van een actuele misstand. Het nadrukkelijke onderscheid dat het Hof in zijn uitspraak in de zaak *The Times v. Verenigd Koninkrijk* maakt tussen internetarchieven met 'oud nieuws' en publicaties waarin actuele publieke misstanden aan de kaak worden gesteld, is mijns inziens een indicatie dat het Hof in toekomstige zaken waarin op internet een actuele publieke misstand wordt geopenbaard, een kleinere margin of appreciation aan de lidstaten zal laten.

De vrijheid van meningsuiting staat thans, eind 2009, hoog op de Nederlandse politieke agenda: het heftige maatschappelijke debat naar aanleiding van de beslissing van het Gerechtshof Amsterdam om het Tweede Kamerlid Geert Wilders te vervolgen wegens het aanzetten tot haat en discriminatie op grond van door hem gedane uitlatingen in diverse media over moslims en hun geloof, is hiervan een voorbeeld. Het Gerechtshof overwoog in die uitspraak onder meer dat "de uitleg die door het EHRM aan artikel 10 EVRM is gegeven, de bescherming van de vrije meningsuiting op basis van artikel 7 Gw heeft overvleugeld".[30] Mijns inziens is die overweging een juiste analyse en een signaal dat gehoord zou moeten worden. In deze bijdrage heb ik getracht aan te tonen dat artikel 7 Grondwet, door zijn techniek-afhankelijke en daarmee verouderde formulering, alsmede door het ontbreken van een proportionaliteitstoets, in de verdrukking dreigt te komen: het wordt verdrongen door art. 10 EVRM dat wèl duidelijk toepasbaar is in een digitale omgeving en een proportionaliteitstoets biedt. Het toetsingsverbod van art. 120 Grondwet, naast de doorwerking van een ieder verbindende verdragsbepalingen (waaronder art. 10 EVRM) in de nationale rechtsorde, versterkt de tendens tot 'overvleugeld worden' van artikel 7 Grondwet.

De opdracht van de regering aan de Staatscommissie Grondwet om te adviseren over 'grondrechten in het digitale tijdperk' biedt mijns inziens een nieuwe kans om een wijziging van artikel 7 Grondwet te initiëren. Reeds in

30 Gerechtshof 21 januari 2009, *LJN* BH0496.

2000 schreef A.H.J. Schmidt, in een publicatie voor *RM Themis*[31] tezamen met G. Wiarda, dat het hierbij niet gaat om normering van zich wijzigende techniek. Het gaat om gedrag van natuurlijke personen en rechtspersonen, ook onder ten gevolge van nieuwe technologieën gewijzigde omstandigheden. Het is de kunst om communicatiehandelingen zodanig te omschrijven dat de gebruikte formuleringen ook bij nieuwe communicatietechnieken voldoende aanknopingspunten blijven verschaffen voor het normeren daarvan. Die woorden zijn thans, tien jaar later, actueler dan ooit tevoren.

Verwijzingen

Asscher 1999
L. Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie*, ITeR-reeks deel 26, 1999.

Barkhuysen & Dimitrova
T. Barkhuysen en A.L. Dimitrova *et al.*, *De Nederlandse Grondwet geëvalueerd; anker- of verdwijnpunt?*, Alphen aan den Rijn: Kluwer 2009.

Commissie Grondrechten in het Digitale Tijdperk 1999
Commissie Grondrechten in het Digitale Tijdperk, advies *Grondrechten in het digitale tijdperk,* Den Haag 1999.

Dommering 2000
E.J. Dommering, 'De nieuwe Nederlandse Constitutie en de informatietechnologie', *Computerrecht* 2000, nr. 4., blz. 179 – 180

Koekkoek 2000
A. Koekkoek et al., *Protection of Human Rights in the Digital Age. A Compararive Study of the freedom of Information and Communication and Privacy in Sweden, Germany, France, Belgium, The United States of America and Canada*, Tilburg: Tilburg University 2000.

Koops en Groothuis 2000
E.J. Koops en M.M. Groothuis, 'Constitutional Rights and Technologies in the Netherlands', in: Leenes, Koops & De Hert 2000, p. 182.

Leenes, Koops en De Hert 2000
R.E. Leenes, E.J. Koops en P. De Hert (red.), *Constitutional Rights and New Technologies. A Comparative Study* (Information Technologies and Law Series), The Hague: Asser Press 2007.

Schmidt & Wiarda 2000
A.H.J. Schmidt en G.C.Th. Wiarda, 'Communicatierechten in de Grondwet', *RM Themis* 2000/9, p. 323-334.

Studiecommissie VMC 2000
Studiecommissie VMC, 'Preadvies inzake een nieuwe tekst voor de artikelen 7 en 13 van de Grondwet', in *Mediaforum* 1999, nr. 11/12, blz. I-VIII.

31 Schmidt & Wiarda 2000.

Publieke media op internet: zorgplicht en concurrentievervalsing

Wouter Hins■

Inleiding

Op een deur van de afdeling eLaw@Leiden hangt een papier dat groot ontzag inboezemt. Het is een fotokopie van een wetenschappelijk artikel, waarvan de titel luidt: *Technologie komunikacyjno-informatyczne a sądownictwo w Holandii – aktualna sytuacja*. De publicatie is afkomstig uit de Monotor Prawniczy, zeg maar het Nederlands Juristenblad van Polen, aflevering 16 van het jaar 2006. De naam van de schrijver staat eronder*:* 'A. Schmidt, eLaw@Leiden, Centrum Prawa i Społeczeństwa Informacyjnego'. Het moge duidelijk zijn: Aernout Schmidt, ter ere van wie deze bundel verschijnt, heeft zijn vleugels tot ver in Oost-Europa uitgeslagen. Onderstaande bijdrage is mede geïnspireerd door de indrukwekkende Poolse titel. Mijn onderwerp heeft ook te maken met informatie- en communicatietechnologie, Europese ontwikkelingen en de 'aktualna sytuacja' in Nederland. Veiligheidshalve heb ik wel gekozen voor een onderwerp waarbij ik mij thuis voel, te weten het mediarecht. Dit vakgebied, dat zich bezighoudt met de openbare communicatie, kent als belangrijke beginselen de vrijheid van meningsuiting en het streven naar een eerlijke mededinging.

Een kort woord ter inleiding. Vroeger was het medialandschap scherp onderverdeeld in een publieke en een private sector. Aan de ene kant lag het gebied van de geschreven pers, waar het vrije ondernemerschap kon floreren. De overheid hield zich afzijdig, indachtig artikel 7, eerste lid, van de Grondwet: 'Niemand heeft voorafgaand verlof nodig om door de drukpers gedachten of gevoelens te openbaren (..)'. Aan de andere kant lag het gebied van de omroep, waarmee de overheid zich juist heel stevig bemoeide. Er was immers een schaarste aan frequenties en de invloed op de openbare meningsvorming van radio en televisie was groot. Illustratief is het uitgangspunt van artikel 7, tweede lid, van de Grondwet: 'De wet stelt regels omtrent radio en televisie (..)'. In 1989 – een maand voor het vallen van de Berlijnse muur – blijkt de Nederlandse wetgeving echter niet in staat commerciële televisie vanuit Luxemburg te weren. De voorloper van RTL4 doet zijn intrede.[1] Vanaf die tijd is het gebied van de omroep gesplitst. Het geheel van door

---

■ Wouter Hins is hoogleraar Mediarecht aan de Faculteit der Rechtsgeleerdheid in Leiden. Hij is daarnaast universitair docent staats- en bestuursrecht aan de Universiteit van Amsterdam.

1 Vzr. 29 september 1989, NOS e.a. vs CvdM, KG 1989, 393 en AB 1991, 371 m.nt. B.P. Vermeulen. De uitspraak werd bekend gemaakt op 4 oktober 1989.

de Staat gefinancierde en gereguleerde verenigingen en stichtingen wordt aangeduid als de 'publieke omroep'. Dit in tegenstelling tot de commerciële omroep, die bestaat uit private ondernemingen. Sedert een wetswijziging van 1991 hoeven zij niet meer via de achterdeur binnen te sluipen.[2] Zij kunnen zich gewoon in Nederland vestigen. Wat betreft de geschreven pers blijft de overheid afzijdig, afgezien van een beperkte steunregeling.

Op 1 januari 2009 is de Mediawet geheel herzien.[3] De wetgever overwoog 'dat het wenselijk is de taakopdracht van de publieke omroep te wijzigen in het licht van ontwikkelingen in technologie, media-aanbod, mediaproductie, distributie en mediagebruik' en heeft de publieke omroep ruim baan gegeven om nieuwe elektronische media te gebruiken. Eigenlijk mag men niet meer spreken van publieke omroepinstellingen. Het nieuwe woord luidt 'publieke media-instellingen'. De bedoeling is duidelijk. Er moet een publieke sector komen in de sfeer van digitale televisie, IPTV, mobiele televisie en 'video on demand'. Zou de publieke omroep zich moeten beperken tot zijn oorspronkelijke domein, dan dreigt hij te marginaliseren. Probleem is echter dat de geschreven pers ook in zijn oorspronkelijke domein bekneld is geraakt. Wil een krant overleven, dan zal ook zij haar vleugels moeten uitslaan naar het internet.[4] De vraag rijst dan of de aanwezigheid van door de overheid gesubsidieerde themakanalen en on-line-content moet worden beschouwd als concurrentievervalsing. Moet de publieke omroep terug in zijn hok of is een vruchtbare werkrelatie mogelijk?

Publieke mediadiensten

De expansie van de publieke omroep naar nieuwe platforms is een geleidelijk proces geweest. Een belangrijk moment was de vaststelling van de zogeheten Concessiewet van 23 maart 2000.[5] De wet introduceerde in artikel 13c van de vorige Mediawet een taakomschrijving voor de publieke omroep. Blijkens het eerste lid, onderdeel a, kreeg de publieke omroep onder meer tot taak: 'het op landelijk, regionaal en lokaal niveau verzorgen van een veelzijdig en kwalitatief hoogstaand aanbod van programma's voor algemene omroep op het gebied van informatie, cultuur, educatie en verstrooiing en deze uit te zenden of te doen uitzenden op open netten'. In het tweede lid van hetzelfde artikel stonden kwaliteitseisen die grotendeels overeenkomen

2 Wet van 18 december 1991, *Stb.* 769.

3 Wet van 29 december 2008, *Stb.* 583 (Mediawet 2008). De wet trad grotendeels in werking op 1 januari 2009 krachtens koninklijk besluit van 29 december 2008, *Stb.* 585. Inmiddels is die wet weer gewijzigd bij Wet van 2 juli 2009, *Stb.* 300, deels in werking getreden op 17 juli 2009 krachtens koninklijk besluit van 3 juli 2009, *Stb.* 301.

4 Zie het rapport 'De volgende editie' van de Tijdelijke Commissie Innovatie en Toekomst Pers (Commissie-Brinkman) d.d. 23 juni 2009, p. 34.

5 Wet van 23 maart 2000, *Stb.* 138 (Wet tot wijziging van de Mediawet in verband met de invoering van een vernieuwd concessiestelsel voor de landelijke publieke omroep).

met artikel 2.1 van de huidige Mediawet. Over nieuwe distributieplatforms bepaalde artikel 13c, derde lid: 'De publieke omroep kan mede invulling geven aan zijn taak, bedoeld in het eerste lid, door tevens te voorzien in andere dan de in het eerste lid, onderdeel a, bedoelde wijzen van aanbod en verspreiding van programmamateriaal.' De publieke omroep hoefde zich dus niet te beperken tot *open netten*. Andere wijzen van verspreiding, bijvoorbeeld themakanalen op de kabel of op internet, werden in de Kamerstukken aanduid als 'neventaken'. Zij hoorden weliswaar niet tot de hoofdtaak, maar mochten wel worden bekostigd uit de omroepmiddelen.

Om te bevorderen dat investeringen in neventaken doelmatig zouden worden gedaan voegde de Concessiewet van 2000 ook een nieuw artikel 55b aan de Mediawet toe. Het artikel bepaalde in de eerste plaats dat niet iedere omroepvereniging op eigen houtje een geprofileerd themakanaal mocht gaan opzetten. Dat zou afbreuk doen aan de samenhang van de publieke omroep als geheel en leiden tot geldverspilling. Als AVRO, EO, KRO en andere omroepen ieder apart gaan onderhandelen met kabelexploitanten om een themakanaal door te geven, vliegen de uitzendkosten de hoogte in. Vandaar dat een meldplicht werd voorgeschreven bij de Raad van Bestuur van NPO. Binnen twee maanden kon de Raad van Bestuur een veto uitspreken ter bescherming van het gemeenschappelijk belang van de landelijke omroep. Daarnaast stelde artikel 55b, tweede lid, enige grenzen aan het verrichten van neventaken. Door een verwijzing naar een ander artikel gold onder meer de eis dat de activiteit niet mocht leiden of kunnen leiden tot 'concurrentievervalsing ten opzichte van andere aanbieders van dezelfde of vergelijkbare goederen of diensten'.[6]

Er heeft een zich een kluwen van juridische procedures afgespeeld over de vraag of de publieke omroep nu wel of niet gerechtigd was speciale themakanalen op de kabel aan te bieden zoals Colorful Radio voor jongeren en de Concertzender voor liefhebbers van klassieke muziek.[7] Commerciële omroepen zoals Radio 538 en Classic FM meenden dat sprake was van ongeoorloofde staatssteun en concurrentievervalsing. Hier kan volstaan worden met de opmerking dat het omroepbeleid van de regering zeer kritisch gevolgd werd door de Europese Commissie. Nederland stond niet als enige in het verdachtenbankje. Op basis van artikel 88, tweede lid, van het EG-verdrag besloot de Europese Commissie diverse regeringen op te dragen verleende steun aan publieke omroepen terug te vorderen. Nederland kreeg daartoe een bevel op 22 juni 2006, al had dit bevel vooralsnog geen betrek-

6 Artikel 55b, tweede lid, verwees naar artikel 57a, eerste lid, van de Mediawet. Zie ook de Notitie neventaken publieke omroep 2002 van het Commissariaat voor de Media d.d. 4 december 2001, welke notitie gewijzigd werd op 8 april 2003, *Stcrt*. 86, p. 25.

7 Chavannes 2004; Kroes 2005, in het bijzonder p. 254; Robichon-Lindenkamp 2007.

king op de financiering van neventaken.[8] De wetenschap dat er een EG-rechtelijk probleem dreigde was voor de regering wel aanleiding de teugels strakker aan te trekken. Er zou scherper gecontroleerd worden of een concrete taak niet beter aan de vrije markt kan worden overgelaten. Dit leidde tot een algemene maatregel van bestuur die inhield dat elke neventaak vooraf door de minister van OCW moest worden goedgekeurd.[9]

Zoals gezegd is er sinds 1 januari 2009 een geheel vernieuwde Mediawet. Volgens de memorie van toelichting gaat het om een 'multimediawet' omdat het wetsvoorstel de regelgeving 'aanpast aan de digitale en multimediale praktijk'.[10] In het digitale tijdperk horen, aldus de regering, themakanalen, websites en audiovisuele diensten als 'Uitzending gemist' onlosmakelijk bij de publieke taak. Om dat duidelijk te maken, schrapte het wetsvoorstel het onderscheid tussen hoofd- en neventaken.[11] Een kernbegrip in artikel 1.1 van de Mediawet 2008 is het begrip 'mediadienst'. Dat is een dienst die bestaat uit het verzorgen van media-aanbod door middel van elektronische communicatienetwerken als bedoeld in artikel 1.1, onderdeel h, van de Telecommunicatiewet, waarvoor de verzorger redactionele verantwoordelijkheid draagt. Mediadienst is een zeer ruim begrip dat elke elektronische communicatie naar een publiek omvat: niet alleen omroepdiensten, maar ook informatiediensten die op individueel verzoek worden geleverd.

Tot 1 januari 2009 droeg het grootste hoofdstuk van de Mediawet het opschrift 'De publieke omroep'. Nu heet het grootste hoofdstuk 'Publieke mediadiensten' (artikel 2.1 tot en met 2.188). Dat is een inhoudelijke verandering. Hieruit blijkt dat de 'publieke omroep' zich niet hoeft te beperken tot het verzorgen van omroep.[12] Een beetje inconsequent is dat het coördinerende orgaan van de landelijke publieke mediadienst wel de wettelijke naam Nederlandse Publieke Omroep heeft gekregen. Het zal een praktische reden hebben: de naam was al ingeburgerd. Hoofdstuk 2 blijkt vervolgens uit drie soorten bepalingen te bestaan. Men moet de definities van artikel 1.1 bij de hand houden om ze uit elkaar te houden. Bevat een bepaling de woorden 'media-aanbod' of 'aanbodkanaal' dan heeft zij betrekking op alle audiovisuele diensten. Leest men de woorden 'programma', 'programma-aanbod' of 'programmakanaal', dan is de reikwijdte van het artikel beperkt tot

8 De beschikking aan het adres van Nederland d.d. 22 juni 2006 is gepubliceerd in *Pb L* 49 van 22 februari 2008, p. 1. Beschikkingen aan het adres van diverse andere lidstaten worden vermeld in voetnoten 29 en 37 van de herziene Omroepmededeling 2009 van de Europese Commissie d.d. 2 juli 2009.

9 K.B. van 28 september 2006, Stb. 448 (Besluit tot wijziging van het Mediabesluit in verband met nadere regels inzake het verrichten van neventaken door publieke omroepinstellingen). Zie in het bijzonder het hierin opgenomen artikel 32d, derde lid, van het Mediabesluit.

10 *Kamerstukken II* 2007-08, 31 356, nr. 3, p. 1.

11 *Kamerstukken II* 2007-08, 31 356, nr. 3, p. 2.

12 Een omroepdienst wordt volgens artikel 1.1. van de Mediawet 2008 gekenmerkt door een chronologisch uitzendschema en gelijktijdige ontvangst door het publiek.

omroepdiensten.[13] Dat begrip omvat mede abonneetelevisie, IPTV en omroep voor mobiele telefoons.[14] De derde categorie ten slotte wordt gevormd door bepalingen die verwijzen naar 'de algemene programmakanalen'. Zo'n bepaling heeft betrekking op wat vroeger de 'hoofdtaak' heette, de traditionele radio en televisie.[15]

Wat de publieke mediaopdracht inhoudt, staat in zeer algemene bewoordingen omschreven in artikel 2.1 van de Mediawet. Om een idee te geven: de publieke mediadiensten moeten voldoen aan democratische, sociale en culturele behoeften van de Nederlandse samenleving. Dat blinkt niet uit door scherpte. De nadere invulling van de opdracht geschiedt – althans op landelijk niveau – op voorstel van de Nederlandse Publieke Omroep (NPO). Eens in de vijf jaar stelt de NPO een concessiebeleidsplan op, waarin onder meer moeten zijn opgenomen:

> *a. een beschrijving van de wijze waarop in de komende vijf jaar de publieke mediaopdracht op landelijk niveau wordt uitgevoerd, tevens uitgewerkt in kwantitatieve en kwalitatieve doelstellingen voor het media-aanbod en het publieksbereik van de landelijke publieke mediadienst;*
>
> *b. aard en aantal van de programmakanalen en de daarvoor gewenste frequentieruimte;*
>
> *c. aard en aantal van de overige aanbodkanalen.*
>
> *(..)*[16]

De onderwerpen genoemd onder b en c behoeven de instemming van de minister van OCW, zo bepaalt artikel 2.21 Mediawet. Vervolgens wordt op basis van het beleidsplan een prestatieovereenkomst gesloten.

In de ogen van de pers is de uitbreiding van de publieke taak te ver gegaan. In een open brief van 14 december 2008 aan de minister van OCW sprak een groot gezelschap van hoofdredacteuren en uitgevers bezorgdheid uit over de economische situatie van de gedrukte media. Minister Plasterk had een maand eerder aan de Tweede Kamer geschreven niets te voelen voor overheidssteun aan de pers, omwille van haar onafhankelijkheid.[17] Akkoord, zo stelde de open brief, maar bescherm ons dan in ieder geval tegen oneerlijke concurrentie. De brief vervolgde:

"De ondertekenaars willen zich zeker niet keren tegen al het goede dat de publieke omroepen te bieden hebben, maar vragen zich wel af of het

---

13 Verwarrend is dat de EG-richtlijn audiovisuele mediadiensten het begrip 'programma' in een ruimere betekenis hanteert dan de Mediawet. Volgens artikel 1 onderdeel b van de richtlijn betekent het een reeks bewegende beelden die hetzij via een uitzendschema, hetzij op aanvraag, aan het publiek worden aangeboden. Richtlijn 2007/65/EG van het Europees Parlement en de Raad van 11 december 2007 tot wijziging van Richtlijn 89/552/EEG van de Raad (Richtlijn audiovisuele mediadiensten).

14 *Kamerstukken II* 2007-08, 31 356, nr. 3, p. 22.

15 Zie artikel 2.1, derde lid, van de Mediawet.

16 Artikel 2.20, tweede lid, van de Mediawet.

17 Brief van de minister van OCW over het persbeleid d.d. 14 november 2008, *Kamerstukken II*, 2008-09, 31 777, nr. 1.

publiceren van tijdschriften en het bouwen van websites niet wat te ver staan van de oorspronkelijke taak van de publieke omroep. In elk geval zorgen deze activiteiten, samen met het uitzenden van reclame, voor concurrentievervalsing. De gedrukte media moeten immers opboksen tegen een concurrent die zich financieel gesteund weet door de overheid, waardoor het extra moeilijk is voldoende gelden te vergaren die weer nodig zijn om innovaties te plegen."[18]

Zorgplicht van de overheid

Het kan nooit kwaad af en toe stil te staan bij de vraag waarom de overheid zich überhaupt met de media moet bemoeien. Waarom zijn er door de overheid georganiseerde en gefinancierde media? Natuurlijk, het verschijnsel van een publieke naast een private sector komt wel vaker voor. Wij komen dit model tegen op allerlei terreinen van het maatschappelijk leven, zoals onderwijs, volkshuisvesting, gezondheidszorg, vervoer en cultuur. Daarmee staat echter nog niet vast dat een duaal bestel ook voor de media passend is. Zeker bij het verstrekken van informatie over zaken van algemeen belang moet de staat de vrijheid meningsuiting respecteren. Dat grondrecht dwingt tot terughoudendheid. Theoretisch zou de staat kunnen besluiten de media vrijwel geheel aan de vrije markt over te laten, om slechts bij een falen van de markt corrigerend in te grijpen. Bijvoorbeeld door diensten die commercieel niet rendabel zijn, maar die wel van maatschappelijk belang worden geacht, in het openbaar aan te besteden. Of door een zeer beperkte steunregeling te handhaven, zoals bij dagbladen en opinietijdschriften.

Binnen de Raad van Europa is echter de algemene opvatting dat een publieke mediadienst gewenst is. Deze hoeft niet beperkt te blijven tot een steeds kleiner wordend reservaat van radio en televisie. Dit blijkt uit een Recommendation van het Comité van Ministers van 31 januari 2007 'on the remit of public service media in the information society'.[19] De tekst mondde uit in aanbevelingen aan de regeringen van de lidstaten om de volgende dingen te doen:

> "i. guarantee the fundamental role of the public service media in the new digital environment, setting a clear remit for public service media, and enabling them to use new technical means to better fulfil this remit and adapt to rapid changes in the current media and technological landscape, and to changes in the viewing and listening patterns and expectations of the audience;

18 De brief van de hoofdredacteuren en de uitgevers d.d. 14 december 2008 is gepubliceerd op www.nrc.nl/redactie/media/krantenbriefaanplasterk.pdf.

19 Recommendation CM/Rec(2007)3 of the Comittee of Ministers to Member States on the remit of public service media in the information society, adopted by the Committee of Ministers on January 31, 2007 at the 985th meeting of the Ministers' Deputies. Zie ook de eerdere Recommendation 1641 (2004) of the Parliamentary Assembly on Public Service Broadcasting, January 27, 2004.

ii. include, where they have not already done so, provisions in their legislation/regulations specific to the remit of public service media, covering in particular the new communication services, thereby enabling public service media to make full use of their potential and especially to promote broader democratic, social and cultural participation, inter alia, with the help of new interactive technologies;

iii. guarantee public service media, via a secure and appropriate financing and organisational framework, the conditions required to carry out the function entrusted to them by member states in the new digital environment, in a transparent and accountable manner;

iv. enable public service media to respond fully and effectively to the challenges of the information society, respecting the public/private dual structure of the European electronic media landscape and paying attention to market and competition questions;

v. ensure that universal access to public service media is offered to all individuals and social groups, including minority and disadvantaged groups, through a range of technological means;

vi. disseminate widely this recommendation and, in particular, bring to the attention of public authorities, public service media, professional groups and the public at large, the guiding principles set out below, and ensure that the necessary conditions are in place for these principles to be put into practice.

(..)"

Recommendations van het Comité van Ministers zijn geen bindende besluiten, maar hebben wel een juridische relevantie. Vaak ziet men dat dergelijke teksten invloed hebben op de jurisprudentie van het Europese Hof voor de Rechten van de Mens. De Recommendation over de publieke omroep is al geciteerd in een arrest tegen Polen van 16 juli 2009.[20] De klacht was ingediend door een journaliste van 'Telewizja Polska Spółka Akcjna', de Poolse publieke televisie, die openlijk kritiek had geuit op de culturele verschraling van het programma-aanbod. Zij had voor deze uiting een berisping gekregen van haar werkgever, wat door het Hof – mede in het licht van de Recommendation – in strijd met de vrijheid van meningsuiting wordt geoordeeld. Denkbaar is dat in de toekomst de vraag zal worden gesteld hoe een uitbreiding van de taken van de publieke omroep naar het internet moet worden beoordeeld in het licht van artikel 10 EVRM. Is het subsidiëren van nieuwe diensten geoorloofd? Bestaat er zelfs een positieve verplichting om dit te doen?

Het belang van pluralisme is al in een vroeg stadium door het EHRM onderkend. Reeds in het Handyside-arrest van 1976 overwoog het Hof dat pluralisme een onmisbare voorwaarde is voor het bestaan van een democratische samenleving.[21] Deze woorden zijn dikwijls herhaald, zodat men kan spreken van vaste jurisprudentie. Anders dan artikel 11, tweede lid, van het Handvest Grondrechten van de Europese Unie[22] maakt artikel 10 EVRM niet

20 EHRM 16 juli 2009, appl. no. 20436/02, Wojtas-Kaleta vs Polen.
21 EHRM 7 december 1976, Handyside vs UK, NJ 1978, 236, r.o. 49. Zie ook Komorek 2009.
22 *PbEG* 2000, C 364/1.

uitdrukkelijk melding van een plicht tot het eerbiedigen van de pluriformiteit van de media. Wel is aannemelijk dat artikel 10 EVRM een positieve verplichting impliceert om het belang van het publiek bij een geschakeerd aanbod van informatie zo goed mogelijk te dienen. In het Sunday Times arrest overwoog het Hof dat artikel 10 niet alleen de vrijheid van de media beschermt, maar ook 'the right of the public to be properly informed'.[23] Eerder had de Europese Commissie voor de Rechten van de Mens geschreven dat het kan voorkomen dat 'a State fails in its duty to protect against excessive press-concentrations', al deed zich die situatie in de onderhavige zaak niet voor.[24] In dezelfde lijn ligt het arrest Lentia, waarin gesproken wordt van 'the principle of pluralism of which the State is the ultimate guarantor'.[25]

Hoe kan een geschakeerd aanbod van informatie het beste kan worden bereikt? Is het financieren van een brede publieke mediadienst daarvoor de beste methode? Het zal duidelijk zijn dat deze vraag in hoge mate politiek van aard is. Een VVD'er zal andere antwoorden geven dan een SP'er. Wat dat betreft is er een parallel te trekken met sociale grondrechten. De wetgever moet streven naar een bepaald doel, maar mag zelf de middelen kiezen om dat doel te bereiken. De rechter past een terughoudende opstelling, want hij is niet door het volk gekozen. Zelfs beperkingen van de uitingsvrijheid om het ideaal van pluriformiteit te bereiken zijn niet uitgesloten. Het EHRM heeft nog niet zo lang geleden geoordeeld dat het belang van 'the quality and balance of programmes' kan rechtvaardigen dat een zendvergunning voor televisie wordt geweigerd.[26] Echter, net als bij sociale grondrechten moet de rechter ingrijpen wanneer de keuzes van de wetgever volstrekt onredelijk zijn. Het Comité van Ministers wees in bovenstaande Recommendation – onder punt iv – op de noodzaak aandacht te besteden aan vragen van mededingingsrecht. In het bijzonder zou het niet te verkopen zijn wanneer de schrijvende pers geheel wordt opgeofferd ten behoeve van een publieke mediadienst.

Concurrentievervalsing

Op 2 juli 2009 publiceerde de Europese Commissie de lang verwachte Omroepmededeling 2009.[27] In Nederlandse termen kunnen we spreken van

23 EHRM 26 april 1979, Sunday Times vs UK, NJB, 1980, 146, r.o. 66.
24 ECRM 6 juli 1976, De Geïllustreerde Pers NV vs Nederland, NJ 1978, 237, r.o. 88.
25 EHRM 24 november 1993, Lentia vs Oostenrijk, NJ 1995, 382, r.o. 38. Herhaald in o.a. EHRM 3 mei 2007, appl. no. 1543/06, Bączkowski and Others v. Poland, r.o. 64.
26 EHRM 5 november 2002, appl. no. 38743/97, Demuth vs Zwitserland, r.o. 33. Zie ook EHRM 28 maart 1990, Groppera Radio vs Zwitserland, NJ 1991, 739, r.o. 70.
27 Te vinden op http://ec.europa.eu/competition/index_nl.html. Zie het persbericht van de Commissie IP/09/1072. Commissaris Neelie Kroes van Mededinging is primair verantwoordelijk.

een beleidsregel waarin de Commissie haar beleid inzake staatssteun aan publieke media uiteenzet. Het werd hoog tijd dat de oude Omroepmededeling van 2001 werd vervangen, zowel om juridische als om praktische redenen. Een juridische reden is dat het Hof van Justitie in 2003 duidelijkheid heeft gecreëerd over de vraag wat staatssteun eigenlijk is. In het Altmark-arrest[28], dat betrekking had op de financiering van openbaar vervoer, bepaalde het Hof van Justitie dat een compensatie voor de kosten van een openbare dienstverplichting niet als staatssteun is te beschouwen als aan vier voorwaarden is voldaan:

1. De openbare dienstverplichtingen moeten duidelijk zijn afgebakend.
2. De maatstaven voor de berekening van de compensatie moeten vooraf op objectieve en doorzichtige wijze zijn vastgesteld.
3. De compensatie mag niet hoger zijn dan de kosten, rekening houdend met de opbrengsten en een redelijke winst.
4. Als niet gekozen is voor een openbare aanbesteding, moet de noodzakelijke compensatie worden vastgesteld aan de hand van de kosten die een gemiddelde, goed beheerde onderneming zou hebben gemaakt.

Is een bepaalde subsidie geen staatssteun, dan komt men niet meer toe aan de vraag of staatssteun gerechtvaardigd is op grond van de artikel 86, tweede lid, of artikel 87, tweede en derde lid, van het EG-verdrag.

Er is ook een praktische reden waarom de oude Omroepmededeling moest worden vervangen. Sedert 2001 zijn de distributieplatforms voor audiovisuele diensten veel talrijker geworden, zoals voor digitale televisie, IPTV, mobiele televisie en 'video on demand'. Het traditionele model van passieve consumptie verandert geleidelijk in een model met actieve participatie en controle door consumenten. Publieke en commerciële partijen pogen daarop in te spelen door diversificatie. Dat heeft geresulteerd in concurrentie met nieuwe spelers, zoals netwerkexploitanten en internetbedrijven. Er vindt bovendien een convergentie van audiovisuele diensten plaats nu consumenten steeds meer via één platform of toestel meerdere diensten kunnen ontvangen of één dienst via meerdere platforms of toestellen aangeboden krijgen. De Omroepmededeling van 2001 was niet op deze ontwikkelingen toegesneden. Wel moest de Europese Commissie de afgelopen jaren al oordelen over activiteiten van de Duitse publieke omroepen ARD en ZDF op het terrein van de nieuwe media. Bij het verrichten van deze diensten handelden beide omroepen in opdracht van het Rundfunkstaatsvertrag, een verdrag dat gesloten is tussen de Duitse deelstaten. Nadat Duitsland enkele toezeggingen had gedaan, besloot de Commissie de procedure te staken.[29]

---

28 HvJEG 24 juli 2003, zaak C-280/00, Altmark Trans GmbH, Jur. 2003, p. I-7747.

29 Zie de uitvoerige beschikking van de Europese Commissie d.d. 24 april 2007, C(2007)1761 FINAL, alsmede de persberichten IP/07/543 en MEMO/07/150.

In de Omroepmededeling van 2009 wordt veel aandacht besteed aan de uitleg van artikel 86, tweede lid, van het EG-verdrag. Kennelijk gaat de Commissie ervan uit dat het voor een lidstaat heel moeilijk zal zijn aan de Altmark-criteria te voldoen. Dat sluit aan bij de beschikkingenpraktijk van de afgelopen jaren. Het blijkt vooral lastig de opgedragen openbare dienstverrichtingen 'duidelijk' af te bakenen. Dat lukt wel op het gebied van openbaar vervoer – laat twee keer per uur een bus rijden van Bussum naar Naarden – maar niet voor informatie, educatie, cultuur en verstrooiing in de media. Ook het vooraf vaststellen van objectieve maatstaven om de hoogte van de vergoeding vast te stellen, levert in de praktijk problemen op. Dat betekent dat er een rechtvaardiging moet worden gevonden voor het verlenen van staatssteun krachtens artikel 86 of 87 van het EG-verdrag. Artikel 87, derde lid onderdeel d, dat betrekking heeft op cultuurbeleid, lijkt een mogelijkheid te bieden. De Commissie meent echter dat deze uitzondering zeer beperkt moet worden uitgelegd. Bedoeld zijn cultuuruitingen in enge zin en niet het brede scala van programma's dat een publieke omroep pleegt uit te zenden.

Essentieel is dus artikel 86, tweede lid, van het EG-verdrag. Onder bepaalde voorwaarden kan een afwijking van het verdrag worden toegestaan voor bepaalde categorieën diensten. De Omroepmededeling 2009 vat deze voorwaarden als volgt samen:

> i. de betrokken dienst moet een dienst van algemeen economisch belang zijn en duidelijk als dusdanig door de lidstaat zijn omschreven (omschrijving);
>
> ii. de betrokken onderneming moet door de lidstaat uitdrukkelijk met de verlening van die dienst zijn belast (toewijzing);
>
> iii. de toepassing van de mededingingsregels uit het Verdrag (in dit geval, het verbod op staatssteun) moet de vervulling van de aan deze onderneming toevertrouwde bijzondere taken verhinderen, en de ontheffing van die regels mag de ontwikkeling van het handelsverkeer niet beïnvloeden in een mate die strijdig is met het belang van de Gemeenschap (evenredigheidstoets).

De voorwaarde onder i doet een beetje denken aan de eerste voorwaarde van het Altmark-arrest. In het kader van artikel 86, tweede lid, is de eis echter minder streng. De Commissie wijst er namelijk op dat artikel 86 moet worden uitgelegd in het licht van het 'Protocol betreffende het publieke omroepstelsel in de lidstaten', behorende bij het Verdrag van Amsterdam.[30] In dit interpretatieve Protocol wordt overwogen dat *'het publieke omroepstelsel in de lidstaten rechtstreeks verband houdt met de democratische, sociale en culturele behoeften van iedere samenleving en met de noodzaak pluralisme in de media te behouden*'. De lidstaten zijn volgens het Protocol in beginsel vrij de publieke omroepdienst van hun land te omschrijven en toe te wijzen. Zij kunnen

30 *PB* 1997, C 340, blz. 109. In een resolutie betreffende de publieke omroep van 25 januari 1999 hebben de Raad en de lidstaten het 'vitale' belang van de publieke omroep nog eens bevestigd, *Pb EG* C 30, p. 1.

ervoor kiezen een organisatie te belasten met het uitzenden van een breed scala aan programma's, mits er kwalitatieve eisen worden gesteld.[31] De omschrijving van de publieke taak mag inhouden dat audiovisuele diensten via nieuwe distributieplatforms worden aangeboden. Aan de Commissie komt slechts een marginale controle toe. Zij kan ingrijpen wanneer de opgedragen activiteiten redelijkerwijs geen verband houden met 'democratische, sociale en culturele behoeften'.

De voorwaarde onder ii is dankzij het Protocol van Amsterdam evenmin erg streng. Wel wijst de Commissie erop dat de toewijzing van taken gepaard moet gaan met een onafhankelijke controle op de uitvoering. De slager moet niet zijn eigen vlees keuren. Wat betreft de controle op wettelijke voorschriften zit Nederland veilig. Het Commissariaat voor de Media, dat toezicht houdt op de naleving van de meeste voorschriften in de Mediawet, is onafhankelijk van de omroepen. Wat betreft de controle op de kwaliteit is het ingewikkelder. Hier is de Raad van Bestuur van NPO bevoegd.[32] Weliswaar is dat ook een bestuursorgaan, maar deze raad geeft tevens leiding aan de stichting NPO. Dat is de houdster van de concessie, die zelf het concessiebeleidsplan opstelt en een prestatieovereenkomst sluit met de minister van OCW.[33] Daar komt bij dat de Raad van Bestuur van rechtswege de raad van toezicht vormt van de grootste media-instelling, de Nederlandse Omroep Stichting.[34] Het is niet zeker of de Commissie deze combinatie van functies zal accepteren. Zou het op een conflict aankomen dat zal Nederland waarschijnlijk wijzen op de regeling voor taakverwaarlozing in artikel 2.16 Mediawet. Volgens de memorie van toelichting kan de minister van OCW bij taakverwaarlozing door NPO verreikende maatregelen treffen, zoals het aanstellen van tijdelijke bewindvoerders.[35]

Het venijn zit hem in de derde voorwaarde. Het Protocol van Amsterdam deed geen afbreuk aan de slotzin van artikel 86, tweede lid, van het EG-verdrag: de ontwikkeling van het handelsverkeer mag niet worden beïnvloed in een mate die strijdig is met het belang van de Gemeenschap. De Commissie benadrukt het belang van financiële transparantie, om te voorkomen dat publieke middelen wegvloeien naar commerciële activiteiten. Bij de consultaties ter voorbereiding van de Omroepmededeling is ook veel aandacht uitgegaan naar 'diversificatie'. Steen des aanstoots was de onafhankelijke 'market impact assessment' die de Commissie wilde voorschrij-

---

31 Twee recente uitspraken van het Gerecht van Eerste Aanleg illustreren dit.
GvEA 26 juni 2008, zaak T-442/03, Sociedade Independente de Comunicação SA vs Commissie, r.o. 201 en 211.
GvEA 22 oktober 2008, gevoegde zaken T-309/04, T-317/04, T-329/04 en T-336/04, TV 2/Danmark A/S e.a. vs Commissie, r.o. 122-124.

32 Artikel 2.10, tweede lid, juncto 2.54, 2.55 en 2.60 van de Mediawet. De Raad van Bestuur kan media-instellingen bestraffen op grond van artikel 2.154. In extreme gevallen kan 2.33, derde lid, worden toegepast.

33 Artikel 2.19, 2.20 en 2.22 van de Mediawet.

34 Artikel 2.34c van de Mediawet.

35 *Kamerstukken II* 2007-08, 31 356, nr. 3, p. 29.

ven voordat een publieke omroep nieuwe diensten mag aanbieden. Verscheidene landen, waaronder Nederland, zagen hierin een poging de publieke omroep te beperken tot zijn traditionele domein.[36] In de definitieve versie zijn de voornemens van de Commissie afgezwakt. De mogelijkheid is open gelaten dat burgers een bijdrage betalen in de transmissiekosten voor extra diensten. Een openbare raadpleging om vooraf te onderzoeken of een activiteit marktverstorende effecten heeft, is alleen verplicht wanneer sprake is van 'significant nieuwe' audiovisuele diensten. Belangrijk is dat het in eerste instantie aan de lidstaten wordt overgelaten om uit te maken welke voorgenomen diensten 'significant nieuw' zijn.

Een vruchtbare werkrelatie?

Het lijkt erop dat een aanval uit Brussel in de kiem is gesmoord. Staatssteun voor publieke internetdiensten blijft mogelijk als deze vergelijkbaar zijn met de diensten die de publieke omroep al jaren verricht. In de Omroepmededeling 2009 noemt de Commissie als voorbeeld de gelijktijdige transmissie van het avondjournaal op andere platforms (o.a. internet en mobiele toepassingen).[37] Ook een dienst als 'Uitzending gemist' zit niet in de gevarenzone. Alleen bij de invoering van significant nieuwe diensten moet aan de hand van een openbare raadpleging vooraf worden onderzocht wat de gevolgen zijn voor de markt. Een instantie die onafhankelijk is van het management van de publieke omroep moet dan over de invoering beslissen. Aan die eisen kan op grond van de Mediawet worden voldaan. NPO kan niet zelfstandig besluiten tot een wijziging van de aard en het aantal van de 'overige aanbodkanalen'. Haar voornemen behoeft op grond van artikel 2.21 van de Mediawet de instemming van de minister van OCW. Een dergelijke instemming is een voor beroep vatbaar besluit. Omgekeerd zou de stichting NPO in beroep kunnen gaan tegen de afwijzing van een verzoek tot instemming. Als de minister van oordeel is dat wellicht sprake is van een significant nieuwe audiovisuele dienst, kan hij besluiten toepassing te geven aan artikel 3:10 e.v. van de Awb. Een uniforme openbare voorbereidingsprocedure is precies wat de Commissie verlangt.

Naast het algemene mededingingsrecht staat de plicht om waarborgen te scheppen voor pluralisme. Dat is ook de gedachte achter de publieke financiering van mediadiensten. Zou nu blijken dat de staatssteun aan NPO ten koste gaat van de pers, dan wordt deze doelstelling ondergraven. De zorgplicht die inherent is aan artikel 10 EVRM en artikel 11 van het Handvest Grondrechten van de EU geldt voor media in het algemeen. Bij het ver-

36 Brief van de minister van OCW aan de Tweede Kamer d.d. 20 juni 2008, *Kamerstukken II* 2007-08, 31 356, nr. 9 en 21501-34, nr. 105. Zie ook diens brief d.d. 12 januari 2009, *Kamerstukken II* 2008-09, 21 501-34, nr. 111.

37 Omroepmededeling 2009, p. 23, voetnoot 51.

lenen van staatssteun moet de overheid dus letten op nadelige effecten voor persorganen, in het bijzonder die waarop artikel 8.10 van de Mediawet doelt. Dat zijn persorganen die 'in belangrijke mate nieuws, analyse, commentaar en achtergrondinformatie bevatten over een gevarieerd deel van de maatschappelijke actualiteit, mede in het belang van de politieke meningsvorming'. Zij verschijnen niet alleen op gedrukt papier. Persorganen gebruiken internet onder meer voor het openstellen van hun archief, het aanbieden van een discussieforum en het leveren van bewegende beelden. Winst leveren deze activiteiten nauwelijks op, wat mede wordt veroorzaakt door de sterke presentie van NPO online. Om een vruchtbare werkrelatie van beide sectoren te bevorderen, heb ik drie suggesties.

1. Laat de pers profiteren van publieke producties.
Volgens een bericht in NRC-Handelsblad van 29 juli 2009 heeft de BBC besloten gratis nieuwsbeelden ter beschikking te stellen aan Britse kranten die deze vervolgens kunnen gebruiken op hun eigen sites. Het betreft materiaal dat al is gepubliceerd op de website van de BBC zelf. De beelden vallen in de categorie Brits nieuws, economie, gezondheid en wetenschap/technologie. Uitgezonderd zijn opnames van sportevenementen. Vooralsnog kunnen alleen de *Daily Telegraph*, de *Guardian*, de *Independent* en de *Daily Mail* van het aanbod profiteren. Andere kranten zullen binnenkort volgen, op voorwaarde dat hun website dagelijks een minimumaantal bezoekers trekt. In Nederland deed de Commissie-Brinkman onlangs een vergelijkbaar voorstel. De Nederlandse overheid zou moeten bevorderen dat de stichting NPO tegen redelijke condities videomateriaal levert voor websites van derden die primair gericht zijn op het verschaffen van journalistieke informatie.[38] Van een commerciële omroep zou men zoiets niet mogen eisen, maar de situatie van de NPO is anders. Het is goed te verdedigen dat wat met publiek geld is gemaakt beschikbaar wordt gesteld voor hergebruik.

2. Schaf wettelijke belemmeringen voor samenwerking af
Samenwerking tussen publieke media-instellingen en de pers stuit op dit moment op allerlei juridische hindernissen. Maakt een uitgever dankzij de samenwerking een meer dan normale winst, dan overtreedt de publieke media-instelling artikel 2.141 van de Mediawet. Levert zo'n instelling videobeelden aan een krant, dan kan sprake zijn een verboden nevenactiviteit (artikel 2.132 Mediawet). Levert een krant informatie aan een publieke media-instelling, dan dreigt het gevaar van verboden sponsoring (artikel 2.106 Mediawet). Bij een gelijkwaardige samenwerking zijn er meer mogelijkheden, maar dan moet eerst worden vastgesteld of een samenwerking inderdaad 'gelijkwaardig' is. Dat is lastig als de ene partij een creatieve inbreng heeft en de andere een organisatorische. Het Commissariaat voor de

38 Rapport 'De volgende editie' van de Tijdelijke Commissie Innovatie en Toekomst Pers (Commissie-Brinkman) d.d. 23 juni 2009, p. 9.

Media heeft in 2008 bepaalde openingen gecreëerd, maar alleen voor zover de wet beleidsvrijheid biedt. In het media-aanbod van een publieke media-instelling mag de naam van een krant bijvoorbeeld niet te vaak genoemd worden,want dat is verboden reclame (artikel 2.89 Mediawet jo. artikel 9 e.v. Mediabesluit). Bovenstaand systeem is veel te ingewikkeld. Ik zou zeggen: maak in de wet een generieke uitzondering voor de pers. NPO en de uitgevers kunnen dan in vrijheid onderhandelen.

3. Overweeg een openbare aanbesteding

Stel dat er in Nederland een 'democratische, sociale of culturele behoefte' ontstaat aan een significant nieuwe audiovisuele dienst. Een optie is dat NPO die taak ter hand neemt door een wijziging aan te brengen in het concessiebeleidsplan en dit ter goedkeuring voorlegt aan de minister van OCW. Overeenkomstig de wensen van de Commissie moeten er dan hoorzittingen plaats vinden om te onderzoeken welke invloed een eventuele toewijzing aan NPO zal hebben op het functioneren van de markt. Het valt nu al te voorspellen dat daar langdurig over geprocedeerd gaat worden. Zelfs het overnemen van de Concertzender, een verlieslijdend project, door de publieke omroep leidde tot een procedure tot en met de Raad van State.[39] Dat kan simpeler. Als de overheid een budget beschikbaar wil stellen voor een nieuwe voorziening, kan ook een openbare aanbesteding worden gehouden. Misschien komt NPO als beste uit de bus, maar het is ook niet uitgesloten dat een uitgever in staat blijkt betere kwaliteit voor hetzelfde geld te leveren. In het Altmark-arrest liet het Hof van Justitie al doorschemeren een voorkeur te hebben voor het instrument van de openbare aanbesteding. Na zo'n procedure hoeft de staat zich niet meer af te vragen welke kosten een 'gemiddelde, goed beheerde onderneming' voor deze activiteit zou hebben gemaakt. Bijkomend voordeel: over openbare aanbestedingen kan men altijd advies vragen aan Aernout Schmidt.[40]

Verwijzingen

Chavannes 2004
R. Chavannes, 'Neventaakfinanciering, staatssteun en de toekomst van de publieke omroep: back to basics?', *Mediaforum* 2004-10, p. 302-308.

Komorek 2009
E. Komorek, 'Is Media Pluralism a Human Right? The European Court of Human Rights, the Council of Europe and the Issue of Media Pluralism', *European Human Rights Law Review* 2009-3, p. 395-414.

39 ABRvS 1 juni 2005, Commissariaat voor de Media c.s. vs Classic FM c.s., Mediaforum 2005-11/12, nr. 37, m.nt. L. Hancher en Q.R. Kroes.

40 Zie o.a. Schmidt & Corvers 2009.

Kroes 2005
Q. Kroes, 'Het Commissariaat als scheidsrechter op een (un)level playing field', *Mediaforum* 2005-7/8, p. 252-257.

Robichon-Lindenkamp 2007
M. Robichon-Lindenkamp, 'Het nieuwe regime voor neventaken: 'Brusselproof' lapmiddel in afwachting nieuwe Mediawet, *Mediaforum* 2007-3, p. 70-79.

Schmidt & Corvers 2009
A.H.J. Schmidt & Corvers, S.F.M. (2009), *Aanbesteding & Innovatie. Juridisch handboek functioneel specificeren van aanbestedingen*, Den Haag, Sdu.

De nabuurrechtelijke aanspraak op een billijke vergoeding voor privé-kopiëren naar internationaal recht

Cyril van der Net■

Inleiding

Aernout Schmidt heeft bijzondere belangstelling voor criteria aan de hand waarvan de kwaliteit van het recht in het algemeen en wet- en regelgeving in het bijzonder kan worden beoordeeld. Hij heeft zich veelvuldig ingelaten met multidisciplinair onderzoek, waaraan de door hem duidelijk geventileerde gedachte ten grondslag ligt dat eerder genoemde criteria ook buiten het recht kunnen c.q. moeten worden gevonden. Zijn conclusies en aanbeveling werden vaak mede gedragen door een (rechts)economische pijler[1] en hadden alleen daarom al – zeker voor wetgevingsjuristen (waartoe ik mijzelf aanstonds ook weer mag rekenen) – wezenlijke meerwaarde.

Deze bijdrage, een bewerking van een eerder gepubliceerd artikel in Ami[2], geschreven voor de voormalige begeleider van mijn scriptie en proefschrift, steekt ogenschijnlijk schril af bij de door Aernout voorgestane multidisiplinaire aanpak. Betoogd wordt namelijk niet meer dan dat niet-Europese uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties (en hun rechtverkrijgenden) geen aanspraak kunnen maken op de billijke vergoeding voor privé-kopiëren uit hoofde van het vigerende internationaal nabuurrechtelijk kader. Dat kader wordt achtereenvolgens gevormd door (1) de Conventie van Rome, (2) de Conventie van Genève, (3) het TRIPs-verdrag en (4) het WPPT. [3] Maar schijn bedriegt. Binnenkort zal de Hoge Raad namelijk een oordeel vellen over de uitleg van het nationale recht dat de vertaling vormt van die verdragen.

Aan het licht komt dan of het nationale recht eigenlijk wel strookt met het internationale recht. En dat is interessant, omdat het internationale recht de weerslag vormt van langdurige onderhandelingen die er juist op nabuurrechtelijk gebied vooral ook toe strekken welbepaalde economische belan-

---

■ Cyril van der Net was op het moment dat deze op persoonlijke titel geschreven bijdrage werd afgerond advocaat te Amsterdam.

1 Schmidt, Dolfsma & Keuvelaar, 2007.

2 Van der Net 2008a.

3 Internationaal Verdrag inzake de bescherming van uitvoerende kunstenaars, producenten van fonogrammen en omroeporganisaties (Conventie van Rome) van 26 oktober 1961 (*Trb*. 1986, 182), Overeenkomst ter bescherming van producenten van fonogrammen tegen het ongeoorloofd kopiëren van hun fonogrammen van 29 oktober 1971 (*Trb*. 1986, 183), Overeenkomst inzake de handelsaspecten van de intellectuele eigendom van 15 april 1994 (*Trb*. 1995, 130) en WIPO uitvoeringen- en fonogrammenverdrag van 20 december 1996 (*Trb*. 1998, 248).

gen veilig te stellen. In feite wordt in deze bijdrage dus een mede door rechtseconomische motieven geïnspireerd referentiekader geduid. Aan de hand daarvan kan het nationale recht, zoals dat volgens de Hoge Raad moet worden geïnterpreteerd, in kwalitatieve zin worden beoordeeld. Mochten er discrepanties bestaan, dan kan het kader wellicht ook dienst doen als patroon waarnaar het nationale recht moet worden gemodelleerd. Als de thuiskopieregeling blijft bestaan tenminste. Het kabinet heeft recentelijk namelijk te kennen gegeven te overwegen de hele regeling af te schaffen.[4] De (on)zin van die plannen blijft in deze bijdrage buiten beschouwing.

Artikel 10, onderdeel e, van de Wet op de naburige rechten wordt dus als een vaststaand gegeven beschouwd. Uit hoofde van die bepaling mogen natuurlijke personen een reproductie voor eigen oefening, studie of gebruik maken van nabuurrechtelijk beschermde prestaties (uitvoeringen, fonogrammen en uitzendingen) zonder dat zij daarvoor aan de nabuurrechthebbenden (uitvoerende kunstenaars, fonogrammenproducenten respectievelijk omroeporganisaties, of hun rechtverkrijgenden) vooraf toestemming behoeven te vragen. Aan de inroepbaarheid van de uitzondering op het reproductierecht voor privé-kopiëren is de voorwaarde van het betalen een billijke vergoeding verbonden teneinde rechthebbenden in lijn met artikel 5 lid 2 onderdeel b van de richtlijn auteursrecht en naburige rechten in de informatiemaatschappij, waarop de beperking voor privé-kopiëren is gebaseerd,[5] te compenseren voor de schade die zij dientengevolge lijden. De vergoeding moet worden betaald door de fabrikanten of importeurs van voorwerpen die bestemd zijn om daarop nabuurrechtelijk beschermde prestaties voor privé-gebruik vast te leggen. Die vergoeding wordt in de praktijk vanzelfsprekend doorberekend aan de consument. In deze bijdrage wordt per verdrag aangegeven waarom de internationale erkenning van de aanspraken van nabuurrechthebbenden niet zo ver reikt dat ook de vergoeding voor privé-kopiëren wordt bestreken.

Conventie van Rome

De Conventie van Rome strekt ertoe de prestaties van uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties te beschermen. Daartoe worden aan uitvoerende kunstenaars, in het bijzonder artiesten, onder andere de economische exploitatierechten verleend (1) de vastlegging van hun uitvoeringen en (2) de reproductie van hun uitvoeringen toe te staan of te verbieden (ex artikel 7 lid 1). Voor acteurs doet artikel 7 niet langer opgeld, wanneer zij eenmaal hebben ingestemd met de vastlegging van

4 Kabinetsreactie nieuwe aanpak auteursrecht op internet, www.boek9.nl, B9 8311.

5 Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, *PbEG* 2001, L 167/10.

hun uitvoeringen op film (ex artikel 19). Fonogrammenproducenten hebben onder andere het recht om toestemming te verlenen voor het reproduceren van hun fonogrammen dan wel zulks te verbieden (artikel 10). Aan omroeporganisaties komen, onder andere, de rechten toe (1) de vastlegging en (2) de reproductie toe te staan dan wel te verbieden (artikel 13). De ratio die aan de bescherming ten grondslag ligt, is dat uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties niet alleen erkenning verdienen voor de door hen geleverde prestaties maar ook dat zij bescherming verkrijgen tegen het gebruik daarvan door anderen zonder hun toestemming of vergoeding. Hierdoor worden (investeringen in) nieuwe prestaties gestimuleerd, hetgeen ook de samenleving in cultureel en economisch opzicht ten goede komt. Bij de Conventie van Rome zijn inmiddels 86 Staten aangesloten. Nederland is sinds 7 oktober 1993 partij bij het verdrag.

De Conventie van Rome gaat er vanuit dat een Verdragsluitende Staat de prestaties van uitvoerende kunstenaars en fonogrammenproducenten zal beschermen voor zover het eigen onderdanen betreft (natuurlijke personen respectievelijk rechtspersonen). Op grond van artikel 2 lid 1 onderdeel a is dat voor uitvoerende kunstenaars het geval indien de uitvoeringen op zijn grondgebied (1) hebben plaatsgevonden, (2) worden uitgezonden of (3) voor het eerst zijn vastgelegd. Op grond van artikel 2 lid 1 onderdeel b is dat voor fonogrammenproducenten het geval indien de fonogrammen op zijn grondgebied voor het eerst (1) zijn vastgelegd of (2) openbaar gemaakt. De Conventie van Rome geeft ook aan wanneer een Verdragsluitende Staat gehouden is omroeporganisaties te beschermen die hun hoofdkantoor op zijn grondgebied hebben. Op grond van artikel 2 lid 1 onderdeel c is dat namelijk het geval indien de uitzendingen plaatsvinden via zendinstallaties die zijn gelegen op zijn grondgebied.

De Conventie van Rome bepaalt ook wanneer een Verdragsluitende Staat verplicht is om de prestaties van uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties te beschermen voor zover het buitenlanders en/of buitenlands repertoire betreft. Uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties kunnen zich voor bescherming kwalificeren door de op hen toegesneden toepassingscriteria te vervullen. De op uitvoerende kunstenaars betrekking hebbende toepassingscriteria zijn neergelegd in artikel 4. Op grond van die bepaling dient een Verdragsluitende Staat buitenlandse uitvoerende kunstenaars en hun rechtverkrijgenden te beschermen, wanneer: (1) de uitvoering plaats heeft gevonden in een ander land dat partij is bij de Conventie van Rome, (2) de uitvoering is opgenomen op een fonogram dat wordt beschermd op grond van de Conventie van Rome, of (3) de uitvoering, die niet is vastgelegd op zo'n fonogram, wordt uitgezonden door middel van een uitzending die wordt beschermd op grond van de Conventie van Rome. De vraag rijst of het laatste criterium alleen betrekking heeft op live muziekuitvoeringen dan wel tevens op – al dan niet live – audiovisuele uitvoeringen. Blijkens de totstandkomingsgeschiedenis gaat het vermoedelijk alleen om live muziekuitvoeringen.

De op fonogrammenproducenten betrekking hebbende toepassingscriteria zijn neergelegd in artikel 5 lid 1. Op grond van die bepaling dient een Verdragsluitende Staat buitenlandse fonogrammenproducenten en hun rechtverkrijgenden te beschermen, wanneer: (1) de fonogrammenproducent onderdaan is van een andere Verdragsluitende Staat (nationaliteitscriterium), (2) de eerste vastlegging van de klanken op het fonogram werd verricht in een andere Verdragsluitende Staat (vastleggingscriterium), of (3) het fonogram voor het eerst werd openbaar gemaakt in een andere Verdragsluitende Staat (openbaarmakingscriterium). Op grond van artikel 5 lid 2 wordt het laatstgenoemde toepassingscriterium door middel van een juridische fictie opgerekt. Een fonogram wordt namelijk ook beschouwd als zijnde voor het eerst openbaar gemaakt in een Verdragsluitende Staat, indien de openbaarmaking in de Verdragsluitende Staat plaatsvond binnen dertig dagen na eerste openbaarmaking in een niet-Verdragsluitende Staat. Artikel 5 lid 3 bepaalt dat iedere Verdragsluitende Staat door middel van een kennisgeving kan verklaren dat hij het openbaarmakingscriterium of het vastleggingscriterium niet zal toepassen. Een Staat die vóór het tot stand komen van de Conventie van Rome op 26 oktober 1961 aan producenten van fonogrammen uitsluitend op basis van het vastleggingscriterium bescherming toekent, kan op grond van artikel 17 door middel van een kennisgeving verklaren dat uitsluitend het vastleggingscriterium als toepassingscriterium zal worden aangelegd.[6]

De toepassingscriteria die gelden voor de bescherming van de prestaties van omroeporganisaties, zijn neergelegd in artikel 6 lid 1. Op grond van die bepaling dient een Verdragsluitende Staat uitzendingen van buitenlandse omroeporganisaties en hun rechtverkrijgenden te beschermen, wanneer: (1) het hoofdkantoor van de omroeporganisaties is gelegen op het grondgebied van een andere Verdragsluitende Staat, of (2) de uitzending plaatsvond via een zendinstallatie gelegen op het grondgebied van een andere Verdragsluitende Staat. Artikel 6 lid 2 biedt Verdragsluitende Staten de mogelijkheid om de voornoemde toepassingscriteria cumulatief in plaats van facultatief toe te passen middels een daartoe strekkende kennisgeving.

Artikel 2 schrijft nationale behandeling voor. Dat betekent dat een Verdragsluitende Staat de prestaties van buitenlandse uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties (die voor bescherming in aanmerking komen) op gelijke wijze als die van eigen onderdanen dient te beschermen. De verplichting nationale behandeling te verlenen strekt zich blijkens artikel 2 lid 2 nadrukkelijk niet verder uit dan tot de expliciet in het verdrag voorziene bescherming. Anders dan tot op grote hoogte geldt in het internationale auteursrecht, is er op het gebied van de naburige rechten onder de Conventie van Rome dus geen sprake van een beginsel van volledige gelijkstelling of assimilatie. De internationale erkenning van hun aan-

6 Over de verschillende wijzen waarop daaraan door de vijftien 'oude' lidstaten van de EG invulling is gegeven: Van der Net 2005.

spraken heeft namelijk nog niet het niveau bereikt van die van makers van werken van letterkunde, wetenschap of kunst onder het auteursrecht ingevolge artikel 5 lid 1 van de Berner Conventie.

De vraag die moet worden beantwoord is of uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties aan de Conventie van Rome een recht op een billijke vergoeding voor privé-kopiëren kunnen ontlenen. Goed verdedigbaar is dat dit niet het geval is. De Conventie van Rome voorziet weliswaar ten behoeve van de voornoemde nabuurrechthebbenden in een (vastleggings- en) reproductierecht. Maar de Conventie van Rome laat de Verdragsluitende Staten nadrukkelijk ruimte om in hun nationale wet- en regelgeving te voorzien in een uitzondering op dat recht tot privé-kopiëren (artikel 15 lid 1 onderdeel a). Bovendien schrijft de Conventie van Rome niet voor dat daaraan alsdan beperkende voorwaarden moeten worden gesteld. Het staat een Verdragsluitende Staat natuurlijk vrij de inroepbaarheid van die uitzondering uit hoofde van een andere internationaalrechtelijke verplichting of uit eigen beweging aan stringente voorwaarden te verbinden, waaronder een recht op een billijke vergoeding ter compensatie voor de schade die zij ten gevolge van privé-kopiëren lijden. Op basis van de Conventie van Rome kunnen buitenlandse nabuurrechthebbenden, ook al kwalificeren zij zich voor bescherming door de vervulling van de op hen toegesneden toepassingscriteria, daarop evenwel geen aanspraak maken.

Conventie van Genève

De Conventie van Genève strekt ertoe fonogrammenproducenten te beschermen tegen piraterij van hun fonogrammen. De bezorgdheid over de toenemende mate waarin fonogrammen, zonder voorafgaande toestemming, werden gereproduceerd en gedistribueerd en de daaruit voortvloeiende schade voor fonogrammenproducenten alsmede in hun kielzog auteurs en artiesten was aanleiding voor het sluiten van het Verdrag. Artikel 2 bepaalt dat fonogrammenproducenten moeten worden beschermd tegen (1) het zonder toestemming van de fonogrammenproducent vervaardigen van kopieën, (2) het invoeren van dergelijke kopieën, indien het vervaardigen of invoeren geschiedt met het oog op het afleveren aan het publiek, en (3) het afleveren van dergelijke kopieën aan het publiek. Verdragsluitende Staten hebben een grote discretionaire bevoegdheid ten aanzien van de wijze waarop die bescherming gestalte moet krijgen. Op grond van artikel 3 kan de noodzakelijke bescherming worden gerealiseerd door fonogrammenproducenten naburige rechten te verlenen met betrekking tot fonogrammen. Daarbij kan dan natuurlijk worden gedacht aan het zogenaamde reproductie- en distributierecht. De noodzakelijke bescherming kan echter ook bestaan uit wetgeving op het gebied van de mededinging, terwijl ook strafrechtelijke sancties een met zoveel woorden genoemd middel zijn om het voorgeschreven doel te bereiken. De Conventie van Genève is vooral een anti-piraterijverdrag, waarbij naburige rechten van fonogrammenproducenten een rol

kunnen, maar niet noodzakelijkerwijs behoeven te spelen. Bij de Conventie van Genève zijn inmiddels 76 Staten aangesloten. Nederland is partij sinds 12 oktober 1993.

De Conventie van Genève geeft niet aan wanneer Verdragsluitende Staten geacht worden bescherming te verlenen aan fonogrammen van de producenten die eigen onderdanen zijn. Evenmin bepaalt de Conventie wanneer Verdragsluitende Staten fonogrammen van buitenlandse producenten moeten beschermen. Laat staan dat duidelijk wordt omschreven dat de uitvoeringen van buitenlandse uitvoerende kunstenaars (lees: musici en zangers) ook voor bescherming in aanmerking behoren te komen, wanneer die uitvoeringen zijn vastgelegd op een beschermd fonogram (ofschoon de opstellers in artikel 7 lid 2 wel nadrukkelijk ruimte hebben geschapen om in een dergelijk, ook in artikel 4 onderdeel b van de Conventie van Rome voorkomend toepassingscriterium te voorzien). De Conventie van Genève laat de Conventie van Rome blijkens de preambule niet voor niets nadrukkelijk onverlet. Het ligt dan ook voor de hand dat Verdragsluitende Staten die tevens partij zijn bij de Conventie van Rome in hun nationale wet- en regelgeving aansluiting zullen zoeken bij de in het laatstgenoemde verdrag wel over de volle breedte uitgewerkte regels.

De Conventie van Genève dwingt de daarbij aangesloten Staten niet om meer bescherming te verlenen dan met zoveel woorden is voorgeschreven. De vraag rijst of de Conventie betrekking heeft op de vergoeding die aan de inroepbaarheid van de uitzondering op het reproductierecht voor privékopiëren is verbonden. Het antwoord op die vraag luidt ontkennend. De Conventie van Genève verleent fonogrammenproducenten bescherming tegen de ongeautoriseerde vervaardiging (alsook invoering en aflevering) van ongeautoriseerde kopieën. De kopieën die worden vervaardigd voor eigen oefening, studie en gebruik zijn op grond van de nationale wet- en regelgeving van de Verdragsluitende Staat geoorloofd. Fonogrammenproducenten (en in hun voetspoor allicht ook artiesten) hebben op grond van de Conventie van Genève geen recht op de daaraan dikwijls verbonden vergoedingsaanspraak. De vergoeding compenseert rechthebbenden voor de schade die zij lijden ten gevolge van het op grond van de nationale wet- en regelgeving toegestane privé-kopiëren. De vergoeding is niet bedoeld om rechthebbenden te compenseren voor de schade die zij lijden ten gevolge van piraterij (het zonder de noodzakelijke toestemming vervaardigen van kopieën buiten de scope van de uitzondering voor privé-kopiëren of een andere door de wetgever erkende gebruiksvrijheid).

TRIPs-verdrag

Artikel 14 van het TRIPs-verdrag voorziet in de bescherming van uitvoerende kunstenaars, producenten van fonogrammen en omroeporganisaties. Op grond van artikel 14 lid 1 hebben uitvoerende kunstenaars (lees: artiesten) met betrekking tot de vastlegging van hun uitvoeringen op fonogram-

men de mogelijkheid de volgende handelingen te beletten, wanneer deze worden verricht zonder hun toestemming: (1) de vastlegging van hun niet vastgelegde uitvoering en (2) de reproductie van deze vastlegging. Producenten van fonogrammen genieten uit hoofde van artikel 14 lid 2 het recht de directe of indirecte reproductie van hun fonogrammen toe te staan of te verbieden. Omroeporganisaties hebben onder andere het recht de volgende handelingen te verbieden, wanneer deze worden verricht zonder hun toestemming: (1) de vastlegging en (2) de reproductie van vastleggingen. Bij het TRIPs-verdrag zijn inmiddels 151 staten partij. Nederland is met ingang van 1 januari 1995 bij het TRIPs-verdrag aangesloten.

In het TRIPs-verdrag wordt, anders dan in de Conventie van Rome, niet aangegeven wanneer een Verdragsluitende Partij de prestaties van uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties die zijn onderdanen zijn, in ieder geval dient te beschermen. Omdat TRIPs daaromtrent niets bepaalt, staat het een Verdragsluitende Partij vermoedelijk vrij te bepalen, wanneer uitvoeringen, fonogrammen en uitzendingen van nabuurrechthebbenden die eigen onderdanen zijn, voor bescherming in aanmerking komen als referentiepunt voor het verlenen van nationale behandeling aan vreemden. Voor Verdragsluitende Staten die tevens partij zijn bij de Conventie van Rome, ligt het in de rede om aansluiting te zoeken bij de in het laatstgenoemde verdrag ter zake wel uitgewerkte regels.

Het verdrag bepaalt wel wanneer de prestaties van buitenlandse nabuurrechthebbenden voor bescherming in aanmerking dienen te komen. Op grond van artikel 1 lid 3 TRIPs is dat het geval wanneer wordt voldaan aan de criteria om voor bescherming in aanmerking te komen zoals voorzien in de Conventie van Rome als zouden alle Verdragsluitende Staten daarbij tevens zijn aangesloten (wat niet steeds het geval is). De toepassingscriteria uit de Conventie van Rome moeten met andere woorden worden doorgetrokken naar het verdrag. Dat betekent dat een buitenlandse uitvoerende kunstenaar (of zijn rechtverkrijgende) voor bescherming in aanmerking komt als (1) de uitvoering plaats heeft gevonden in een ander land dat partij is bij het verdrag, (2) de uitvoering is opgenomen op een fonogram dat wordt beschermd op grond van het verdrag, of (3) de uitvoering, die niet is vastgelegd op zo'n fonogram, wordt uitgezonden door middel van een uitzending die wordt beschermd op grond van het verdrag. Duidelijker nog dan onder de Conventie van Rome is dat het hier gaat om de bescherming van live muziek (en niet – al dan niet live – audiovisuele uitvoeringen), omdat het TRIPs-verdrag anders dan de Conventie van Rome slechts de prestaties van artiesten en niet die van acteurs beschermt.

Een buitenlandse fonogrammenproducent (of zijn rechtverkrijgende) komt voor bescherming in aanmerking wanneer: (1) hij onderdaan is van een ander land dat partij is bij het TRIPs-verdrag (nationaliteitscriterium), (2) de eerste vastlegging van de klanken op het fonogram werd verricht in een ander land dat partij is bij het TRIPs-verdrag (vastleggingscriterium), of (3) het fonogram voor het eerst werd openbaar gemaakt in een ander land dat partij is bij het TRIPs-verdrag (openbaarmakingscriterium). Ook de juri-

dische fictie waarmee het openbaarmakingscriterium onder de Conventie van Rome wordt opgerekt, doet onverminderd opgeld onder het verdrag. Op grond van artikel 1 lid 3 TRIPs jº artikel 5 lid 3 van de Conventie van Rome kan een Verdragsluitende Staat door middel van een kennisgeving aangeven dat alleen het vastleggings- of openbaarmakingscriterium in combinatie met het nationaliteitscriterium wordt gebruikt. Omdat in artikel 1 lid 3 van het TRIPs-verdrag – opmerkelijk genoeg – niet wordt verwezen naar artikel 17 van de Conventie van Rome, lijkt het niet toegestaan om de fonogrammen van buitenlandse producenten uitsluitend over de band van het vastleggingscriterium voor bescherming in aanmerking te laten komen (en het nationaliteitscriterium dus geheel buiten beschouwing te laten).

De uitzending van een buitenlandse omroeporganisatie (of haar rechtverkrijgende) wordt beschermd indien: (1) het hoofdkantoor van de omroeporganisatie is gelegen op het grondgebied van een andere, bij het TRIPs-verdrag aangesloten Staat, of (2) de uitzending plaatsvond via een zendinstallatie gelegen op het grondgebied van een andere bij het TRIPs-verdrag aangesloten staat. Evenals onder de Conventie van Rome is het toegestaan de op de buitenlandse omroeporganisatie toegesneden toepassingscriteria cumulatief in plaats van alternatief toe te passen (ex artikel 1 lid 3 van het TRIPs-verdrag jº artikel 6 lid 2 van de Conventie van Rome).

In artikel 3 lid 1 TRIPs wordt nationale behandeling voorgeschreven. De plicht buitenlanders op dezelfde wijze als eigen onderdanen te behandelen is, waar het de bescherming van de prestaties van uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties betreft, beperkt tot de met zoveel woorden in het verdrag verleende naburige rechten. Net zo min als onder de Conventie van Rome is er onder het TRIPs-verdrag dus sprake van volledige assimilatie.

De vraag die moet worden beantwoord is of buitenlandse nabuurrechthebbenden aan het TRIPs-verdrag een aanspraak kunnen ontlenen op de billijke vergoeding voor privé-kopiëren, wanneer hun prestaties worden gereproduceerd voor eigen oefening, studie of gebruik. Het antwoord op die vraag luidt ontkennend. Evenals de Conventie van Rome voorziet het TRIPs-verdrag ten behoeve van uitvoerende kunstenaars, fonogrammenproducenten en omroeporganisaties weliswaar in een (vastleggings- en) reproductierecht. Maar het TRIPs-verdrag laat de Verdragsluitende Staten nadrukkelijk ruimte om in hun nationale wet- en regelgeving te voorzien in een uitzondering voor privé-kopiëren zonder dat daaraan beperkende voorwaarden, laat staan een recht op een (billijke) vergoeding, moeten worden gesteld (artikel 14 lid 6 van het TRIPs jº artikel 15 lid 1 onderdeel a van de Conventie van Rome). Het is waar dat de uitzondering op het reproductierecht voor privékopiëren op grond van artikel 13 van het TRIPs-verdrag in overeenstemming dient te zijn met de driestappentoets op grond waarvan de uitzondering beperkt moet blijven tot een bijzonder geval voor zover daarbij geen afbreuk wordt gedaan aan de normale exploitatie van de beschermde prestaties en de belangen van de rechthebbenden niet op ongerechtvaardigde wijze wor-

den geschaad.[7] Aan die driestappentoets kunnen nabuurrechthebbenden evenwel geen argument ontlenen voor de stelling dat zij door middel van een billijke vergoeding behoren te worden gecompenseerd voor de schade die zij lijden ten gevolge van privé-kopiëren. De driestappentoets is slechts van toepassing op uitzonderingen op het auteursrecht en niet op uitzonderingen op de naburige rechten. Aan het TRIPs-verdrag kan dan ook geen recht op een billijke vergoeding voor privé-kopiëren van nabuurrechtelijk beschermde prestaties worden ontleend.[8]

WPPT

Het WPPT beoogt het bestaande internationaal nabuurrechtelijke instrumentarium in het algemeen en de Conventie van Rome in het bijzonder aan te vullen en te moderniseren om recht te doen aan de snel voortschrijdende technologische ontwikkelingen. Het WPPT heeft, anders dan de Conventie van Rome, uitsluitend betrekking op muziek en niet op film. Het WPPT beschermt in de categorie uitvoerende kunstenaars dus wel musici en zangers maar niet acteurs. Op grond van artikel 6 hebben uitvoerende kunstenaars met betrekking tot hun niet vastgelegde uitvoeringen onder andere het recht de vastlegging ervan toe te staan of te verbieden. Ten aanzien van hun op fonogrammen vastgelegde uitvoeringen hebben uitvoerende kunstenaars op grond van artikel 7 het recht het reproduceren toe te staan of te verbieden. Fonogrammenproducenten beschikken ook over het reproductierecht (artikel 11). Bij het WPPT zijn inmiddels 62 Staten aangesloten. Nederland heeft het verdrag stilzwijgend goedgekeurd en verwacht in de loop van 2008 ook daadwerkelijk te kunnen toetreden.

In het WPPT wordt niet aangegeven wanneer een Verdragsluitende Partij uitvoerende kunstenaars (musici en zangers) en fonogrammenproducenten die zijn onderdanen zijn, dient te beschermen als referentiepunt voor het verlenen van nationale behandeling. Omdat het WPPT daaromtrent niets bepaalt, staat het een Verdragsluitende Partij vermoedelijk vrij te bepalen, daaraan invulling te geven. Zoals hiervoor bij de behandeling van het TRIPs-verdrag, dat op het onderhavige punt geheel met het WPPT correspondeert, al is aangegeven ligt het voor de Verdragsluitende Staten die ook partij zijn bij de Conventie van Rome natuurlijk voor de hand om aan te sluiten bij de in het laatstgenoemde verdrag ter zake wel uitgewerkte regels.

Het WPPT bepaalt wel wanneer de prestaties van buitenlandse nabuurrechthebbenden voor bescherming in aanmerking dienen te komen. Artikel 3 WPPT bevat een op het TRIPs-verdrag gebaseerde oplossing die er in feite op neer komt dat de toepassingscriteria uit de Conventie van Rome van overeenkomstige toepassing worden verklaard met inbegrip van de moge-

7 Over de driestappentoets: Senftleben 2004.
8 Visser 2007 & Van Engelen 2007.

lijkheid om door middel van kennisgevingen aan te geven dat bepaalde criteria in relatie tot de fonogrammenproducent buiten beschouwing worden gelaten. Een buitenlandse uitvoerende kunstenaar (of zijn rechtverkrijgende) komt daarmee voor bescherming in aanmerking als (1) de uitvoering plaats heeft gevonden in een ander land dat partij is bij het WPPT of (2) de uitvoering is opgenomen op een fonogram dat wordt beschermd op grond van het WPPT. De Conventie van Rome bepaalt ook nog dat een buitenlandse uitvoerende kunstenaar ook voor bescherming in aanmerking komt als de uitvoering, die niet is vastgelegd op een dergelijk fonogram, wordt uitgezonden door middel van een uitzending die wordt beschermd op grond van de Conventie van Rome. Dat criterium kan niet van overeenkomstige toepassing zijn. Het WPPT voorziet in tegenstelling tot de Conventie van Rome namelijk niet in de bescherming van uitzendingen van omroeporganisaties. Uitvoerende kunstenaars kunnen dan ook niet via een ingevolge het WPPT beschermde uitzending van een omroeporganisatie voor bescherming in aanmerking komen.[9]

Een buitenlandse fonogrammenproducent (of zijn rechtverkrijgende) komt op grond van artikel 3 WPPT voor bescherming in aanmerking wanneer: (1) hij onderdaan is van een ander land dat partij is bij het WPPT (nationaliteitscriterium), (2) de eerste vastlegging van de klanken op het fonogram werd verricht in een ander land dat partij is bij het WPPT (vastleggingscriterium), of (3) het fonogram voor het eerst werd openbaar gemaakt in een ander land dat partij is bij het WPPT (openbaarmakingscriterium). Een Verdragsluitende Staat kan door middel van een kennisgeving aangegeven dat alleen het vastleggings- of openbaarmakingscriterium in combinatie met het nationaliteitscriterium wordt gebruikt. Ook is onder de in artikel 17 VvR aangegeven voorwaarden toegestaan om uitsluitend het vastleggingscriterium te hanteren.

Het WPPT schrijft evenals de Conventie van Rome en het TRIPs-verdrag nationale behandeling voor. De verplichting zowel eigen als buitenlandse onderdanen identiek te behandelen, geldt op grond van artikel 4 lid 1 WPPT slechts met betrekking tot (1) de uitdrukkelijk toegekende exclusieve rechten en (2) het vergoedingsrecht voor het uitzenden en mededelen aan het publiek van voor handelsdoeleinden uitgebrachte fonogrammen. Derhalve is er net zo min als onder de Conventie van Rome en het TRIPs-verdrag sprake van een volledige gelijkschakeling.

9 In het kader van de Wereldorganisatie voor de Intellectuele Eigendom wordt onderhandeld over een verdrag dat omroeporganisaties beschermt. Mocht dat verdrag ooit tot stand komen – een voor eind 2007 voorziene diplomatieke conferentie moest worden uitgesteld, omdat er ook op hoofdlijnen nog geen duidelijke lijn is uitgekristalliseerd – dan moet het onderhavige toepassingscriterium voor uitvoerende kunstenaars wellicht in verband met dat verdrag worden gelezen. Maar helemaal duidelijk is dat (nog) niet. Zie voor enige alternatieve interpretaties: Fiscor 2002.

Kunnen uitvoerende kunstenaars (artiesten) en fonogrammenproducenten uit hoofde van het WPPT aanspraak maken op een billijke vergoeding voor privé-kopiëren? Voorstanders van een bevestigende beantwoording wijzen er op dat het WPPT ten behoeve van uitvoerende kunstenaars en fonogrammenproducenten in een reproductierecht voorziet. Het WPPT staat er niet aan de in weg dat op dat recht wordt voorzien in een uitzondering voor privé-kopiëren, mits de uitzondering recht doet aan de driestappentoets zoals neergelegd in artikel 16 lid 2 WPPT. Op grond van de driestappentoets moet de uitzondering beperkt blijven tot een bijzonder geval voor zover daarbij geen afbreuk wordt gedaan aan de normale exploitatie van de beschermde prestaties en de belangen van de rechthebbenden niet op ongerechtvaardigde wijze worden geschaad. Als buitenlandse nabuurrechthebbenden geen aanspraak zouden kunnen maken op de aan de inroepbaarheid van de uitzondering voor privé-kopiëren verbonden voorwaarde van een billijke vergoeding ter compensatie van de schade die zij ten gevolge van de uitzondering lijden, dan wordt de driestappentoets met voeten getreden.[10]

Daar staat echter tegenover dat de plicht nationale behandeling te verlenen ex artikel 4 lid 1 WPPT niet verder reikt dan tot de in het verdrag nadrukkelijk toegekende uitsluitende rechten en het met zoveel woorden genoemde vergoedingsrecht voor openbaar muziekgebruik. Uit de totstandkomingsgeschiedenis van die bepaling blijkt duidelijk dat het niet de bedoeling is dat de billijke vergoeding voor privé-kopiëren wordt bestreken door het WPPT. De redactie van artikel 4 lid 1 WPPT werd zelfs aangepast om zulks duidelijker over het voetlicht te brengen en was een belangrijke voorwaarde voor de EG om het verdrag te ondertekenen.[11] De Raad heeft 12 juli 2007 een verklaring afgelegd met gemeenschappelijke uitgangspunten voor de ratificatie van het WPPT, waarin nogmaals wordt gesteld dat buitenlandse nabuurrechthebbenden geen aanspraak op een billijke vergoeding voor privé-kopiëren aan het WPPT kunnen ontlenen.[12] De rechtspolitieke achtergrond van die verklaring behoeft nauwelijks toelichting. Het niveau van bescherming van nabuurrechthebbenden in de EG en de EER ligt, zeker na de omzetting van de richtlijn waaraan rechthebbenden een recht op billijke compensatie voor privé-kopiëren ontlenen, nu eenmaal beduidend hoger dan in andere bij het WPPT aangesloten Staten. Er moet alsdan natuurlijk tegen worden gewaakt dat betalingsstromen ontstaan naar rechthebbenden afkomstig uit laatstgenoemde Staten, zonder dat daar betalingsstromen in omgekeerde richting (van die Staten naar rechthebbenden uit de EG en EER) tegenover staan.

10 Fiscor 2002

11 Reinbothe & von Lewinsky 2002

12 Besluit van de Europese Raad van 12 juli 2007 betreffende gemeenschappelijke uitgangspunten voor de ratificatie van de Wipo-verdragen, 11517/07, PI 34, CULT 37.

Conclusie

Uit het vigerende internationaal nabuurrechtelijke kader kan geen recht op een billijke vergoeding voor privé-kopiëren worden afgeleid. Slechts nabuurrechthebbenden die onderdanen zijn van de EG of EER kunnen daarop aanspraak maken. Zij worden met Nederlanders gelijkgeschakeld vanwege het gemeenschapsrechtelijke verbod te discrimineren op grond van nationaliteit op grond van artikel 12 van het EG-verdrag respectievelijk artikel 4 van het EER-verdrag. Uitvoerende kunstenaars (artiesten en/of acteurs) wier uitvoeringen in Nederland worden gereproduceerd voor eigen oefening, studie of gebruik, hebben recht op de billijke vergoeding als hun uitvoeringen op het grondgebied van de EG of EER (1) hebben plaatsgevonden, (2) worden uitgezonden of (3) voor het eerst zijn vastgelegd. Ook fonogrammenproducenten die rechtspersonen zijn, opgericht naar het recht van een lidstaat van de EG of EER, komen voor die bescherming in aanmerking. Hetzelfde geldt voor omroeporganisaties die hun hoofdkantoor hebben gevestigd in een lidstaat van de EG of EER.

Natuurlijk kunnen Verdragsluitende Staten besluiten om vrijwillig meer bescherming te verlenen dan waartoe zij gelet op het internationale recht zijn gehouden. De Commissie Auteursrecht heeft er terecht op gewezen dat bedacht moet worden dat de in het internationaal nabuurrechtelijk kader voorkomende rechten en reciprociteitsregels de uitkomst van onderhandelingen daarover reflecteren. Hoewel op het eerste gezicht wellicht niet altijd even sympathiek, zijn de regels die nationale behandeling limiteren zowel vanuit juridisch, politiek en economisch perspectief beschouwd nuttige instrumenten om toe te werken naar mondiale oplossingen. Nederland dient behoedzaam om te gaan met het verlenen van voordelen aan andere Staten, zonder dat daartoe een internationaalrechtelijke verplichting bestaat, omdat daardoor de onderhandelingspositie van de Europese Gemeenschap ten opzichte van het buitenland kan worden ondergraven (hetgeen zelfs een inbreuk zou kunnen betekenen op het beginsel van Gemeenschapstrouw zoals neergelegd in artikel 10 EG-verdrag). Dat geldt des te meer, wanneer Nederlanders in het buitenland geen c.q. geen vergelijkbare bescherming genieten.[13]

Het gerechtshof te Amsterdam had geheel in lijn met het vigerend internationaal nabuurrechtelijk kader besloten dat Amerikaanse uitvoerende kunstenaars, zowel artiesten als acteurs, geen recht hebben op de billijke vergoeding voor privé-kopiëren.[14] Het is echter zeer de vraag of het hof aldus op basis van het vigerende nationale recht kon beslissen.[15] A-G Strikwerda concludeerde daarom ook tot vernietiging van het bestreden arrest.[16]

13 Advies van de Commissie Auteursrecht over de ratificatie van het Uitvoeringen- en fonogrammenverdrag en de verwerking daarvan in de toepassingscriteria van de Wet op de naburige rechten van 17 januari 2003, p. 7-8.

14 Hof Amsterdam 17 september 2007, *iept* 20070913 m.nt. D. van Engelen.

15 Van der Net 2008b.

16 De uitleg van de "scope rule", www.boek9.nl, B9 8162.

Of de Hoge Raad het arrest van het hof dan ook geheel of gedeeltelijk zal vernietigen was op het moment dat deze bijdrage werd afgerond niet bekend. Mocht dat echter het geval zijn, dan zal de wetgever – als de thuiskopieregeling niet wordt afgeschaft – moeten overwegen het nationale recht aan te passen aan de daadwerkelijk aangegane internationale verplichtingen. Anders betalen Nederlandse consumenten te veel (omdat ook Amerikaanse nabuurrechthebbenden worden gecompenseerd voor privé-kopiëren) of krijgen Nederlandse nabuurrechthebben te weinig (omdat de vergoeding voor privé-kopiëren ook met Amerikaanse nabuurrechthebbenden moet worden gedeeld). En dat is, either way, vanuit rechtseconomisch en -politiek perspectief beschouwd natuurlijk geen goede wetgeving.

Verwijzingen

Van Engelen 2007
D. van Engelen, noot bij het arrest van Hof Amsterdam 17 september 2007, *iept* 20070913.

Fiscor 2002
M. Ficsor, *The Law of Copyright and the Internet, The 1996 WIPO Treaties, their Interpretation and Implementation*, New York, 2002, p. 614.

Van der Net 2005
C.B. van der Net, 'De ratificatie van het WPPT door de EG en de lidstaten (deel 1): nationale behandeling, materiële wederkerigheid een toepassingscriteria op het gebied van de naburige rechten', in: *AMI* 2005/3, p. 81-86.

Van der Net 2008a
C.B. van der Net, 'Geen privé-kopie-vergoeding voor buitenlandse nabuurrechthebbenden naar internationaal recht', in: *AMI* 2008/3, p. 61-65.

Van der Net 2008b
C.B. van der Net, 'Amerikaanse uitvoerende kunstenaars en de billijke vergoeding voor privékopiëren', in: *AMI* 2008/5, p. 129-135.

Reinbothe & von Lewinsky 2002
J. Reinbothe and S. von Lewinsky, *The WIPO Treaties 1996, The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, Commentary and Legal Analysis*, London, 2002.

Schmidt, Dolfsma & Keuvelaar 2007
A. Schmidt, W. Dolfsma and W. Keuvelaar, Fighting the war on filesharing, Information Technology & Law Series, Cambridge University Press, 2007.

Senftleben 2004
M. Senftleben, *Copyright, limitations and the three-step test. An analysis of the Three-Step test in International and EC Copyright Law*, Information Law Series 13, Den Haag: Kluwer Law International 2004.

Visser 2007
D.J.G. Visser, 'Thuiskopievergoeding ook voor buitenlanders van buiten Europa', in: *AMI* 2003/3, p. 90.

File sharing bedreigt handhaving auteursrecht

Leonie Siemerink■

Inleiding

De oratie van Aernout Schmidt draagt de titel: 'Bedreigen computers ons rechtssysteem?'.[1] Voor wat betreft het auteursrecht is dit zeker het geval. Computers, in het bijzonder de mogelijkheden van file sharing, bedreigen het auteursrecht. Handhaving van auteursrechten en naburige rechten op internet lijkt met de komst van *peer to peer* (P2P)-ruilnetwerken onmogelijk geworden.

Door dematerialisering – informatie is niet tastbaar (op een fysieke informatiedrager geplaatst) maar digitaal – heeft het auteursrecht een andere dimensie gekregen. De digitale vorm biedt voordelen qua kwaliteit en techniek en het is eenvoudig om via internet digitale bestanden (wereldwijd) te verspreiden. Regels die handhaving van auteursrecht op bijvoorbeeld muziek reguleren zijn geschreven vanuit de gedachte dat de muziek op een cd, cassette of lp (fysieke gegevensdrager) staat. Dat de auteursrechtelijk relevante handelingen verspreiden en kopiëren op grote schaal vanuit de huiskamer gebeuren, maakt handhaving van auteursrechten in een digitale omgeving lastig.

P2P-netwerken zijn een juridisch gezien belangrijke ontwikkeling. P2P-technologie is net zo oud als het internet zelf, maar het gebruik van deze techniek is het laatste decennium substantieel toegenomen. Bij P2P kunnen individuele gebruikers zelfstandig informatie aanbieden, maar ook informatie vinden en downloaden van andere individuele gebruikers. De bekendste vorm van P2P-verkeer is het uitwisselen van muziekbestanden in het gecomprimeerde MP3-formaat. Omdat met behulp van P2P-netwerken veelvuldig muziek en films zonder toestemming van de rechthebbende beschikbaar worden gesteld, ligt P2P-verkeer voortdurend onder vuur van muziek- en filmindustrie en van de autoriteiten.

Wanneer een houder van een P2P-netwerksite via een Internet Service Provider (ISP) is te achterhalen en juridisch is aan te spreken, is het kwaad al geschied. Nu gebruikers van die betreffende site gebruik zullen gaan maken van andere (in het buitenland gehoste) sites die nog niet zullen zijn gewraakt, zal het kwaad blijven geschieden. P2P-netwerken zijn niet tegen te houden en zullen zich verder ontwikkelen. Problemen die voorheen ook al beston-

---

■ Leonie Siemerink is gerechtsauditeur bij de Hoge Raad der Nederlanden. Deze bijdrage is geschreven op persoonlijke titel en afgesloten in augustus 2009.

1 Schmidt 2004.

den, worden op internet zoveel groter, dat het niet alleen kwantitatief maar ook kwalitatief andere problemen worden.[2]

In het boek 'Fighting the War on File Sharing' besteedt Schmidt aandacht aan P2P-netwerken en de problemen die file sharing meebrengt voor de handhaving van het auteursrecht.[3] In deze bijdrage aan het liber amicorum voor Schmidt ga ik vanuit de ISP bezien nader in op de vraag of handhaving van auteursrechten op internet nog mogelijk is.[4]

ISP's

Vragen betreffende privaatrechtelijke aansprakelijkheid voor onrechtmatige gedragingen op internet richten zich vaak op de positie van de ISP. Oorzaak hiervan is dat op internet veelal niet direct te achterhalen zal zijn welke persoon achter een onrechtmatige gedraging zit en waar hij zich bevindt. De ISP is dan logischerwijs degene waarop de ogen zich richten, omdat deze daarmee wel bekend is. In de praktijk gaat het bij aansprakelijkheid voor onrechtmatige gedragingen van klanten van ISP's vaak om inbreuk op intellectuele eigendomsrechten of portretrecht.[5]

Een ISP kan in mijn opvatting vier functies verrichten: *access*, *hosting*, *extra value* en *content*.[6] Access is het aan een klant de technische faciliteit verschaffen om via het systeem van de ISP toegang te verkrijgen tot het internet (de dienst internettoegang). Hosting is het aan een klant de mogelijkheid verschaffen om op de ISP-server(s) bepaalde informatie van en voor derden toegankelijk te maken. De internetdiensten die hieronder vallen zijn: website, e-mail, nieuwsgroep en chat. Extra value betreft het verrichten van diensten die een meerwaarde betekenen voor de klant ten opzichte van access en hosting. Een ISP kan bijvoorbeeld op verzoek van een klant een domeinnaam registreren of zijn klant de mogelijkheid bieden om voor ondersteuning gebruik te maken van een helpdesk. Onder extra value wordt ook begrepen de mogelijkheid om klachten over onrechtmatige informatie te kunnen deponeren, informatie te filteren of anti-virussoftware en filterprogrammatuur ter beschikking te stellen. Het aanbieden van content betreft het aanbieden van inhoudelijke informatie op het internet. In dit geval gaat het om informatie afkomstig van de ISP zelf. De inhoud, het ontwerp, de

2 Zie Van der Linden 2008. Zie ook brief van het Ministerie van Justitie, Directoraat-Generaal Rechtspleging en Rechtshandhaving, aan de tweede kamer van 14 april 2008 over Rechtshandhaving en internet en beleidsbrief auteursrecht van 20 december 2007, *Kamerstukken II* 2007-08, 29 838, nr. 6.

3 Schmidt, Dolfsma & Keuvelaar 2007.

4 Deze bijdrage is grotendeels ontleend aan Siemerink 2008.

5 Zie bijvoorbeeld Vzr. Rb Amsterdam 1 november 2007, LJN: BB6926; tevens in Computerrecht 2008/1 nr. 8, m.nt. Chr.A. Alberdingk Thijm en in Mediaforum 2008/1, nr. 3, m. nt. K.J. Koelman (Prins Willem-Alexander c.s./Vereniging Martijn).

6 Zie Siemerink 2007, p. 11-23.

inrichting en de ordening van informatie op de portal-site dan wel website van de ISP vallen onder de verantwoordelijkheid van de ISP.

Art. 6:196c BW gaat over de vraag wanneer een ISP een hem toerekenbare bijdrage heeft geleverd aan verspreiding van informatie en hij daardoor aansprakelijk kan worden gehouden. In het eerste en tweede lid zijn vrijwaring van aansprakelijkheid voor *mere conduit* (de ISP fungeert als 'doorgeefluik') neergelegd. In het derde lid is vrijwaring van aansprakelijkheid voor *caching* (wijze van opslag) neergelegd.[7] Deze zijn met betrekking tot de aansprakelijkheidspositie van de ISP bij het uitoefenen van de functie access van belang. In het vierde lid is vrijwaring van aansprakelijkheid voor *hosting* neergelegd. Deze is van toepassing op de functie hosting, met uitzondering van de dienst e-mail. In het vijfde lid wordt uiteengezet dat de mogelijkheid onverlet wordt gelaten een rechterlijk verbod of bevel ten aanzien van de (potentieel) schadetoebrengende informatie te verkrijgen. Voorwaarde is wel dat de ISP daartoe redelijkerwijs in staat is. Dat is het geval wanneer hij in een contractuele relatie staat met de persoon die verantwoordelijk is voor de inhoud van de schade toebrengende informatie.

De vrijwaringen bij het verrichten van access die uitsluitend is gericht op mere conduit respectievelijk hosting beschermen ISP's tegen aansprakelijkheid voor schade die het gevolg is van het onrechtmatige karakter van informatie, met inbegrip van hyperlinks of interactieve verwijzingen, afkomstig van een ander, klant dan wel derde (de informatieverschaffer). De ISP's zijn bij het verrichten van access die uitsluitend is gericht op mere conduit respectievelijk hosting onder voorwaarden gevrijwaard van aansprakelijkheid ten opzichte van degene die ten gevolge van de onrechtmatige informatie schade heeft geleden.

Van de ISP die de functie hosting uitoefent, wordt verwacht dat hij 'prompt handelt' om de onrechtmatige informatie van zijn systeem te verwijderen of de toegang daartoe onmogelijk te maken zodra hij van die informatie kennis heeft. Een ISP die van een klant afkomstige informatie opslaat (hosting), is doorgaans in staat adequaat op te treden tegen de bij hem opgeslagen informatie. Dit is anders bij de ISP die de functie access alleen gericht op mere conduit uitoefent, en er wel weet van heeft dat zijn systemen worden gebruikt voor het uitvoeren van onrechtmatige activiteiten, maar geen maatregelen lijkt te hoeven nemen om daaraan een einde te maken. De ratio voor de uitsluiting van de aansprakelijkheid bij mere conduit is dat hetgeen de ISP in dat geval doet een louter technisch, automatisch en passief karakter heeft. Dat veronderstelt dat hij kennis van, noch controle over de informatie heeft die wordt doorgegeven.[8] Het belang van wijdverbreide internettoegang heeft de wetgever hier vooropgesteld.

---

7 Caching dient niet te worden gezien als een activiteit van een ISP. Het is niets anders dan een technische handeling. Een ISP installeert een proxy-server en zet deze aan. Wat het auteursrecht betreft is hier sprake van een tijdelijke reproductie dan wel een technische reproductie handeling, zie art. 13a AW.

8 *Kamerstukken II* 2001-02, 28 197, nr. 1-3, p. 26.

Art. 6:196c BW biedt een ISP niet voldoende houvast. Op het moment dat ISP's geen aanspraak kunnen maken op een vrijwaring uit art. 6:196c BW staat daarmee nog niet vast dat ze ook aansprakelijk zijn. En inmiddels is de technische achtergrond waartegen deze regeling tot stand is gekomen in die mate veranderd dat deze regeling niet meer tot tevredenstellende uitkomsten leidt. Wanneer een ISP geen aanspraak kan maken op een vrijwaring van aansprakelijkheid zoals neergelegd in art. 6:196c BW moet de vraag of, en zo ja in hoeverre, een ISP aansprakelijk kan worden gesteld, worden beantwoord aan de hand van het algemene leerstuk van de onrechtmatige daad. De vraag welke mate van zorg in de gegeven omstandigheden van de ISP kan worden gevergd ten aanzien van de belangen van derden staat daarbij centraal. In het algemeen wordt aangenomen dat de mate van zorg die in het maatschappelijke verkeer bij het verrichten van een bepaalde activiteit betaamt, in het bijzonder afhankelijk is van: de aard en de omvang van de schade die als gevolg van de activiteit kan worden verwacht, de mate van waarschijnlijkheid dat deze schade zal optreden, de aard en het maatschappelijke nut van de activiteit en de mate van bezwaarlijkheid van het nemen van voorzorgsmaatregelen.[9] Het feit dat een ISP een belangrijke functie vervult in de publieke informatievoorziening (beschikbaarheid) zal in de meeste gevallen behoren tot de relevante omstandigheden van het geval.

Verschillende factoren hebben invloed op de aansprakelijkheidspositie van de ISP in het geval van auteursrechtinbreuken: de mate van betrokkenheid van de ISP bij de inhoud van de inbreuk; de mate waarin de ISP redelijkerwijs controle op en zeggenschap over de inbreuk kan uitoefenen, waarbij ook technische belemmeringen en mogelijkheden een rol kunnen spelen; de wijze waarop de ISP zich profileert tegenover het publiek of de klanten, waarbij kan worden gedacht aan bepaalde uitlatingen over aard, kwaliteit of betrouwbaarheid van de informatie.

P2P-netwerken

Een P2P-netwerk, bijvoorbeeld BitTorrent, werkt als volgt. Op een BitTorrent website worden hyperlinks naar torrentbestanden aangeboden van onder andere films, muziek en software (de werken). Torrentbestanden bevatten zelf geen auteursrechtelijk beschermd materiaal maar coördineren het downloaden via het P2P-systeem BitTorrent. Middels deze software is het mogelijk om muziekalbums of films in korte tijd binnen te halen op de computer. De persoon die deze 'down- en uploadwebsite' in stand houdt is de websitehouder die een overeenkomst heeft met een ISP. De ISP verbindt de server waarop de website draait met internet. De ISP kan daarbij als host voor de

9 Zie HR 5 november 1965, *NJ* 1966, 136, m.nt. G.J.S (Kelderluik).

websitehouder fungeren of enkel de dienst access verlenen.[10] Door deze torrentbestanden te downloaden wordt het voor de gebruiker van de website mogelijk verbinding te maken met de computers van andere gebruikers. De werken (of delen daarvan) worden vervolgens vanaf de computers van die andere gebruikers gedownload en daarna vanaf de computer van de gebruiker weer geupload, zodat zij ter beschikking komen van weer andere gebruikers die de bestanden willen downloaden.

Er kunnen zodoende twee verschillende soorten ISP-klanten worden onderscheiden. Een klant van de ISP kan ten eerste gebruiker van een P2P-netwerk zijn. De klant gebruikt dan P2P-software om te up- en downloaden. Ten tweede kan een klant van de ISP een aanbieder van een P2P-netwerk zijn. De klant is dan eigenaar van een P2P-site, bijvoorbeeld een hierboven beschreven BitTorrent-site. Wat betreft de P2P websitehouder verschilt de mate van betrokkenheid van de ISP indien de klant gebruik maakt van access of hosting.

Het auteursrecht en P2P-netwerken

Als zonder toestemming van de auteursrechthebbende een werk wordt verveelvoudigd of openbaar gemaakt, is sprake van inbreuk op het auteursrecht[11] (art. 1 jº. 12-14 AW).[12] Downloaden via P2P-netwerken van muziek en films voor thuisgebruik (thuiskopie), zonder commercieel oogmerk, mag in Nederland (art. 16 c t/m g AW).[13] Deze thuiskopie-exceptie is ontstaan vanuit het oogpunt dat handhaving van auteursrechten bij consumenten thuis niet mogelijk is. Wanneer een consument bijvoorbeeld een kopie van een cd van hem op een cassettebandje maakt, is het niet mogelijk dit te controleren. Daarnaast vindt het in de privésfeer plaats zodat daar het recht op privacy geldt. De exceptie is ontstaan vanuit het oogpunt van kopiëren op fysieke dragers en geldt nu dus ook voor downloaden van muziek.[14] Commercieel oogmerk wil zeggen dat je er economisch gewin uit behaalt. Wanneer een internetgebruiker een film gratis downloadt zodat hij deze niet hoeft te huren

10 Zie Vzr. Rb. 's-Gravenhage 5 januari 2007, LJN: AZ5678, Computerrecht 2007, m.nt. L.A.R. Siemerink, p. 108-113 (Brein/KPN).

11 Of naburig recht, zie Wet op de naburige rechten.

12 Vindt deze op grootschalige en/of georganiseerde wijze plaats, dan is sprake van digitale piraterij (internetpiraterij); het illegaal uploaden van auteursrechtelijk en nabuurrechtelijk beschermd materiaal. Zie *Kamerstukken II* 2007-08, 29 838, nr. 6, p. 8-9.

13 Anders: Rb 's-Gravenhage 25 juni 2008, rolnr. 246698, HA ZA 05-2233 (Importeurs en/of fabrikanten blanco informatiedragers/Thuiskopie), raadpleegbaar via Boek9.nl, B9 6341. De rechtbank stelt voorop (rov. 4.4.3) dat het maken van een privekopie van illegaal materiaal een illegale handeling is die niet onder de werkingssfeer van art. 16c Aw valt. Maar tevens oordeelt de rechtbank (rov. 4.4.4) dat bij de vaststelling van de hoogte van de thuiskopievergoeding wel rekening mag worden gehouden met privekopieën van illegaal materiaal.

14 Zie ook het rapport van de Parlementaire Werkgroep Auteursrecht, 2009, raadpleegbaar via B9 7973.

of ervoor naar de bioscoop hoeft te gaan, biedt dat economisch gewin, maar is geen sprake van een commercieel oogmerk. Wanneer de betreffende film nog niet in de Nederlandse bioscopen draait en dus ook nog niet te huur dan wel te koop is op DVD weet, dan wel behoort een internetgebruiker te weten dat hij moreel gezien niet juist bezig is. Het probleem is dat dit niet te bewijzen en ook niet te handhaven is.

Al kent het auteursrecht enig respijt voor de thuiskopiist, bestanden uploaden is verboden. Een thuiskopie mag niet aan iemand anders worden gegeven. Alleen downloaden zonder te uploaden, is mogelijk bij sommige P2P-programma's, maar vaak kan downloaden alleen als de internetgebruiker ook uploadt en dus illegaal bezig is. Dat geldt bijvoorbeeld bij BitTorrent.[15] Een internetbestand met muziek of film downloaden mag als dat zonder direct of indirect commercieel oogmerk gebeurt en de download uitsluitend voor eigen gebruik is. Het downloaden van illegaal gekopieerde muziek is zodoende in Nederland toegestaan.[16] Software mag niet worden gekopieerd, ook niet voor eigen gebruik (art. 45n AW). Downloaden van illegaal en legaal gekopieerde software is zodoende niet toegestaan.[17] Uitgezonderd hiervan zijn open source software en free software.

ISP's en P2P-netwerken

ISP's zijn genoodzaakt mee te werken aan de bestrijding van vermeende wetsovertredingen.[18] Een ISP moet het belang van een auteursrechthebbende op naleving van zijn rechten voor ogen hebben, maar tegelijkertijd dient hij ook de privacy van zijn klanten te bewaken. Stichting Brein[19] gaat namens veel rechthebbende auteurs, uitvoerend kunstenaars, uitgevers, producenten en distributeurs de strijd aan met inbreuken op intellectuele eigendomsrechten op muziek, films, video's en interactieve software. Een ISP komt in een lastige positie te verkeren wanneer hij wordt gedwongen een klacht over onrechtmatig handelen van zijn klant te beoordelen, niet in de laatste plaats omdat de vraag of in het betrokken geval sprake is van onrechtmatig handelen zeer complex kan zijn. Hij voelt zich tussen twee vuren zitten, dat van Stichting Brein en dat van zijn klant. Een ISP wil en/of kan informatie waarover wordt geklaagd niet inhoudelijk beoordelen. Hij opereert slechts als

15 Zie Rietjens 2006.

16 Zie MvT, *Kamerstukken II* 2001-02, 28 482, nr. 3, p. 20-26 en 45-48. Zie ook Visser 2001, p. 132 en Wichers Hoeth 2007, p. 477. Anders: Seignette 2001, p. 32.

17 Software kan overigens online worden gekocht waartoe het vervolgens moet worden gedownload om er de beschikking over te krijgen. Dan is sprake van legaal online aangeschafte software.

18 Zie Rb 's-Gravenhage 9 juni 1999, LJN: AA1039 (Scientology/XS4ALL) en Gerechtshof Amsterdam 7 november 2002, LJN: AF0091 (XS4ALL/Deutsche Bahn). Zie ook Vzr. Rb Utrecht 12 juli 2005, NJ 2005, 387, LJN: AT9073 en hof Amsterdam 13 juli 2006, LJN: AY3854 (Brein c.s./5 ISP's). Zie tevens Vzr. Rb Amsterdam 24 augustus 2006, LJN: AY6903 (Brein/UPC).

19 Stichting Bescherming Rechten Entertainment Industrie Nederland, zie www.anti-piracy.nl.

tussenpersoon. Pas indien er een rechterlijk vonnis is gewezen, kan een ISP zeker zijn van de onrechtmatigheid van informatie.

Uit een uitspraak van het Hof van Justitie van de Europese Gemeenschappen kan worden opgemaakt dat EU-landen niet verplicht zijn om van ISP's te eisen dat ze naam, adres en woonplaats (NAW-gegevens) van muziek- en filmruilers (P2P-gebruikers) voor civiele zaken afdragen aan de waakhonden van de muziek- en filmindustrie (in Nederland Stichting Brein) om auteursrecht te handhaven.[20] In Nederland was er al het arrest van de Hoge Raad in de zaak Lycos/Pessers.[21] In dat arrest is bevestigd dat er aanleiding kan zijn een ISP te veroordelen NAW-gegevens bekend te maken indien onrechtmatig zou kunnen zijn gehandeld, daardoor schade kan zijn geleden en er geen minder ingrijpende manier is om achter de NAW-gegevens te komen. Vervolgens dient dan nog een belangenafweging plaats te vinden tussen het privacybelang van de klant en het belang van de rechthebbende. De uitspraak van het Europese Hof van Justitie bracht daarom voor Nederland niets nieuws.

Er heerst onduidelijkheid over de vraag wat een ISP precies moet doen wanneer hij in kennis is gesteld van de openbaarmaking van onrechtmatige informatie via zijn systemen. Volgens art. 6:196c lid 4 BW, dat betrekking heeft op hosting, kan de ISP ervoor kiezen de informatie te verwijderen dan wel de toegang daartoe onmogelijk te maken.[22] Door de betreffende informatie te verwijderen kan de ISP schade toebrengen aan zijn klant, terwijl later alsnog kan komen vast te staan dat geen sprake is geweest van onrechtmatige informatie. Omdat de ISP ook aan de belangen van zijn klant moet denken – hij heeft met hem immers een contractuele relatie – zal hij er veelal verstandig aan doen hooguit de toegang tot de vermeende inbreukmakende informatie te blokkeren, totdat definitief duidelijk is of wel of geen sprake is van onrechtmatige informatie. In de praktijk zal vaak niet direct duidelijk zijn of wel of geen sprake is van een inbreukmakende handeling, zodat een ISP tussen twee kwaden dreigt te moeten kiezen. De ISP die de informatie niet ontoegankelijk maakt, riskeert aansprakelijkheid uit hoofde van onrechtmatige daad. De ISP die de informatie wel ontoegankelijk maakt, riskeert een vordering van zijn klant wegens wanprestatie. Bovendien zullen ISP's bang zijn hierdoor hun klanten te verliezen omdat zij overstappen naar andere ISP's die minder snel informatie ontoegankelijk maken. Een ISP heeft zodoende te maken met twee aansprakelijkheden; aansprakelijkheid voor wat zijn klanten doen en aansprakelijkheid tegenover zijn klanten.

Het probleem doet zich voor dat klanten van ISP's door middel van P2P-netwerken muziek dan wel films downloaden en uploaden en hiermee auteursrechten schenden. Het is een ISP die zijn klanten door middel van een overeenkomst de diensten access en hosting aanbiedt waardoor zij

20 HvJEG 29 januari 2008, C-275/06 (Promusicae/Telefónica de Espaáa SAU).

21 HR 25 november 2005, LJN: AU4019; RvdW 2005, 133 (Lycos/Pessers).

22 Informatie van het internet verwijderen is in wezen onmogelijk, zie bijvoorbeeld Vzr Rb Dordrecht 15 februari 2007, LJN: AZ8818. Zie ook www.archive.org.

gebruik kunnen maken van P2P-netwerken. Een ISP maakt zodoende een wezenlijk onderdeel uit van het faciliteren van P2P-netwerken.[23] Sommige ISP's adverteren ook met teksten dat via hun abonnementen nu nog sneller films en muziek kunnen worden gedownload. De wijze waarop een ISP zich profileert tegenover het publiek en zijn klanten speelt zodoende een rol bij de vaststelling van zijn aansprakelijkheid.[24]

Oplossingsrichtingen

Op grond van art. 11.3 van de Telecommunicatiewet rust op ISP's, aanbieders van openbare telecommunicatiediensten, een zorgplicht. Dit betekent dat zij maatregelen moeten treffen voor een veilig gebruik van hun netwerk. Ook zijn zij verplicht hun klanten goede voorlichting te geven over de mogelijke gevaren en risico's van het gebruik van het netwerk. Het is echter niet duidelijk hoe ver deze zorgplicht gaat. Op grond van deze zorgplicht kan mijns inziens van de ISP een informatieplicht worden gevergd die inhoudt dat ISP's hun klanten wijzen op en bewust maken van de werking van het auteursrecht en handhaving daarvan op internet. ISP's zouden moeten beginnen verantwoording te nemen voor content. Door de mogelijkheid die een consument heeft om een breedband-internetovereenkomst af te sluiten wordt P2P-gebruik en daarmee auteursrechtinbreuk immers door ISP's gestimuleerd. Er kan daarom een beroep worden gedaan op ISP's omdat zij de partij zijn die het plegen van auteursrechtinbreuk mede faciliteren. Dit beroep kan echter niet verder gaan dan klanten informeren en waarschuwen omdat lidstaten op grond van art. 15 van de Richtlijn inzake elektronische handel[25] dienstverleners geen algemene verplichting mogen opleggen om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onrechtmatige activiteiten duiden.

In ISP-maatregelen zoals de uploader eerst een waarschuwing geven en na herhaling de toegang tot bijvoorbeeld e-mail en internetbankieren blokkeren, kan ik mij niet vinden. Ten eerste wordt de kern van het probleem hier niet mee aangepakt en ten tweede wordt een ISP belast met uitvoeringstaken (het blokkeren van internetdiensten) waar hij wel toe in staat is, maar waarbij het recht op toegang tot informatie wordt geschonden. Het afsluiten van een internetverbinding, zoals in Frankrijk is voorgesteld om bij wet te regelen maar door de constitutionele Raad (gelukkig) is tegengehou-

23 Zie ook P.B. Hugenholtz in zijn noot onder HR 19 december 2003, (Buma/KaZaA) *AMI* 2004/1, p. 24.

24 Zie ook Hof Amsterdam 15 juni 2006, *LJN* AX7579, NJF 2006, 427, *AMI* 2006/5, 173 m.nt. K.J. Koelman (Brein/Techno Design).

25 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG* L178 van 17 juli 2000.

den, vind ik zeer vergaand.[26] Internetgebruik is inmiddels zo'n belangrijk onderdeel van ons dagelijks leven geworden dat afsluiting niet op een dergelijke grond kan en mag plaatsvinden.

Wanneer er een klacht binnenkomt, kan een Nederlandse ISP op grond van de huidige wetgeving niet anders dan informatie beoordelen op onrechtmatigheid. Wanneer de ISP dat niet doet en de informatie eenvoudig doorleidt, ontstaat er een zekere mate van *chilling effect* ten aanzien van de klant.[27] Een *abuse* e-mail-adres waar internetgebruikers met klachten over misbruik via de desbetreffende ISP – bijvoorbeeld verspreiding van auteursrechtinbreukmakende informatie – terechtkunnen, kan een oplossing bieden. Hiervoor moet dan een goed protocol worden opgemaakt; alleen zeggen dat er iets verdachts plaatsvindt, is niet voldoende. Nederlandse ISP's moet ruimte worden geboden om een standaardprocedure te hanteren voor het afwikkelen van binnenkomende klachten. Een meldingsformulier waarop de klager met behulp van een questionnaire moet aangeven waarom de informatie volgens hem onrechtmatig is, moet daarvan onderdeel uitmaken. Een ISP heeft tijd nodig om een afweging te maken en mag dat ook.[28] Daartoe kan een ISP in contact treden met de desbetreffende klant.

Een goede oplossing vind ik een 'notice and take down'-procedure (NTD procedure) voor ISP's die access en hosting bieden.[29] Daarmee kan de handhaving van auteursrechten beter worden gerealiseerd. Een NTD-procedure houdt kort gezegd het volgende in. De ISP ontvangt van een auteursrechthebbende die claimt dat zijn rechten worden geschonden een verzoek tot blokkering van vermoedelijk auteursrecht-inbreukmakende informatie en vervolgens wordt de informatie geblokkeerd door de ISP. Het maakt niet uit of aan die claim kan worden getwijfeld. Daarna zorgt de ISP dat de klant hiervan op de hoogte wordt gebracht en vraagt aan de klant een reactie. Geeft de klant een reactie en zegt hij bijvoorbeeld dat geen sprake is van auteursrechtinbreuk, dan zal de ISP proberen deze twee partijen met elkaar in contact te brengen. De ISP fungeert als tussenpersoon. Hij zorgt voor het contact maar hoeft op dat moment geen oordeel te vellen over de (on)rechtmatigheid van de informatie.

Wanneer de ISP aan de hand van de ontvangen klacht twijfelt over de (on)rechtmatigheid van de informatie dient de informatie online te blijven totdat een rechter hierover heeft beslist. ISP's moeten klachten altijd doorsturen aan de desbetreffende klant en een redelijke termijn hanteren voor het geven van antwoord aan de indiener van de klacht. Blijft een reactie van de klant uit, dan zou een ISP alleen moeten ingrijpen als hij onmiddellijk gevaar,

---

26 Ook op Europees niveau wordt momenteel over een dergelijk voorstel nagedacht.

27 Zie ook Schellekens 2001, p. 63.

28 Zie *Kamerstukken II* 2001-02, 28 197, nr. 1-3, p. 25-28.

29 In artikel 14 lid 3 van de Richtlijn inzake elektronische handel wordt de mogelijkheid tot aanvullende nationale wetgeving uitdrukkelijk geboden. Zie ook De Jongh & Siemerink 2002, p. 12-20. Over 'notice and take down' zie ook Julia-Barcelo 1998, p. 461-462 en Schellekens 2001, p. 236-238.

onmiskenbare onrechtmatigheid of aantoonbare grote financiële schade verwacht. Het hangt geheel van de omstandigheden van het geval af of een ISP door de rechter wordt verplicht om persoonsgegevens af te staan. Wanneer de ISP aan de hand van een ontvangen klacht twijfelt over het verschaffen van persoonsgegevens, dienen deze niet te worden verstrekt totdat een rechter hierover heeft beslist. Transparantie is met betrekking tot deze onderwerpen cruciaal. ISP's moeten de reeds door hun gehanteerde NTD-procedure publiceren. Statistieken over notice and take down en gevolgen daarvan kunnen het probleem beter onder de aandacht brengen en leiden tot een wenselijke oplossing.

De rol van een ISP moet mijn inziens worden beperkt tot informatie verwijderen dan wel blokkeren, en het verschaffen van persoonsgegevens wanneer een rechter hem dit oplegt (art. 6:196c lid 5 BW) of wanneer dit in de wet is bepaald. Hiertoe zou een wettelijke NTD-procedure in het leven kunnen worden geroepen om meer duidelijkheid en rechtszekerheid te verkrijgen. Daarin kan een wettelijke vrijwaring voor ISP's worden gerealiseerd wanneer een ISP wordt verzocht informatie te verwijderen en/of persoonsgegevens te verschaffen. Zelfregulering in de vorm van een klachtenprocedure en/of een regeling in de algemene voorwaarden is niet voldoende omdat derden zich er niet aan hoeven te houden. Het instellen van een meldpunt dat een oordeel velt over de inhoud van de informatie acht ik niet realiseerbaar.[30] Technisch gezien kan een dergelijk meldpunt 24 uur per dag bereikbaar zijn. Juridisch gezien zie ik het echter als een probleem wie deel moeten uitmaken van het meldpunt om de informatie te beoordelen en hoe (snel) een oordeel dient te worden geveld. In de praktijk is behoefte aan een uniforme, transparante wettelijke NTD-procedure.

Afsluitend

Het antwoord op Schmidts oratievraag of computers ons rechtssysteem bedreigen luidt voor wat betreft het auteurs recht volmondig ja. P2P-netwerken bedreigen de handhaving van auteursrechten op internet. Ik zou zelfs zo ver willen gaan dat het niet enkel meer bij bedreigen is gebleven maar dat er daadwerkelijk een ommekeer is ontstaan. Digitalisering heeft het auteursrecht een andere dimensie gegeven. Klanten van een ISP kunnen door middel van gebruik van P2P software auteursrechtelijk beschermde werken uploaden en downloaden. Daarnaast kunnen klanten van een ISP websitebeheerder zijn van een P2P-netwerksite. Om handhaving van auteursrechten op internet niet onmogelijk te maken is het van belang de rol van de ISP

30 Zie hierover Schellekens 2001, p. 239-242 en Julia-Barcelo Koelman 2000, p. 237. Een meldpunt is vergelijkbaar met een 'expert'commissie die XS4ALL in haar klachtenregeling hanteert. De XS4ALL-klachtenprocedure is raadpleegbaar via http://www.xs4all.nl/overxs4all/contact/media/beleidsregels_klachten.pdf.

nader te belichten. Het is immers een ISP die zijn klanten door middel van een overeenkomst de diensten access en hosting aanbiedt waardoor zij gebruik kunnen maken van P2P-netwerken en P2P-netwerksites kunnen aanbieden. Een ISP maakt zodoende een wezenlijk onderdeel uit van het faciliteren van P2P netwerken. In 'Fighting the War on File Sharing' kan een wettelijke NTD-procedure een oplossing bieden.

Verwijzingen

De Jongh & Siemerink 2002
W.Z. de Jongh en L.A.R. Siemerink, Amerikaanse en Finse elementen voor de Nederlandse implementatie van de Richtlijn inzake elektronische Handel, Computerrecht 2002, p. 12-20

Julia-Barcelo 1998
R. Julia-Barcelo, *Liability for On line Intermediaries: A European Perspective*, E.I.P.R. 1998.

Julia-Barcelo & Koelman 2000
R. Julia-Barcelo en K.J. Koelman, *Intermediary liability. Intermediary liability in the E-commerce Directive: so far so good, but it's not enough*, Computer & Law Security Report 2000,

Van der Linden 2008
T. van der Linden, 'Vrijheid en vogels', *Ars Aequi* 2008, p. 96-97.

Rietjens 2006
B. Rietjens, 'Over leechers, seeds en swarms: auteursrechtelijke aspecten van BitTorrent', *AMI* 2006/1, p. 10.

Schellekens 2001
M.H.M. Schellekens, *Aansprakelijkheid van Internetaanbieders* (diss. Tilburg UT), 2001.

Schmidt 2004
A.H.J. Schmidt, Bedreigen computers ons rechtssysteem?, rede uitgesproken bij de aanvaarding van het ambt van hoogleraar Recht en Informatica aan de Universiteit Leiden, 2004.

Schmidt, Dolfsma & Keuvelaar 2007
A.H.J. Schmidt, W. Dolfsma en W. Keuvelaar, *Fighting the War on File Sharing*, IT&Law nr. 14, 2007.

Seignette 2001
J.M.B. Seignette, 'Napster en de controle van de rechthebbende over de distributie van zijn werk', *AMI* 2001.

Siemerink 2008
L.A.R. Siemerink, 'IE(-rechten), P2P en ISP: handhaving van auteursrechten op internet nog mogelijk?, *MvV* 2008 7/8, p. 179-189.

Siemerink 2007
L.A.R. Siemerink, *De overeenkomst van Internet Service Providers met consumenten* (diss. Leiden UL), Recht & Praktijk nr. 149, 2007, p. 11-23.

Visser 2001
D.J.G. Visser, 'Napsteren', 'Gnutellen' en de afwezigheid van legale muziek op Internet, Computerrecht 2001

Wichers Hoeth 2007
L. Wichers Hoeth, *Kort begrip van het intellectuele eigendomsrecht*, 2007.

DEEL III

METHODE

De geesteswetenschappen, rechtsgeleerdheid en kunstgeschiedenis vergeleken

Annemarie Beunen■

Inleiding

In 2004 schreef Aernout:

> 'Bij de bepaling van optimaal recht belanden we onvermijdelijk in een vraagstelling die niet met alleen juridische argumenten kan worden beslist. De rechtstheorie levert belangrijke argumenten (…), maar minstens even belangrijk zijn overwegingen van economie, cultuur en architectuur. Met De Geest ben ik van mening dat het de rechtswetenschap verder zal brengen, wanneer voor de methoden en technieken vaker leentjebuur wordt gespeeld bij de ervaringswetenschappen.'[1]

Deze passage, waaruit Aernouts grensoverschrijdende interdisciplinaire interesse blijkt, vat ik (als kunsthistoricus) op als een uitnodiging om over 'overwegingen van cultuur en architectuur' in enge zin uit te weiden. Daarvoor zal ik onderzoeksmethoden die binnen de kunstgeschiedenis worden gehanteerd, vergelijken met die van het recht. Tot slot hoop ik de lezer ervan te overtuigen dat Aernouts pleidooi voor leentjebuur spelen inderdaad loont en wat er dan voor een jurist te leren valt van een geesteswetenschap zoals de kunstgeschiedenis.

ICT-recht

Als rechtgeaarde jurist begin (ook) ik eerst met een casus,[2] natuurlijk op het terrein van het ICT-recht en wel het mij zo welbekende databankrecht. De zaak betreft de zoekmachine Gaspedaal.nl, die via deeplinks (onder meer) Autotrack.nl, de online databank van Wegener met occasionadvertenties ontsluit.[3] De vraag die de rechter te beantwoorden krijgt, is: maakt zoek-

---

■ Annemarie Beunen is als jurist werkzaam bij de Koninklijke Bibliotheek en als universitair docent verbonden aan eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij.

1 Schmidt 2004, p. 1438.

2 In zijn hoofdstuk 'De kunst om met casus om te gaan' lijkt Vranken de kenmerkende casusgerichtheid van juristen eerder als een vloek dan als een zegen te beschouwen, zie Asser-Vranken 2005, p. 4-13.

3 Rb Den Haag 11 februari 2009 (Wegener/Innoweb), *Mediaforum* 2009, p. 139 m.nt. T.F.W. Overdijk; *Computerrecht* 2009, p. 131 m.nt. O.M.B.J. Volgenant; *AMI* 2009, p. 206 m.nt. P.B. Hugenholtz. Voorafgaand kort geding: Vzr. Rb Utrecht 21 november 2007 (Wegener/Innoweb), *Mediaforum* 2008, p. 42 m.nt. D.J.G. Visser; *AMI* 2008, p. 109 m.nt. K.J. Koelman.

machine Gaspedaal.nl inbreuk op het databankrecht van Wegener? Volgens de Databankenwet is dat (in letterlijke navolging van de Europese Databankrichtlijn) het geval wanneer Gaspedaal:

1) een substantieel deel uit de databank opvraagt en/of hergebruikt, dan wel

2) daaruit herhaald en systematisch niet-substantiële delen opvraagt en/of hergebruikt, *voor zover dit in strijd is met de normale exploitatie van die databank of ongerechtvaardigde schade toebrengt aan de rechtmatige belangen van de producent van de databank* [mijn cursivering].[4]

Zowel in het kort geding als de bodemzaak wordt geoordeeld dat aan de eerste voorwaarde niet is voldaan. Anders dan de Utrechtse Voorzieningenrechter komt de Haagse rechtbank echter tot de conclusie dat aan de tweede voorwaarde wel is voldaan. Zij oordeelt dat Gaspedaal door het cumulatief effect van de vele zoekopdrachten uiteindelijk een substantieel deel van Wegeners databank aan het publiek ter beschikking stelt en citeert hiervoor de uitleg die het Europese Hof van Justitie aan het bewuste art. 7(5) van de Databankrichtlijn heeft gegeven.[5] Deze uitleg geef ik hier weer in de originele taal van het vonnis:

> '(…) 'acts which conflict with a normal exploitation of a database or which unreasonably prejudice the legitimate interests of the maker of the database' refer to unauthorised actions for the purpose of reconstituting, through the cumulative effect of acts of extraction, the whole or a substantial part of the contents of a database protected by the *sui generis* right and/or of making available to the public, through the cumulative effect of acts of re-utilisation, the whole or a substantial part of the contents of such a database, which *thus* seriously prejudice the investment made by the maker of the database.'

De Nederlandse vertaling als weergegeven door de Rechtbank: 'en die *aldus* ernstige schade toebrengen aan de investering van de samensteller van deze databank'. [Mijn cursiveringen].

De Haagse rechtbank vervolgt:

> 'Uit het feit [sic][6] dat Innoweb door het cumulatief effect van de vele zoekopdrachten via Gaspedaal.nl een substantieel deel van de databank van Wegener aan het publiek ter beschikking stelt, *volgt dat* het handelen van Innoweb ernstige schade toebrengt aan de investering van Wegener (zie de laatste zin van het (…) citaat uit het Hill-arrest).'

Deze passage is bekritiseerd door annotatoren. Het door het Europese Hof gebezigde woordje 'thus/aldus' legt de rechtbank zo uit dat de vereiste

4 Art. 2(1) sub a en b Databankenwet en art. 7(1) en 7(5) Databankrichtlijn.

5 EHvJ 9 november 2004, zaak C-203/02 (British Horseracing Board/William Hill Organization Ltd.), *European Court Reports* 2004, p. I-10415, overwegingen 89 en 95.

6 Dit is mijns inziens geen feit maar slechts een mening, gegeven het feit dat men in literatuur en jurisprudentie sterk van mening verschilt over de rechtsvraag of deeplinkende gespecialiseerde zoekmachines inbreuk maken op het databankrecht.

schade gegeven is wanneer men – zoals de rechtbank – oordeelt dat overname van een substantieel deel in het spel is: is aan X voldaan, dan volgt dat Y (schade) gegeven is. Annotator Volgenant wijst er echter terecht op dat deze tekstanalyse niet de enig mogelijke interpretatie is. 'Thus/aldus' kan ook een extra eis inleiden waaraan het voorafgaande moet voldoen (dat sprake is van X is niet genoeg: X moet tevens Y tot gevolg hebben). Volgt men deze uitleg (en de wettekst zelf spreekt hiervoor),[7] dan is het zeer de vraag of in deze zaak wel inbreuk aan de orde was. Kortom: een alternatieve tekstanalyse had de uitkomst in deze zaak radicaal kunnen doen omslaan.

Voor de (rechts)wetenschapper is dit vonnis om twee redenen onbevredigend. Ten eerste geeft de rechtbank er niet expliciet blijk van te erkennen dat tekstanalyse tot uiteenlopende resultaten kon leiden – terwijl aangenomen mag worden dat zij dit wel besefte. Ten tweede expliciteert zij niet waarom ze juist voor die ene tekstinterpretatie heeft gekozen. Nu kunnen wij alleen gissen welke afweging van belangen en argumenten de rechtbank hiervoor heeft gemaakt. Speculerend: wellicht heeft zij in dit geval teruggeredeneerd vanuit de door haar wenselijk geachte uitkomst. Door-speculerend: dit zou bescherming van Wegeners huidige business model kunnen zijn,[8] maar zeker weten we het dus niet. Bij gebrek aan expliciete inhoudelijke overwegingen kan een jurist zich aldus geen mening vormen over de 'juistheid' en falsifieerbaarheid van dit oordeel.

Dat is jammer, te meer omdat de uitkomsten van rechtszaken over nieuwe ICT-fenomenen vaak onvoorspelbaar blijken. Meer dan op andere rechtsgebieden worstelen rechters binnen het ICT-recht met de vraag wat recht(vaardig) is als ze moeten oordelen over innovatieve technologieën of producten. Rechtsregels zelf bieden weinig houvast voor de vraag hoe zij kunnen/moeten worden toegepast op noviteiten. Het recht heeft die niet kunnen voorzien en loopt dus altijd achter, maar al ware het mogelijk om techniekonafhankelijke wetgeving te ontwerpen,[9] dan nog wijst het recht niet de weg naar 'die ene rechtvaardige uitkomst'. Rechtsregels zeggen immers niets over de wenselijkheid van (de gevolgen van) ICT-verschijnselen en hoe de rechter geschillen daarover moet behandelen. Het is bijvoorbeeld niet zo simpel om antwoord te geven op de vraag: Maakt Google's zoekmachine inbreuk op andermans IE-rechten? Jurisprudentie over nieuwe ICT-verschijnselen pioniert er dan ook lustig op los en geeft daarom uiteenlopende oplossingen te zien; meestal is er niet één 'right answer'.[10]

---

7 Maar kennelijk was dat voor de rechtbank geen gegeven. Dit illustreert dat het niet (iedereen) steeds mogelijk is om in de woorden van (en in weerwil van) De Geest 'de echte oorspronkelijke (zender)betekenis' van een tekst te achterhalen. Vergelijk De Geest 2004a, p. 59, 61 en 64 en De Geest 2004b, p. 1440 en 1441.

8 Zoals bepleit door Visser in zijn noot bij het Kort Geding en Visser 2008. Anderszins: Koelman in zijn noot bij het Kort Geding en Beunen 2007.

9 Bepleit door De Cock Buning 1998.

10 Stolker 2003, p. 768-769.

Recht als wetenschap – een vergelijking met de kunstgeschiedenis

Niet alleen het ICT-recht, maar ook de traditionele rechtsgebieden zien zich door de technologische vooruitgang met nieuwe soorten claims geconfronteerd. En ook hier geven de rechters in hun uitspraken niet één 'right answer', maar uiteenlopende oordelen. Stolker illustreert dit aan de hand van de uiterst verschillende vonnissen die wrongful life-claims in diverse landen hebben opgeleverd. Naar aanleiding hiervan heeft hij de belangwekkende vraag opgeworpen of het recht wel een wetenschap kan worden genoemd: 'Als dát dan zo is – zullen collega's uit andere disciplines zeggen – als de mogelijkheid van een 'right answer' zó ver weg ligt, hoort de rechtsgeleerdheid, waarin het mogelijk is dat kennelijk verstandige mensen over een en dezelfde zaak tot zulke uiteenlopende conclusies komen, dan wel thuis in een universiteit?' Onder verwijzing naar de Amerikaanse jurist Posner[11] stelt Stolker de rechtsgeleerdheid tegenover de natuurwetenschap, hét prototype van 'de wetenschap'. De natuurwetenschap streeft ernaar om tot universeel geldende uitspraken te komen die objectief bewijsbaar zijn. Dit streven is het recht, met zijn normatieve uitspraken, echter vreemd. Daarmee zou de rechtswetenschap niet voldoen aan de traditionele opvatting van wat wetenschap is en staat zij bloot aan twijfels over haar wetenschappelijk karakter.

Maar verschilt de rechtswetenschap hierin wel zoveel van de geesteswetenschappen? De vraag stellen is hem (negatief) beantwoorden. In wat volgt zal ik deze hypothese nader proberen te onderzoeken en onderbouwen. Zoals al in de inleiding aangekondigd, wil ik daartoe een vergelijking trekken tussen de onderzoeksmethoden van het recht en die van de geesteswetenschap kunstgeschiedenis. Ik neem de kunstgeschiedenis als voorbeeld, omdat ik deze geesteswetenschap als kunsthistoricus het best ken.

Afbakening binnen de kunstgeschiedenis

Laat ik voorop stellen dat ik mij concentreer op de traditionele (ouderwetse, zouden veel kunsthistorici tegenwoordig zeggen) onderzoeksrichting van de stilistiek: de kunsthistorische discipline die zich bezighoudt met onderzoek naar de persoonlijke stijl van een kunstenaar en de authenticiteit van zijn/haar werken. Stilistisch onderzoek resulteert in toe- en afschrijvingen van werken waarvan de authenticiteit wordt betwist. De ultieme stilistische publicatie is de *catalogue raisonné* die het gehele oeuvre van een kunstenaar opsomt en beschrijft, meestal in chronologische volgorde. Een voorbeeld van een wereldwijd bekend Nederlands onderzoeksproject op dit terrein is het Rembrandt Research Project (RRP), dat al sinds 1969 onderzoek doet naar de vele aan Rembrandt toegeschreven schilderijen. Het RRP staat sinds 1993

11 Citaat uit R.A. Posner, *The Problems of Jurisprudence*, Harvard University Press 1993, zoals (verkort) overgenomen uit Stolker 2003, p. 769: 'What is missing from law are (…) objectively testable – and continually retested – hypotheses.'

onder de bezielende leiding van prof. dr. Ernst van de Wetering en zal hierna nog ruimschoots aan de orde komen.[12]

Door mijn focus op de stilistiek – die ik zelf ook heb beoefend[13] – laat ik vele andere kunsthistorische onderzoeksrichtingen hier grotendeels buiten beschouwing. Om echter toch een beeld te geven van de veelzijdigheid van het kunsthistorisch onderzoek die ik onderbelicht laat, volgt hier een – geenszins uitputtend – overzicht:

- historisch onderzoek naar de ontstaansgeschiedenis van een werk waaronder de relatie opdrachtgever-kunstenaar;
- onderzoek naar de invloed van contemporaine literaire bronnen op een kunstwerk;
- iconografie: beschrijving en bestudering van het onderwerp van een kunstwerk;
- iconologie: interpretatie van de diepere cultuurhistorische betekenis van een werk;
- de geschiedenis van een specifieke privé- of museumcollectie;
- receptiegeschiedenis: de interpretaties en betekenissen die door de eeuwen heen aan een werk zijn gegeven (of: fortuna critica);
- de invloed van een belangrijk werk op latere kunstwerken (of: Nachwirkung).

De onderzoeksvraag binnen het recht en de kunstgeschiedenis

In de geesteswetenschappen is het gebruikelijk om onderzoek te verrichten aan de hand van een duidelijk afgebakende onderzoeksvraag. Voordat een geesteswetenschapper zijn/haar onderzoeksvraag formuleert, kiest hij/zij echter eerst voor een bepaalde onderzoeksrichting. De kunsthistorische opsomming hierboven maakt duidelijk dat iedere onderzoeksrichting haar eigen vragen stelt. De keuze voor een specifieke richting vormt dus de allereerste afbakening van het onderzoek en deze hangt veelal af van de subjectieve interesses van de onderzoeker zelf.

Vervolgens zal hij/zij binnen die richting een specifieke onderzoeksvraag gaan bepalen. Meestal heeft men al een aanmerkelijk (meer of minder globaal) inzicht nodig in de inhoud van het bronnenmateriaal dat men wil gaan bestuderen, voordat men een onderzoeksvraag kan formuleren. Het is immers zaak om een vraag te stellen die *zinvol* onderzoek oplevert, vandaar dat men veelal (impliciet of expliciet) uitgaat van een zelfontwikkelde hypo-

12 Grijzenhout 2007.

13 Beunen 1995: *catalogue raisonné* van de obscure Nederlands-Italiaanse schilder Abraham Casembroot.

these of vooronderstelling, die men door middel van het onderzoek wil gaan toetsen. Een voorafgaande onderzoeksvraag of hypothese *lijkt* daarmee een noodzakelijke eis voor het bedrijven van wetenschap.

Kijken we naar de juridische onderzoeker enerzijds en de stilistische onderzoeker anderzijds, dan valt op dat zij beiden niet altijd geneigd zijn een nauwkeurig afgebakende onderzoeksvraag te stellen. Gezien het soort onderzoek dat zij doen, is dat echter niet verwonderlijk: de stilistische onderzoeker bestudeert het werk van een kunstenaar en kan daarna aan de hand van stijlkenmerken uitspraken doen over authenticiteitsvragen. Juristen onderzoeken vaak juridische leerstukken of regelgeving aan de hand van de wetsgeschiedenis, rechtspraak en literatuur en trekken daaruit conclusies over onder meer wenselijkheid en doelmatigheid. In beide soorten onderzoek worden er (pas) tijdens de bronnenbestudering en als gevolg van deze bestudering vragen opgeroepen, die de onderzoeker aan het eind tracht te beantwoorden. Dat dergelijk onderzoek vooraf een duidelijke probleemstelling ontbeert, wil echter nog niet zeggen dat het daarmee geen wetenschappelijk niveau zou hebben. Integendeel, de kwaliteit ervan kan mijns inziens per onderzoek verschillen, precies zoals ook de kwaliteit van onderzoeken mét een heldere onderzoeksvraag onderling verschilt.[14] De deugdelijkheid van de gebruikte onderzoeksmethoden en het eindresultaat zijn naar mijn mening beslissend voor het wetenschappelijk niveau van een onderzoek, niet de vraag of er een zeer specifiek afgebakende onderzoeksvraag aan ten grondslag ligt (die kan men ten slotte ook nog na afloop van het onderzoek bedenken, als men de inleiding schrijft).

Het is bovendien twijfelachtig of er bij dit soort onderzoek inderdaad een voorafgaande probleemstelling ontbreekt. Na de keuze van hun onderwerp (een kunstenaarsoeuvre, een juridisch leerstuk of rechtsregel), lijkt het alsof de onderzoekers zich gaandeweg hun onderzoek als het ware door het bronnenmateriaal laten 'verrassen', waarna men daaruit conclusies destilleert. Toch is dat verrassingselement slechts relatief; het is mijns inziens niet zo dat deze onderzoekers geheel blanco staan tegenover het bronnenmateriaal (kunstwerken, danwel rechtspraak en literatuur). Onbewust stelt men zich wel degelijk al bepaalde (deel)vragen, daarbij geleid door subjectieve vooronderstellingen en zienswijzen die samenhangen met het eigen referentiekader, achtergrond en interesses.

Overeenstemmende onderzoeksmethoden: categoriseren

Juridisch onderzoek en de kunsthistorische stilistiek vertonen niet alleen overeenkomst ten aanzien van hun vaak weinig specifieke probleemstelling, maar ook wat betreft hun onderzoeksmethoden. Bestudering van de wetsgeschiedenis is een beproefd onderdeel van juridisch onderzoek en ook de rechter grijpt steeds terug naar het verleden, enerzijds om te kunnen bepalen hoe het geschil is ontstaan en anderzijds om te bezien hoe dergelijke casus

14 Stolker 2003, p. 776 haalt Nieuwenhuis aan, die een heldere probleemstelling voor een proefschrift een garantie heeft genoemd voor de onbenulligheid van het resultaat.

eerder door de rechter zijn opgelost. De historische benadering staat ook in veel kunsthistorische onderzoeksrichtingen centraal, met name bij de vraag naar de ontstaansgeschiedenis van een bepaald kunstwerk. Het (ver of minder ver) terugkijken om te reconstrueren hoe het is gegaan of zou kunnen zijn gegaan, is dus een constante in zowel het recht als de (kunst)geschiedenis.

Ten tweede maken beide disciplines gebruik van de meest universele wetenschappelijke methode, namelijk die van het ordenen, indelen of categoriseren. Om grip te krijgen op de chaos van het vele onderzoeksmateriaal (kunstwerken, rechterlijke vonnissen) is dit categoriseren onontbeerlijk. Door bestudering van het materiaal gaat men bepaalde overeenkomsten en verschillen zien, die leiden tot ordeningscriteria die het mogelijk maken om al het onderzoeksmateriaal inclusief nieuw, nog onbekend materiaal in categorieën onder te brengen. Samen met de selectie van het onderzoeksmateriaal is de bepaling van de ordeningscriteria richtinggevend voor de eindconclusies van het onderzoek.

Zo staat de stilistische onderzoeker voor de zware taak om via grondige studie van de onbetwist authentieke werken van een kunstenaar een set stijlkenmerken te identificeren, waarmee hij/zij overtuigende uitspraken kan doen over de eigenhandigheid van betwiste werken. Hoe gaat dit in zijn werk? Net als een jurist begint een kunsthistoricus uiteraard niet bij nul, maar kan hij/zij bogen op een forse basiskennis aan canonwerken. Het eerste universitaire studiejaar bestaat grotendeels uit 'plaatjes stampen', zoals juristen belangrijke arresten moeten stampen. Door honderden plaatjes in het visuele geheugen op te slaan, leert men op macroniveau opeenvolgende schilder-, beeldhouw- en architectuurstijlen te onderscheiden en dateren en op microniveau werken van belangrijke kunstenaars te herkennen. De eerste vraag die een in stilistiek gespecialiseerde kunsthistoricus voor een hem/haar onbekend werk zich stelt, is dan ook: 'Waar lijkt dit op?'. Dit is een vraag die ook een jurist, op zoek naar constanten in rechtspraak en literatuur, niet vreemd is.

'Intuïtief redeneren':[15] *connaisseurschap versus normatief oordelen*

Een kunsthistoricus kan op diverse manieren te werk gaan bij het zoeken naar constanten in de werken van een kunstenaar. Terugkerende stijlkenmerken worden bijvoorbeeld gezocht in de wijze waarop onderwerpen zijn geschilderd die de maker vaak afbeeldt, zoals mensfiguren in een landschap, in de 'bladslag' van bomen en struikgewas, kleurgebruik, dieptewerking, schildertechniek (glad of pasteus), enzovoort. Op detailniveau gericht is de Morelli-methode, genoemd naar de 19e-eeuwse Italiaanse kunsthistoricus en arts Giovanni Morelli. Zijn uitgangspunt was dat elke kunstenaar bepaalde onderdelen steeds op een routinematige manier zal schilderen. De Morellimethode focust dan ook op steeds terugkerende details: hoe schilderde de

15 Term ontleend aan De Geest 2004a, p. 61 en 62. Het gebruik van de intuïtie door juristen wordt ook aan de orde gesteld door Barendrecht/Vranken e.a. 2004, p. 1423, 1425 en 1426.

kunstenaar bijvoorbeeld oren of vingers en is hierin wellicht een unieke constante hand zichtbaar? Inderdaad zijn schilders soms op deze wijze te identificeren. Een gezicht door Botticelli is door kenners vrij eenvoudig als van deze meester te herkennen, door de typische vorm en de (zo men wil, zacht melancholische) expressie van diens gezichten. Door veel authentieke werken van dezelfde maker aandachtig te bestuderen en hun overeenkomsten in het visuele geheugen op te slaan, ontwikkelt men het zogenoemde connaisseurschap (of kennerschap).

Met het connaisseurschap raken we aan de achilleshiel van de kunstgeschiedenis, als het gaat om de discussie over de wetenschappelijkheid van dit vakgebied. Het fenomeen van connaisseurschap staat namelijk onder de verdenking van een grote mate van subjectiviteit, als gevolg van intuïtief redeneren. Twee kunsthistorici die naar hetzelfde schilderij kijken, zullen het op een verschillende manier beschrijven. Diezelfde subjectiviteit kan zich ook voordoen bij de selectie van typerende stijlkenmerken die een kenner maakt van een kunstenaarsoeuvre. Zo resulteert connaisseurschap in een niet onfeilbaar, intuïtief oordeel inzake toe- en afschrijvingen. In de geschiedenis van de Rembrandt-stilistiek zijn er *catalogues raisonnés* gepubliceerd waarin de *raisons* voor toe- en afschrijving zelfs nagenoeg ontbraken.[16] Daartegenover maakte het Rembrandt Research Project bij zijn oprichting in 1969 duidelijk dat het geen genoegen wilde nemen met onbeargumenteerde keuzes, maar dat het Rembrandts oeuvre wilde zuiveren door middel van rationele en navolgbare argumenten. Daartoe introduceerde het RRP diverse natuurwetenschappelijke methoden:[17]

- met dendrochronologisch onderzoek (jaarringenmeting) is de datering van een beschilderd paneel vrij nauwkeurig te bepalen;
- door bepaling van de weefseldichtheid van een doek kunnen schilderijen worden geïdentificeerd die van dezelfde doekrol gesneden zijn;
- dwarsdoorsneden maken de materiële opbouw van een werk zichtbaar;
- verfmonsters geven uitsluitsel over de chemische samenstelling van de verf;
- met röntgen- en infraroodstraling kunnen voorbereidende schetsen en overschilderingen zichtbaar worden gemaakt.

Van de Wetering beschrijft hoe de hoge verwachtingen die het RRP van dit

16 Waaronder die van Abraham Bredius, oud-directeur van het Mauritshuis, die in 1935 in zijn boek *Rembrandt: schilderijen* maar liefst 611 schilderijen aan Rembrandt toeschreef. Daartegenover accepteerde Christian Tümpel (Nijmeegs hoogleraar † van wie ik nog les genoot) in zijn standaardwerk over Rembrandt uit 1986 slechts 285 schilderijen als authentiek.

17 Zie RRP Corpus IV, Summary p. XXIX, op http://www.rembrandtresearchproject.org.

natuurwetenschappelijk onderzoek had in belangrijke mate samenhingen met de Van Meegeren-affaire. In 1937 dook een onbekend schilderij van *De Emmausgangers* op dat door de gerenommeerde kunstkenner Abraham Bredius werd ontdekt als een nieuw werk van Johannes Vermeer (afb. 1).

Afb. 1
Han van Meegeren, De Emmausgangers
olieverf op doek, 115 x 127 cm, gesigneerd: IVERMEER
Collectie Museum Boijmans Van Beuningen, Rotterdam.

Directeur Dirk Hannema van het Rotterdamse Museum Boymans kocht het doek vervolgens aan voor circa *f* 540.000.[18] Direct na de oorlog werd Han van Meegeren gearresteerd wegens collaboratie omdat hij Nederlands erfgoed aan de vijand zou hebben verkocht; er was een Vermeer aangetroffen in de verzameling van Hermann Göring. Gaande het proces bekende Van Meegeren diverse Vermeers, waaraan hij miljoenen had verdiend, zelf geschilderd te hebben. Ten bewijze schilderde hij in de gevangenis een *Christus in de tempel* in Vermeer-stijl.[19] Vanwege ongeloof en verdeeldheid in de kunstwereld moest natuurwetenschappelijk onderzoek uiteindelijk uitsluitsel brengen over de valsheid van *De Emmausgangers*.[20] Kijkt men nu naar dit schilderij, dat nog altijd in Museum Boijmans Van Beuningen hangt, dan is moeilijk te geloven dat het destijds voor een Vermeer kon worden gehouden. Het lijkt in niets op de interieurstukken waarmee Vermeer voornamelijk bekend is. Er zijn echter enkele vroege, door Vermeer gesigneerde schilderijen bekend met afwijkende stijl en onderwerpen (afb. 2 en 3). In de context van die vroege werken kon *De Emmausgangers* (een nieuwe creatie, geen kopie van een bestaand werk) voor een Vermeer worden aangezien.

18 Hannema 1973, p. 107.
19 Van den Brandhof 1979, p. 115.
20 Ondanks dit onderzoek bleef Hannema er zijn hele leven van overtuigd dat *De Emmausgangers* door Vermeer was geschilderd en hij heeft later nog meer Vermeer-toeschrijvingen gedaan, die overigens geen steun vonden onder andere kunsthistorici. Hannema 1973, p. 110, 154-160.

Afb. 2
J. Vermeer, Christus in het huis van Maria en Martha, ca. 1654-1656
Olieverf op doek, 63 x 56 inch
National Galleries of Scotland, Edinburgh

Afb. 3
J. Vermeer, Diana en haar metgezellen, 1655-1656
Olieverf op doek, 39 x 41 inch
Mauritshuis, Den Haag

De Van Meegeren-affaire leidde in de kunsthistorische en museumwereld tot een paranoia voor vervalsingen. Een van de oprichters van het RRP had gewerkt bij kunsthandelaar Hoogendijk, die te goeder trouw had bemiddeld bij de aankoop van *De Emmausgangers* door Museum Boymans. Dit RRP-lid was er sindsdien van overtuigd geraakt dat ook het oeuvre van Rembrandt vervuild was met latere kopieën en vervalsingen. Uitgaande van deze hypothese zette het RRP hoog in op natuurwetenschappelijk onderzoek, dat deze vervalsingen immers op objectieve wijze zou kunnen ontmaskeren.[21] Dit onderzoek leverde het RRP inderdaad veel kennis op, zoals uitsluitsel over de vraag of een schilderij wel of niet uit de 17e eeuw stamde. Zo bleek echter ook dat de RRP-hypothese onjuist was: veruit de meeste schilderijen waren

21 RRP Corpus IV, Preface p. X op http://www.rembrandtresearchproject.org.

wel degelijk in de 17e eeuw geschilderd. Vervolgens konden deze objectieve onderzoeksmethoden niet het beslissende antwoord geven op de hamvraag: Is dit schilderij nu door Rembrandt zelf geschilderd of niet? Zo moesten de RRP-leden zich uiteindelijk toch weer verlaten op hun connaisseurschap, wat ze juist hadden willen vermijden. De objectieve natuurwetenschappelijke methoden bleken kortom toch niet zaligmakend.

Grijzenhout beschrijft dan ook hoe critici kanttekeningen hebben geplaatst bij de poging van het RRP tot objectivering van hun oordeel versus de inherente subjectiviteit van het connaisseurschap. In 1993 viel het RRP-team uiteen en sindsdien staat het onder de eenkoppige leiding van Ernst van de Wetering, die een nieuwe koers is ingeslagen. Hij heeft veel lezenswaardigs geschreven over het RRP-connaisseurschap. Zo wees hij op de neiging om veiligheid te zoeken in consensus; volgens hem heerst er de curieuze veronderstelling dat hoe meer mensen dezelfde mening hebben over een schilderij, hoe groter de kans is dat ze gelijk hebben. Hij schrijft ook dat het herkennen van een Rembrandt wordt bemoeilijkt doordat de schilder geen constante stilistische evolutie doormaakte en niet 'op routine' werkte, maar zoekend was en ieder schilderij aanvatte als een nieuw avontuur. In dat verband wijst Van de Wetering op de gevaarlijke neiging die het RRP-team soms had om Rembrandts stijl en ontwikkeling in een rationeel model van bekende stijlkenmerken te willen persen, om er zo op te anticiperen hoe een werk van Rembrandt eruit zou *behoren* te zien.[22]

In een artikel over een nieuw ontdekte Rembrandt maakt Van de Wetering duidelijk hoe hij bij het wegen van het 'bewijs' te werk is gegaan. Onder verwijzing naar Thomas Bayes – geen onbekende voor het strafrecht en de forensische statistiek – stelt hij voorop:

> 'Because of the complications surrounding the 'searching' Rembrandt (…), the attribution of paintings to the early Rembrandt is never easy, whether the arguments for attribution are based on objective evidence or more subjectively on connoisseurial assessment. Each individual argument may be met with a counter-argument that might undermine its strength. We have long struggled with this methodological problem and have eventually found a way to deal with it, based on the ideas on probability of Thomas Bayes (1702-1761) (…): Applying the Bayesian approach to our own research, one can argue that if several weak pieces of evidence support the belief that a painting could be by Rembrandt, the evidence becomes stronger to the extent that each piece of evidence tends to eliminate an alternative possibility. [Bayes] also observed that a variety of evidence provides better confirmation than an equal amount of homogeneous evidence.'[23]

---

22 Van de Wetering 2008, p. 84-85. Dit terwijl bovendien onduidelijk is in welke mate de vergelijkingsgroep van schilderijen waaraan de connaisseur intuïtief refereert, is vervuild door onjuiste toeschrijvingen.

23 Van de Wetering 2007, p. 23. Hij haalt in Van de Wetering 2008, p. 84 de bekende kunsthistoricus Max Friedländer aan: 'As the "No"man imagines that he stands above the "Yes"man – and probably also to others seems to stand higher – critics will always feel the impulse to attack genuine works in order to win the applause of the maliciously minded. The "Yes"men have done more harm, but have also been of greater usefulness than the rigorous "No"men, who deserve no confidence if they have never proved their worth as "Yes"men.' (M.J. Friedländer, *On Art and Connoisseurship*, Oxford 1946, p. 261).

Vervolgens somt Van de Wetering vier objectieve(re) argumenten op (onder andere de monogramweergave, het koperplaat-formaat en de onderschildering) mét tegen-argumenten, en daarna vier subjectieve, stilistische argumenten (waaronder de contouren, de beeldvlakverdeling en de dikgeschilderde hoogsels), die volgens hem alle gezamenlijk tot de conclusie leiden dat het betreffende schilderij van Rembrandts hand moet zijn. Zo poogt hij zijn conclusie van een onderbouwing te voorzien, die door andere onderzoekers kan worden gefalsifieerd.

Lessen voor juristen?

Illustratief voor juristen is dat Van de Wetering hier inzichtelijk maakt hoe hij tot weging van het bewijs is gekomen, door de diverse objectieve en subjectieve onderbouwingen van zijn eindconclusie te expliciteren. Zo uitgebreid doen de meeste stilistische onderzoekers dat niet en ook juristen zijn meestal niet scheutig met het expliciteren van de onderliggende argumenten voor hun normatieve oordelen. Volgens De Geest maken juristen zich schuldig aan intuïtief redeneren: argumenteren op louter intuïtief niveau zonder de bouwstenen van de eigen redenering te expliciteren.[24] Dit is in feite hetzelfde verwijt als de stilistiek wordt gemaakt, met dezelfde twijfel aan de wetenschappelijkheid als gevolg. Wetenschap, vervolgt De Geest, vereist dat redeneringen expliciet worden gemaakt; pas dan kan worden getoetst of ze geen fouten bevatten. Hij pleit dan ook voor explicitering door juristen. In reactie op zijn artikel doen Franken en Barendrecht/Vranken e.a. dat ook[25] en ik sluit me graag bij hen aan. Daar waar er, zoals ook in het ICT-recht, niet één 'right answer' is maar meer oplossingen mogelijk zijn, is de behoefte aan explicitering van de gebruikte criteria en motivering van de gemaakte keuzes des te groter. Zonder motivering blijft immers in het duister waarom een bepaalde oplossing de meest wenselijke is. Theorie en praktijk van het (ICT-) recht worden daarmee niet verder geholpen.

Al expliciteert kunsthistoricus Van de Wetering zijn conclusie zoveel mogelijk, tegelijkertijd geeft hij blijk van een groot besef van de relativiteit en subjectiviteit van authenticiteitsoordelen. Onvermijdelijk spelen hierin volgens hem impliciete, intuïtieve vooronderstellingen mee die, juist omdat de onderzoeker ze onbewust volgt, niet te expliciteren zijn. Hij schrijft dat één van de redenen van het uiteenvallen van het RRP-team een groeiend meningsverschil was over de vraag met welke mate van zekerheid authenticiteitsoordelen gegeven konden worden.[26] De buitenwereld (musea, kunsthandel) heeft immers juist behoefte aan de grootst mogelijke duidelijkheid, mede ingegeven door de grote financiële gevolgen van RRP-oordelen. Een

24 De Geest 2004a, p. 62 en 66.
25 Franken 2004, p. 1408; Barendrecht/Vranken e.a. 2004, p. 1422, 1423, 1425-27.
26 RRP Corpus IV, Preface p. XIII.

lange disclaimer in het laatste deel van de RRP-reeks *A Corpus of Rembrandt Paintings* benadrukt nu dat de oordelen erin slechts beschouwd moeten worden als meningen die uitsluitend bedoeld zijn voor academisch gebruik en onderhevig zijn aan verandering:

> 'Disclaimer
>
> This is a publication of the Stichting Foundation Rembrandt Research Project. The opinions expressed in this volume (IV), and the previously published volumes I-III in the Series *A Corpus of Rembrandt Paintings*, should be understood as "opinions" that are meant for academic use only. The opinions represent the Foundation's best judgment based on available information at the time of publication. The opinions are not statements or representations of fact nor a warranty of authenticity of a work of art and are subject to change as scholarship and academic information about an individual work of art changes. Opinions have been changed in the past according to new insights and scholarship. It should be understood that forming an opinion as to the authenticity of a work of art purporting to be by Rembrandt is often very difficult and will in most cases depend upon subjective criteria which are not capable of proof or absolute certainty. Therefore, the conclusions expressed in the volumes are only opinions and not a warranty of any kind. Third parties cannot derive any rights from these opinions. Neither the Foundation, nor the members of its board, nor the authors, nor the cooperators, nor any other parties engaged in the Rembrandt Research Project accept any liability for any damages (*schade*), including any indirect or consequential damages or losses and costs. Anyone is free to disagree with the opinions expressed in these volumes.'

Overduidelijk wordt hier gewaarschuwd voor de relativiteit van de oordelen. Deze relativiteit geldt evenzeer voor de normatieve oordelen van juristen op terreinen als het ICT-recht. Franken heeft erop gewezen dat de rechtswetenschap past in de geestes- en gedragswetenschappen, omdat ook zij steeds bezig is met het voorlopige resultaat van een proces van meningsvorming en overtuiging zowel in abstracto als bij de beslissing in concreto; zij levert contextafhankelijke en daarmee voorlopige kennis op.[27]

Juridische onderzoekers lijken echter weinig blijk van dit besef te geven in hun normatieve oordelen. Die worden vaak (onbeargumenteerd) geponeerd met een stelligheid die wel doet denken aan de absoluutheid waarmee wettelijke regels of rechterlijke oordelen zijn geformuleerd.[28] Dit terwijl de stelligheid van hun oordelen nogal eens omgekeerd evenredig is aan de houdbaarheid ervan. Juist in het recht (en met name het ICT-recht) wisselen nieuwe inzichten elkaar immers in hoog tempo af, wat ook blijkt uit de snelle veroudering van rechterlijke uitspraken.

Ook juridische literatuur veroudert snel, vaak sneller dan kunsthistorische. Kunsthistorisch onderzoek blijft veel langer van waarde omdat ze vaak een nieuwe interpretatie toevoegt aan de vele die er al zijn voorgesteld om bepaalde kunstwerken te duiden. Zo'n interpretatie of theorie behoudt naast andere haar waarde zolang ze niet wordt gefalsifieerd en vormt zo een ver-

27 Franken 2004, p. 1405 en 1407.

28 Vergelijk het vonnis waarmee ik begon, waarin de Rechtbank het antwoord dat zij op een sterk bediscussieerde rechtsvraag heeft gegeven vervolgens als een feit bestempelt.

rijking van de algehele kunsthistorische kennis. Voor juristen is het wellicht moeilijker om tijdloos te schrijven, omdat hun onderwerpen (vergeleken met kunsthistorische) vaker 'de waan van de dag' betreffen. Met hun algemene beschouwingen over het recht vormen Scholten en Vranken hierop uiteraard belangrijke uitzonderingen.

Kortom

Deze bijdrage begon ik met Aernouts pleidooi om binnen de rechtsgeleerdheid meer leentjebuur te spelen bij de economie, cultuur en architectuur. Ik heb onderzocht wat de kunstgeschiedenis aan zinvols zou kunnen bijdragen. Interessant is dat men ook in deze discipline toenadering heeft gezocht tot objectieve natuurwetenschappelijke methoden, om het betwiste peil van wetenschappelijkheid op te krikken. De stilistiek bleek van de inzet van dergelijke objectieve metingen veel te kunnen leren, maar zaligmakend zijn deze methoden niet. Voor de inzet ervan in juridisch onderzoek geldt naar mijn mening hetzelfde. Wel kunnen meetresultaten veel nuttigs bijdragen, bijvoorbeeld over de vraag hoe effectief bepaalde regelgeving is.[29]

Uit publicaties van Rembrandtkenner Van de Wetering heb ik geput ter ondersteuning van mijn pleidooi voor het expliciteren en beargumenteren van (al dan niet intuïtieve) juridische oordelen. Daarnaast zouden juristen meer blijk mogen geven van het bewustzijn van de relativiteit en subjectiviteit van hun eigen en ook rechterlijke oordelen. Dit besef klinkt niet altijd door in de stelligheid waarmee zij zich plegen uit te drukken. Hierin verschillen juristen van andere geesteswetenschappers, die dit besef vaak expliciet in hun onderzoek tot uitdrukking brengen. Een voorbeeld uit de inleiding van het proefschrift van een bevriende collega-kunsthistoricus:[30]

> 'Elk oordeel, elke impressie gaat uit van de specifieke achtergrond en interesse van de beschouwer in kwestie en is dus altijd "partijdig", incompleet – en soms zelfs moedwillig vertekenend van aard. Zoals bekend, bevat deze constatering een waarschuwing voor elke (cultuur)historicus om zich bewust te zijn van het relatieve van zijn of haar interpretatie. Wij zijn vaak in staat om aan te tonen door wat voor soort gekleurde bril onze voorgangers hun studieobject beschouwen, maar onze eigen blik is evenzeer geconditioneerd, zij het op een andere manier. Ik ben mij ervan bewust dat zulks ook geldt voor dit onderzoek, hoezeer ook een afgewogen en op zoveel mogelijk gegevens gebaseerd oordeel door mij is nagestreefd.'

Dit relativiteitsbesef kan overigens worden bevorderd door het verrichten van onderzoek in het buitenland en contacten met buitenlandse wetenschappers. De kunsthistorische discipline heeft hierbij het voordeel dat zij naar haar aard veel internationaler geörienteerd is dan de juridische; beeldtaal is

29 Zo werden de vermeend positieve effecten van het nieuwe databankrecht op de Europese databankproductie achteraf door cijfers gelogenstraft, zie Beunen 2007, p. 278.

30 Contant 2005, p. 8.

nu eenmaal universeler te verstaan dan wetteksten uit een klein taalgebied. Het uitvoeren van rechtsvergelijkend onderzoek biedt daarom uitkomst voor Nederlandse juristen; het leert inzien dat ons nationale recht en rechtspraak niet 'the only right answer' is, maar slechts één zienswijze representeert temidden van vele goede oplossingen die in diverse buitenlanden zijn gevonden. Kortom, de bescheidenheid van zijn collega-geesteswetenschappers zou ook de jurist sieren…

Verwijzingen

Asser-Scholten
P. Scholten, *Algemeen deel, Mr. C. Asser's Handleiding tot de beoefening van het Nederlandsch Burgerlijk Recht*, Zwolle: W.E.J. Tjeenk Willink, 2e druk 1934 (1931).

Asser-Vranken 2005
J.B.M. Vranken, *Algemeen deel – Een vervolg, Mr. C. Asser's Handleiding tot de beoefening van het Nederlands Burgerlijk Recht*, Deventer: Kluwer 2005.

Barendrecht/Vranken e.a. 2004
M. Barendrecht, J. Vranken, I. Giesen, M. Borgers, W. van der Burg, H. Tijssen, B. van Roermund, W. van Boom, 'Methoden van rechtswetenschap: komen we verder?', *NJB* 2004/28, p. 1419-1428.

Beunen 2007
A. Beunen, *Protection for databases. The European Database Directive and its effects in the Netherlands, France and the United Kingdom*, Nijmegen: Wolf Legal Publishers 2007 (dissertatie Universiteit Leiden).

Beunen 1995
A. Beunen, 'Abraham Casembroot, een Nederlandse schilder in het Sicilië van de zeventiende eeuw', *Oud Holland* 1995 nr. 1/2, p. 32-62.

Van den Brandhof 1979
M. van den Brandhof, *Een vroege Vermeer uit 1937. Achtergronden van leven en werken van de schilder/vervalser Han van Meegeren*, Utrecht/Antwerpen: Het Spectrum 1979.

De Cock Buning 1998
M. de Cock Buning, *Auteursrecht en informatietechnologie. Over de beperkte houdbaarheid van technologiespecifieke regelgeving*, Amsterdam: Otto Cramwinckel 1998 (dissertatie Universiteit van Amsterdam).

Contant 2005
I.M. Contant, *Kruisbeeld tegen kromzwaard. De neerslag van de zeeslag van Lepanto in de Italiaanse kunst ten tijde van de Contrareformatie*, s.l. 2005 (dissertatie Radboud Universiteit Nijmegen).

Fleuren 2009
B. Fleuren, 'Zonder humaniora worden we meer beest dan mens', *NRC Handelsblad* 1 september 2009.

Franken 2004
H. Franken, 'Rechtsgeleerdheid in de rij der wetenschappen, *NJB 2004*, p. 1400-1408.

De Geest 2004a
G. de Geest, 'Hoe maken we van de rechtswetenschap een volwaardige wetenschap?', *NJB* 2004/2, p. 58-66.

De Geest 2004b
G. de Geest, 'Naschrift', *NJB* 2004/28, p. 1439-1441.

Grijzenhout 2007
F. Grijzenhout, 'De zaak Rembrandt. Van project naar research', in: M. Polak, J. Sevink, S. Noorda (red.), *Over de volle breedte. Amsterdams universitair onderzoek na 1970*, Amsterdam 2007, p. 33-57.

RRP Corpus IV
E. van de Wetering e.a., *A Corpus of Rembrandt Paintings IV Self-Portraits*, Dordrecht: Springer 2005.

Schmidt 2004
A.H.J. Schmidt, 'Methoden en technieken' [reactie op Stolker 2003 en De Geest 2004-I], *NJB* 2004/28, p. 1437-1438.

Stolker 2003
C.J.J.M. Stolker, 'Ja, geléérd zijn jullie wel! Over de status van de rechtswetenschap', NJB 2003/3, p. 766-778.

Tümpel 1896
C. Tümpel, *Rembrandt*, Amsterdam: Becht 1986.

Visser 2008
D.J.G. Visser, 'Doorzoekalledatabanken.nl: enkele opmerkingen over zoekmachines, open-content-databanken, auteursrecht en databankenrecht', in: N. van Eijk, B. Hugenholtz (red.), *Dommering-bundel*, Amsterdam: Otto Cramwinckel 2008, p. 359-370.

Van de Wetering 2007
E. van de Wetering, 'Rembrandt Laughing, c. 1628 – a painting resurfaces', *Kroniek van het Rembrandthuis* 2007, p. 19-40.

Van de Wetering 2008
E. van de Wetering, 'Connoisseurship and Rembrandt's paintings: new directions in the Rembrandt Research Project, part II', *The Burlington Magazine* February 2008, p. 83-90.

Schijn verdwijnt waar ICT verschijnt

Rob van Esch■[1]

Waarneming

Mensen nemen dingen waar. Dat doen zij met hun zintuigen. Zij horen iets, zien iets, voelen iets, ruiken iets of proeven iets. Niet ieder mens hoeft hetzelfde waar te nemen.

Soms neemt iemand iets niet waar. Zo zal een dove niets horen en een blinde niets zien. Maar ook bij een mens wiens zintuigen wel goed functioneren, kan het voorkomen dat dingen niet worden waargenomen. Bijvoorbeeld omdat hij daarvoor op dat moment niet ontvankelijk is. Denk aan het constante geluid van een airco, dat je pas opvalt op het moment dat de airco wordt uitgeschakeld. Of de kleur van iemands trui. Als iemand een ruimte verlaat en je vraagt de mensen die enige tijd met hem in die ruimte hebben verkeerd, wat de kleur is van de trui die hij draagt, dan is de kans groot dat de meesten dat niet weten. Voorts kan het voorkomen dat de omstandigheden iemand belemmeren om iets waar te nemen. Iemand hoort niet wat de ander zegt omdat er juist op dat moment een trein langs rijdt.

Het kan ook gebeuren dat een mens iets niet goed waarneemt. Hij hoort bijvoorbeeld niet goed wat de ander zegt.

Waarnemingen kunnen juridische relevantie hebben. Zo is bij het beantwoorden van de vraag welke betekenis iemand redelijkerwijs heeft kunnen toekennen aan de mondelinge verklaring van een ander, ook hetgeen hij overigens heeft waargenomen relevant. Denk aan een gebaar, een gelaatsuitdrukking, de toon van de stem en wellicht zelfs de geur die de ander verspreidt. Verklaart iemand op verontwaardigde toon mijn auto te willen kopen voor € 10.000 euro terwijl hij zijn middelvinger naar mij opsteekt, dan behoor ik uit de waargenomen intonatie en het waargenomen gebaar af te leiden dat hij juist niet mijn auto voor die prijs wil kopen.

In het recht wordt vaak pas achteraf vastgesteld wat iemand heeft waargenomen. Een getuige wordt gevraagd of hij heeft gezien dat een automobilist met zijn auto te hard reed op het moment dat het ongeluk zich voordeed. Ons geheugen is kwetsbaar. De herinnering van hetgeen wij hebben waargenomen kan worden beïnvloed door tal van externe omstandigheden, zoals

---

■ Rob van Esch is afdelingsdirecteur juridische zaken van Rabobank Nederland. Daarnaast is hij als hoogleraar Juridische aspecten van elektronische handel verbonden aan de Faculteit der Rechtsgeleerdheid in Leiden.

1 De titel van deze bijdrage is ontleend aan een slogan over stof en Swiffer.

verklaringen van anderen omtrent hetgeen zij hebben waargenomen. Als anderen verklaren dat de automobilist veel te hard reed, zal menig getuige geneigd zijn een verklaring af te leggen die daarbij aansluit. De herinnering hoeft dan niet meer aan te sluiten bij de werkelijkheid. Dit kan tot gevolg hebben dat rechtens schijn voor waar geldt. Als ik een schriftelijke koopovereenkomst onderteken waarin een koopprijs wordt genoemd van € 1000 exclusief BTW en mijn vriend, die erbij was, zich niet meer weet te herinneren dat de verkoper heeft verklaard dat de gevraagde koopprijs inclusief BTW is, dan geldt hetgeen in de akte staat voor waar. Ook als in werkelijkheid de verkoper wel degelijk een koopprijs inclusief BTW heeft genoemd. Het recht gaat niet om de werkelijkheid maar om de rechtens vastgestelde werkelijkheid.

Betekenis van waarneming

De mens kan een betekenis toekennen aan een waarneming of een combinatie van waarnemingen. Een mondelinge verklaring in combinatie met een waargenomen glimlach en pretogen kan bijvoorbeeld worden uitgelegd als een scherts. We zeggen niet voor niets: zijn gezicht sprak boekdelen.

De uitleg van een waarneming is vaak persoonlijk, afhankelijk van het referentiekader van de persoon die waarneemt.[2] Zo zal een kenner van het kaartspel klaverjassen het leggen van een bepaalde kaart uitleggen als overtroeven, terwijl degene die het kaartspel niet kent, niets anders waarneemt dan dat een bepaalde kaart wordt opgegooid.

De betekenis die wordt toegekend aan waarnemingen, zal afhangen van de omstandigheden waaronder de waarneming wordt gedaan, zoals de plaats en het tijdstip. Iemand die tijdens carnaval een ander ziet met een boerenkiel, zal ziet niet denken: daar gaat een boer.

Hetgeen wordt waargenomen heeft niet noodzakelijkerwijs een universele betekenis. Dat kan bijvoorbeeld per land of cultuur verschillen. Knikt iemand in Nederland met zijn hoofd, dan kan dat worden uitgelegd als instemming. In India betekent dezelfde hoofdknik echter “nee”.

In het recht kan niet alleen de waarneming, maar ook de betekenis die de waarnemer daaraan heeft toegekend, een rol spelen. Iemand knikt met zijn hoofd en omdat hij dit doet in reactie op mijn aanbod, leg ik hetgeen ik heb waargenomen uit als een aanvaarding van mijn aanbod. Het toekennen van betekenis aan waarnemingen is een subjectief proces, dat zich voltrekt in ons brein. Dat wil overigens niet zeggen dat het resultaat van dit proces zich altijd aan onze waarneming onttrekt. Als ik meen dat iemand met een hoofdknik mijn aanbod heeft aanvaard, kan ik hem in reactie op de hoofdknik met een brede glimlach de hand schudden om te benadrukken dat we een overeenkomst hebben gesloten.

2 Zie Smith 2007, p. 84.

Ook een rechter kan in het kader van rechtsvinding een betekenis toekennen aan zijn eigen waarneming of de waarneming van een ander. Een rechter verzocht mij, toen ik ooit optrad als getuige-deskundige, haar aan te kijken zodat zij mijn gezichtsuitdrukking kon waarnemen terwijl ik de verklaring aflegde. De rechter zal aan waarnemingen van partijen of getuigen een betekenis toekennen, waarmee de waarneming van feit tot rechtsfeit wordt. Een getuige verklaart dat een persoon knikte met zijn hoofd, waaraan de rechter de betekenis toekent van het aanvaarden van een aanbod.

Schijn en werkelijkheid

Met schijn bedoel ik dat de waarnemer een (juridische) betekenis toekent aan zijn waarneming die afwijkt van de (juridische) werkelijkheid. Het gaat hier om een subjectieve schijn. Objectieve schijn behoeft niet altijd samen te gaan met subjectieve schijn. Meijers schetst een aantal situaties waarin er in objectieve zin weliswaar sprake is van schijn, maar de handelende partij desalniettemin niet deze objectieve schijn maar de werkelijkheid voor werkelijkheid houdt. Ik geef het aan hem ontleende voorbeeld van de situatie dat iemand zonder dat te bedoelen een verklaring aflegt die op redelijke gronden kan worden opgevat als een scherts, terwijl degene tot wie de verklaring is gericht de schijn van scherts ontgaat en daarmee in strijd met de schijn handelt op basis van de werkelijkheid.[3] In dat geval wordt bijna bij toeval aan een waarneming de werkelijke betekenis toegekend.

Schijn kan ontstaan doordat we iets niet hebben waargenomen. Ik zie de hoofdknik van de potentiële koper, maar ik zie niet dat er iemand achter me staat. Ik leg zijn hoofdknik uit als een aanvaarding van mijn aanbod, terwijl hij eigenlijk daarmee zijn vriend wil begroeten. Ik hoor iemand tegen een ander zeggen "Ik betaal je niets meer", maar zie omdat hij met zijn rug naar mij toegekeerd staat niet dat hij lacht en knipoogt naar de ander.

Schijn kan ook ontstaan doordat we iets verkeerd waarnemen omdat onze zintuigen of de hulpmiddelen die we gebruiken bij de waarneming, niet goed functioneren. Door de gebrekkige telefoonverbinding denk ik dat een werkgever zegt "Je bent aangenomen", terwijl hij in werkelijkheid zegt "Je bent niet aangenomen". Het woord "niet" is weggevallen.

Schijn hoeft echter niet gebaseerd te zijn op een onjuiste of beperkte waarneming. Hij ontstaat ook als een verkeerde betekenis wordt toegekend aan een correcte waarneming. Een veilingmeester ziet iemand zijn hand opsteken en denkt dat hij een bod doet. De waarneming is correct maar de betekenis die daaraan wordt toegekend is niet juist, omdat de handopsteker alleen een vriend wilde groeten. Overigens kan ook het omgekeerde zich voordoen, dat de veilingmeester op basis van hetgeen hij waarneemt denkt dat iemand met het opsteken van zijn hand een vriend wil begroeten, terwijl hij in werkelijkheid een bod wil doen.

3 Meijers 1948.

Een verkeerde betekenis toekennen aan een waarneming doet zich bijvoorbeeld ook voor als iemand een ander met een fiets ziet en denkt dat hij de eigenaar is, terwijl hij de fiets slechts te leen heeft. In dit voorbeeld gaat het om een schijn, die ik rechtsschijn zou willen noemen: de schijn ten aanzien van de rechtspositie van degene die de feitelijke macht uitoefent over een object. Feitelijke macht gaat gebruikelijk gepaard met eigendom, zodat feitelijke macht ook de schijn van eigendom oproept.

Schijn ontstaat meestal onbedoeld. Soms is het echter de uitdrukkelijke bedoeling van partijen om een (rechts)schijn te creëren. Met het uitgeven van een cognossement spreken de partijen betrokken bij de vervoerovereenkomst, af dat schijn prevaleert boven werkelijkheid: degene die de feitelijke macht uitoefent over het stuk papier mag door de vervoerder als schuldeiser worden beschouwd. De vervoerder hoeft geen onderzoek in te stellen naar de werkelijkheid.

Vaak wordt een schijn al snel na zijn ontstaan gerepareerd. Degene wiens hoofdknik ten onrechte wordt uitgelegd als een aanvaarding van een aanbod, zal de betekenis van zijn hoofdknik duidelijk maken als de wederpartij vervolgens vraagt of hij dan even de schriftelijke koopovereenkomst wil ondertekenen. De werkgever die een sollicitant afwijst, zal hem snel uit de dromen helpen als hij aan de verheugde reactie merkt dat zijn telefonische mededeling van afwijzing niet goed is overgekomen en begrepen. Het heeft geen pas om een direct gerepareerde schijn juridisch voor werkelijkheid te houden.

Rechtsvermoeden, fictie en feiten van algemene bekendheid

Voordat ik verder inzoom op schijn en recht, een enkel woord over het verschil tussen schijn, rechtsvermoeden, fictie en feiten van algemene bekendheid.

Bij een rechtsvermoeden wordt iets geacht waar te zijn tot op tegenbewijs. Het rechtsvermoeden is gebaseerd op de gebruikelijke werkelijkheid, het meest aannemelijke. Degene die het tegendeel van de gebruikelijke werkelijkheid stelt, moet bij een rechtsvermoeden dat tegendeel bewijzen. Zo bepaalt art. 3:109 BW dat wie een goed houdt, wordt vermoed dit voor zichzelf te houden. Dat is ook de meest gebruikelijke situatie. Beweert iemand het tegendeel, dan zal hij dat dienen te bewijzen.[4]

Er hoeft bij een rechtsvermoeden geen sprake te zijn van een schijn in de betekenis van het verkeerd uitleggen van een waarneming. Wel kan een rechtsvermoeden net als een schijn ertoe leiden dat voor waar wordt aangenomen wat niet waar is omdat degene op wie de last wordt gelegd om het tegendeel te bewijzen daaraan niet kan voldoen.

Anders dan bij schijn gaat het bij een fictie niet om een waarneming waaraan een uitleg wordt gegeven die niet strookt met de werkelijkheid, maar om het zonder waarneming of in strijd met een waarneming voor waar aannemen van iets. Om met Eggens te spreken: een fictie is een voorstelling die onwer-

4 Zie Rank-Berenschot 2001, p. 26-27.

kelijk is.[5] De waarneming kan ontbreken omdat hetgeen waarneembaar is niet is waargenomen of omdat iets überhaupt niet waarneembaar is. In het recht is de verleiding groot om een fictie te gebruiken om een gewenst resultaat te halen. Denk aan het toedichten van bedoelingen aan een contractspartij die zij helemaal niet heeft gehad. Vaak zijn er alternatieve instrumenten voorhanden die hetzelfde resultaat opleveren, maar dan zonder dat daarvoor een fictie hoeft te worden gebruikt. Men kan bijvoorbeeld concluderen dat een overeenkomst een bepaalde inhoud heeft omdat uit de verklaring en het gedrag van een van de partijen mag worden afgeleid dat hij de betreffende rechtsgevolgen heeft gewild. Indien echter het bestaan van de wil wordt ontkend door de betreffende partij, is het zuiverder om in lijn met art. 3:35 BW de schijn van het bestaan van een wil op basis van de omstandigheden aan haar toe te rekenen. Zo voorkomt men het onnodig gebruik van een fictie.

Soms lijkt men er niet aan te ontkomen om een onwerkelijkheid voor waar aan te nemen, omdat er geen werkelijkheid is. Een mooi voorbeeld daarvan treft men aan in het arrest van de Hoge Raad inzake een effectenleaseproduct van Dexia. [6] Dexia voert aan dat een causaal verband tussen het nalaten om de koper in voldoende mate te waarschuwen voor de risico's verbonden aan het specifieke product en de daaruit voortvloeiende schade ontbreekt, omdat de koper de overeenkomst ook zou hebben gesloten als zij hem wel in voldoende mate zou hebben gewaarschuwd. Niemand zal ooit weten wat er zou zijn gebeurd als Dexia wel aan haar waarschuwingsverplichting zou hebben voldaan. Dat blijft gissen. Maar de Hoge Raad geeft in rechtsoverwegingen 5.5.2 en 5.5.3 kort samengevat aan dat als uitgangspunt kan worden genomen dat de koper zonder dat tekortschieten van de aanbieder in diens zorgplicht de overeenkomst niet zou hebben gesloten. Daarmee beantwoordt de Hoge Raad naar mijn mening de vraag in het licht van het bewijsrecht: de koper wordt vermoed de overeenkomst niet te hebben gesloten, tenzij Dexia in voldoende mate het tegendeel aannemelijk maakt. De Hoge Raad vermijdt hierdoor het gebruik van een fictie.

Tot slot feiten van algemene bekendheid. Op grond van art 149 lid 2 Rv mag de rechter aan zijn beslissing feiten en omstandigheden van algemene bekendheid ten grondslag leggen. Deze feiten of omstandigheden hoeven niet te worden gesteld of bewezen. Het betreft een regel van bewijsrecht op grond waarvan een rechter voor werkelijk mag houden hetgeen werkelijkheid is, zonder dat een van de partijen dat hoeft te stellen en te bewijzen. Indien dat voor de toepassing van een rechtsnorm relevant is, hoeft bijvoorbeeld het feit dat het op 31 december om zes uur in de avond donker is, niet te worden gesteld en bewezen. In deze gevallen gaat het – anders dan bij schijn – niet om een verschil tussen de werkelijkheid en de aangenomen werkelijkheid.

---

5 Eggens 1958, p. 5-6: "Want een fictie is een voorstelling die onwerkelijk is. ……. En als we van "rechtsficties" spreken, bedoelen we daarmede het (zich door het rechtsdenken) voorstellen van feiten die niet zijn geschied, als geschied, of -omgekeerd- het voorstellen van feiten die geschied zijn, als niet geschied."

6 HR 5 juni 2009, *LJN* BH2815.

Schijn en het recht

Schijn is een bron van rechtsvragen. Deze vragen zijn niet altijd eenvoudig te beantwoorden omdat de keuze tussen schijn en werkelijkheid meebrengt dat moet worden vastgesteld wie de rekening krijgt gepresenteerd van het ontstaan of het voortduren van de schijn.

Denk aan de discrepantie tussen verklaring en wil. Degene die mondeling, schriftelijk of door middel van gebaren een verklaring aflegt, wekt onder normale omstandigheden de indruk dat hij hetgeen hij verklaart ook wil. Dat is immers de gebruikelijke situatie. Als ik in een winkel tegen de verkoper zeg "De nieuwste cd van Ilse de Lange alstublieft', dan mag de verkoper ervan uitgaan dat ik de nieuwste cd van Ilse de Lange wil kopen. Ontbreekt de wil en zijn er naast de verklaring geen additionele waarnemingen mogelijk die wijzen op het ontbreken van de wil, dan is er sprake van schijn: een schijn van wil. Wat dient het recht te laten prevaleren: de schijn of de werkelijkheid, de verklaring zonder wil of het ontbreken van de wil? De ontvanger van de verklaring heeft en hoeft meestal ook niet in de gaten te hebben dat de wil ontbreekt. Maar ook degene die de verklaring heeft afgelegd zonder haar te willen, hoeft niet noodzakelijkerwijs een verwijt daarvan te kunnen worden gemaakt. Ik verwijs naar het hiervoor gegeven voorbeeld van iemand die met een hoofdknik zijn vriend begroet. Een lastig dilemma, dat in ons recht wordt opgelost aan de hand van de norm neergelegd in art. 3:35 BW.

Denk aan de derde te goeder trouw die een roerende zaak van een beschikkingsonbevoegde koopt. De verkoper blijkt later geen eigenaar, maar slechts huurder te zijn geweest. De koper vertrouwde er op dat feitelijke macht (waarneming) samenging met eigendom, dat schijn werkelijkheid was. Of om in de termen van art. 2014 oud-BW te blijven: dat bezit gelijk stond aan volkomen titel. En de eigenaar vertrouwde op de integriteit van de huurder. Als er geen additionele waarnemingen mogelijk waren die op het tegendeel wezen, wie wordt dan de dupe van de foute handeling van de huurder: de eigenaar of de derdeverkrijger? Deze lastige vraag wordt in ons recht beantwoord in art. 3:86 BW.

Denk aan de schijn van vertegenwoordigingsbevoegdheid. Een vennootschap wordt bestuurd door twee compagnons. In de statuten van de vennootschap staat dat de twee compagnons slechts gezamenlijk bevoegd zijn om namens de vennootschap te handelen. In het handelsregister is hier melding van gemaakt. Een van de twee compagnons is ziek. Een toeleverancier sluit een overeenkomst met het bedrijf. Het bedrijf wordt daarbij vertegenwoordigd door de gezonde compagnon, die meldt dat de ander door ziekte is uitgevallen.[7] Een schijn van vertegenwoordigingsbevoegdheid: de toeleverancier wist van de ziekte van de andere compagnon en ging er op basis van de mededelingen van de gezonde compagnon van uit dat hij onder deze omstandigheden bevoegd was de vennootschap te vertegenwoordigen.

7 Een casus die ik tegenkwam in Rb. Den Haag 1 juli 2009, *LJN* BJ3133.

Wie dient het gelag te betalen: de vennootschap of de toeleverancier? Het antwoord kan worden gevonden door de norm van art. 3:61 lid 2 BW toe te passen.

Denk aan de schijn van schuldeiserschap. Een schuldeiser cedeert zijn vorderingsrecht op naam aan een derde. De schuldeiser en de derde doen hiervan mededeling aan de schuldenaar. Nadien wordt de overeenkomst die ten grondslag ligt aan de overdracht van het vorderingsrecht op naam, vernietigd. De schuldenaar wordt hiervan niet in kennis gesteld en hij betaalt te goeder trouw aan de derde. Dient hij alsnog te betalen aan de schuldeiser? Of wordt hij beschermd omdat hij op redelijke gronden de schijn voor werkelijkheid heeft gehouden? Zie art. 6:34 BW.

En zo kunnen er vast nog andere voorbeelden worden aangedragen van situaties waarin schijn een rechtsvraag oproept.

Is er sprake van schijn en werkelijkheid, dan zal bij de beantwoording van de vraag welke rechtsgevolgen dienen te worden toegekend aan rechtsfeiten, een afweging moeten plaatsvinden. Het antwoord is afhankelijk van de omstandigheden van het geval.

Zo kan van belang zijn of er ten tijde van het vertrouwen op de schijn additionele waarnemingen mogelijk waren die op de werkelijkheid wezen. Indien deze vraag bevestigend moet worden beantwoord, leidt dit tot de vervolgvraag of dan nog wel op redelijke gronden de schijn voor werkelijkheid kon worden gehouden.

Voorts kan van belang zijn of de ander tegen wie de schijn wordt ingeroepen, de oorzaak is van het ontstaan van de schijn. Is dat laatste het geval en kan hem deze schijn worden toegerekend, dan ligt het meer voor de hand om hem de nadelige gevolgen daarvan te laten dragen dan in het geval dat hij aan het ontstaan van de schijn part noch deel heeft.

Schijn verdwijnt waar ICT verschijnt

Bij discrepantie tussen werkelijkheid en de betekenis die iemand aan waarnemingen toekent, zal een keuze moeten worden gemaakt: prevaleert de schijn of de werkelijkheid? Toch onbevredigend, zeker als er sprake is van twee partijen die beiden geen verwijt kan worden gemaakt. Het zou natuurlijk mooi zijn als de noodzaak tot het kiezen kan worden vermeden doordat het ontstaan van schijn kan worden voorkomen.

Mijn stelling in deze bijdrage luidt dat het gebruik van middelen uit de informatie- en communicatietechnologie kan bijdragen aan het vermijden van schijn. Laat ik een aantal voorbeelden geven.

De ontwikkelingen in de informatie- en communicatietechnologie stellen ons in staat om waarnemingen te doen die ons anders onder vergelijkbare omstandigheden zouden ontgaan. Zo biedt bijvoorbeeld videoconferencing ons de mogelijkheid om op afstand met iemand te spreken terwijl we hem tegelijkertijd zien. Videoconferencing voegt aan de waarneming met het gehoor een visuele waarneming toe. Dit kan onder omstandigheden

voorkomen dat aan de waarneming met het gehoor een verkeerde betekenis wordt toegekend. Zo zal bijvoorbeeld een scherts gemakkelijker te herkennen zijn als wij naast het gesprokene ook het gezicht en de gebaren kunnen waarnemen van degene die spreekt. Daarmee kan de kans op het ontstaan van schijn worden verkleind.

Ik wijs in dit verband ook op Van den Herik en Postma die in hun inaugurale rede wijzen op de ontwikkeling van wat zij noemen 'de vriendelijke computer', die in staat is om non-verbale communicatie waar te nemen en daar de juiste betekenis aan te geven.[8] Ook dergelijke hulpmiddelen kunnen ertoe bijdragen dat het ontstaan van schijn zo veel mogelijk wordt vermeden.

De ontwikkelingen in de informatie- en communicatietechnologie kunnen ons ook beter in staat stellen om een juiste (juridische) betekenis aan een overigens correcte waarneming of combinatie van waarnemingen toe te kennen.

In paragraaf 4 kwamen reeds houderschap en bezit aan de orde. Uit art. 3:109 BW volgt dat de houder wordt vermoed bezitter te zijn. En art. 3:119 BW bepaalt dat de bezitter wordt vermoed rechthebbende te zijn. Deze twee bepalingen brengen mee dat de houder wordt vermoed rechthebbende te zijn. Zij vormen een juridische weerspiegeling van de betekenis die in het maatschappelijk verkeer gebruikelijk aan de waarneming dat iemand feitelijke macht over een goed uitoefent, wordt gegeven: namelijk dat hij rechthebbende is. Als ik iemand tegenkom op een fiets, mag ik op basis van de waarneming dat hij de feitelijke macht daarover uitoefent, onder normale omstandigheden aannemen dat hij eigenaar is en bevoegd is om daarover te beschikken. Mocht achteraf blijken dat de juridische betekenis die ik aan deze waarneming heb toegekend, afwijkt van de juridische werkelijkheid, dan dient op basis van art. 3:86 lid 1 BW te worden vastgesteld wie de gevolgen van de ontstane schijn moet dragen, ik of de eigenaar.

Begin jaren tachtig nam ik iemand mondeling tentamen af. Ik vroeg haar op welke wijze een pandrecht werd gevestigd, waarop zij antwoordde: door inschrijving in een register. Waarop ik bedacht dat het toch mooi zou zijn als alle roerende zaken net als onroerende zaken registergoederen zouden zijn. Daarmee zou kunnen worden vermeden dat iemand op goede gronden in strijd met de werkelijkheid aanneemt dat de houder van een roerende zaak rechthebbende is, waardoor een hoop ellende zou kunnen worden voorkomen. In die jaren zou een register voor roerende zaken ondoenlijk zijn geweest. In onze tijd is het echter niet ondenkbaar. De moderne informatietechnieken staan het toe om tegen redelijke kosten grote hoeveelheden informatie op te slaan. Het zou dus ook goed mogelijk zijn om voor roerende zaken die er toe doen, een register in te richten waarin op vrijwillige basis omtrent een zaak gegevens kunnen worden opgenomen waaruit kan worden afgeleid wie op welk moment rechthebbende is. Dit register zou in onze tijd met de moderne communicatiemiddelen gemakkelijk op afstand kun-

8 Van den Herik & Postma 2009, p. 31.

nen worden geraadpleegd. Men zou deze zaken kunnen voorzien van een zogenaamde RFID chip: een minuscule goedkope chip waaruit op afstand gegevens kunnen worden gelezen zoals een unieke code verbonden aan de zaak.[9] Met behulp van de mobiele telefoon zou de koper deze informatie uit de chip kunnen uitlezen om vervolgens op basis van deze informatie het register te raadplegen om te controleren of degene die de feitelijke macht uitoefent ook daadwerkelijk de eigenaar is. Het opzetten van een dergelijk informatiesysteem zou de kans op het ontstaan van schijn en daarmee rechtsgeschillen verkleinen.

Ook de kans op het ontstaan van een schijn van vertegenwoordigingsbevoegdheid zou met behulp van de RFID technologie kunnen worden verkleind. De RFID chip is erg klein. De huidige nanochip is zo groot als een stofdeeltje en kan gemakkelijk onderhuids worden geïmplanteerd. Dat gebeurt thans al bijvoorbeeld om in bepaalde bars snel te kunnen afrekenen. Het is dus mogelijk om een informatiesysteem te ontwikkelen dat met behulp van de onderhuidse chip en een mobiele telefoon realtime online toegang geeft tot een register met gegevens omtrent de procuraties die aan personen zijn verleend. Op basis van de unieke code in de chip zou een sms bericht kunnen worden gestuurd naar degene die de controle uitvoert, met daarin een overzicht van de procuraties van de persoon waarmee hij zaken wil doen. Stelt iemand bijvoorbeeld bevoegd te zijn een bedrijf te vertegenwoordigen en overlegt hij daarbij een visitekaartje van dat bedrijf met zijn naam erop, dan kan door een check met behulp van zo'n informatiesysteem op eenvoudige wijze worden vastgesteld wat de werkelijkheid is. Daarmee kan de kans op het ontstaan van schijn van vertegenwoordigingsbevoegdheid worden verkleind.

ICT, schijn en rechtsvinding

In de vorige paragraaf heb ik enkele voorbeelden gegeven van de toepassing van ICT om de kans op het ontstaan van schijn te verkleinen. Een kwestie van een andere orde is of in geval dat schijn is ontstaan, bij de bepaling van de rechtsgevolgen daarvan rekening dient te worden gehouden met het bestaan van de mogelijkheid om met behulp van ICT de werkelijkheid vast te stellen. Zou bijvoorbeeld de uitspraak in de bekende zaak omtrent de Kantharos van Stevensweert anders zijn uitgevallen als de werkelijke waarde van de kantharos op eenvoudige wijze via internet met behulp van beeldanalyse en patroonherkenning[10] had kunnen worden vastgesteld? Ongetwijfeld zullen de ontwikkelingen op het gebied van ICT ons in de toekomst meer en meer in staat stellen om de werkelijkheid vast te stellen. Waar men

9 RFID staat voor Radio Frequency Identification. Thans worden vele roerende zaken om logistieke redenen al voorzien van een RFID chip.

10 Zie Van de Herik & Postma 2009, p. 38.

zich nu wellicht nog de vraag kan stellen of dat een rol mag spelen bij de toerekening van het ontstaan van schijn, schat ik in dat er een tijd komt dat het gebruik van ICT zo'n gemeengoed is dat dit van invloed is op de toepassing van rechtsnormen waarin open begrippen als 'goede trouw', 'op redelijke gronden' etcetera voorkomen.[11]

Tot slot

De titel van deze bijdrage zou de indruk kunnen wekken dat ik van mening ben dat het gebruik van ICT het ontstaan van schijn kan voorkomen. Dat is natuurlijk niet het geval. Zo kan bijvoorbeeld ook degene die tijdens een videoconference een ander ziet en hoort, diens verklaring verkeerd begrijpen. Bovendien realiseer ik me goed dat er aan het gebruik van bepaalde techniek allerlei bezwaren kunnen kleven, zoals inbreuken op de privacy of de mogelijkheid van grootschalige identiteitsdiefstal. Het gebruik zal dan ook met de nodige waarborgen moeten zijn omkleed, maar de discussie daarover wordt volgens mij al in volle omvang gevoerd zodat het niet nodig is dat ik in deze bijdrage verder daarop inga.

Verwijzingen

Drion 2009
C.E. Drion 'De onderzoekende en/of googelende rechter', *NJB* 2009-13.

Eggens 1958
J. Eggens, *Over het fingeren van rechtsficties*, Haarlem: De Erven F. Bohn, 1958.

Van den Herik & Postma 2009
H.J. van den Herik en E.O. Postma, *Geloof in Computers*, 2009.

Meijers 1948
E.M. Meijers, *De algemene begrippen van het burgerlijk recht*, Leiden: Universitaire Pers 1948, p. 215.

Rank-Berenschot 2001.
E.B. Rank-Berenschot, *Bezit*, Deventer: Kluwer 2001.

Smith 2007
C.E. Smith, *Regels van rechtsvinding*, Den Haag: Boom Juridische Uitgevers 2007.

11 Ik wijs in dit verband op Drion 2009, die aangeeft zijn twijfels te hebben over de juiste toepassing van art. 149 lid 2 Rv. als de rechter informatie die hij door middel van google op het internet heeft gevonden, bestempeld als feiten van algemene bekendheid.

Heeft ICT-recht een eigen methode?

Jaap Hage■

In de loop van de inmiddels meer dan 20 jaren dat Aernout Schmidt zich heeft bezig gehouden met ICT en recht, heeft hij in zijn publicaties zijn licht laten schijnen over vele deelonderwerpen. Maar zoals al uit zijn proefschrift[1] bleek, reikt Aernout's belangstelling verder dan praktisch juridische kwesties. Eén zo'n wat theoretischer onderwerp dat zijn belangstelling heeft is de methode van de rechtswetenschap.

Sinds de subsidiëring van rechtsgeleerd onderzoek mede afhankelijk werd van de goedkeuring van sociale wetenschappers, die methodische eisen stelden aan onderzoeksvoorstellen,[2] is er onder de Nederlandse juristen een opmerkelijke belangstelling ontstaan voor de methoden van rechtswetenschappelijk onderzoek.[3] Dat is niets te vroeg, maar de discussie over de methode(n) van de rechtswetenschap lijdt tot nog toe niet aan een overmatige wetenschapsfilosofische diepgang.[4] Aan de hand van de vraag of ICT-recht een eigen methode heeft (antwoord: 'tot op zekere, maar beperkte hoogte'), wil ik hier proberen dat tekort aan diepgang enigszins te remediëren. In dit verband zal ik de volgende vragen aan de orde stellen:

1. Wat is een wetenschappelijke methode en wat is de rol van zo'n methode binnen een wetenschap?

2. Wat is een goede methode en wat is de relatie tussen een methode en het object van onderzoek?

■ Jaap Hage is hoogleraar aan de Universiteit Maastricht en daarnaast verbonden aan de Universiteit Hasselt.

1 Schmidt 1987.

2 Dat komt doordat het rechtsgeleerde onderzoek bij NWO is ondergebracht bij MAGW, waaraan ook de sociale wetenschappen meedoen.

3 Dat het opeens over rechtswetenschap moet gaan, in plaats van de onder juristen meer gangbare term rechtsgeleerdheid, heeft mogelijk te maken met de provocerende titel van de rede van Stolker 'Ja, geleerd zijn jullie wel.' (Stolker 2003). Overigens pleitte Langemeijer ooit nadrukkelijk voor het handhaven van 'rechtsgeleerdheid', omdat hij een normatieve wetenschap – ten onrechte, zie hieronder – principieel onmogelijk achtte. Zie Langemeijer 1956, p. 290-296.

4 Er was een poging van de Utrechtse rechtseconoom De Geest om tot enige diepgang te komen. Hij pleitte voor een rechtswetenschap gebaseerd op het selecteren van middelen bij voorgegeven doeleinden (De Geest 2004). Deze poging werd ten onrechte afgedaan als zijnde te veel geschoeid op natuurwetenschappelijke leest (Franken 2004). Natuurwetenschappen houden zich namelijk niet (primair) bezig met het selecteren van middelen. Overigens nam De Geest te gemakkelijk aan dat wetenschap niet kan bepalen welke doeleinden moeten worden nagestreefd. Ik kom daar nog op terug.

3. Wat is de geschikte methode voor respectievelijk:
   - kennisverwerving in het algemeen,
   - voor rechtswetenschappelijke kennis in het algemeen en
   - voor ICT-rechtswetenschap in het bijzonder.

Wat is een wetenschappelijke methode?

Geen argumentatie is mogelijk zonder premissen die verder niet meer worden beargumenteerd en dat geldt ook hier. Ik zal beginnen met een premisse over de aard van wetenschapsbeoefening. Die premisse luidt:

> *Wetenschapsbeoefening is een wijze waarop mensen samenwerken bij het verwerven van kennis.*

In het vervolg zal ik, als ik schrijf over wetenschap of wetenschapsbeoefening, steeds het oog hebben op wetenschap in de zin van coöperatieve kennisverwerving.

Samenwerking ten behoeve van kennisverwerving is slechts mogelijk als aan enkele voorwaarden is voldaan. Om te beginnen moet worden aangenomen dat het object[5] van de te verwerven kennis tenminste tot op zekere hoogte identiek is voor allen die bij de samenwerking betrokken zijn. Als ieder zijn eigen 'waarheid' zou hebben, heeft het weinig zin om gezamenlijk te proberen die waarheid op te sporen. De ene wetenschapper zou niet kunnen voortbouwen op de resultaten van de ander. Het valt te betogen dat deze veronderstelling uitsluit dat bijvoorbeeld esthetica ooit als wetenschap beoefend zal worden. Maar ook als men, zoals Soeteman,[6] aanneemt dat recht een discursieve grootheid is, dat juridische waarheid niet empirisch is en zelfs niet van cognitieve aard, maar wordt geconstrueerd, is het niet op voorhand zeker dat rechtswetenschap überhaupt mogelijk is.[7]

De tweede vooronderstelling van wetenschap is dat er binnen de gemeenschap van samenwerkenden tot op grote hoogte overeenstemming bestaat over wat als goede redenen gelden voor het aanvaarden of het verwerpen van een opvatting. [8] Stel dat bijvoorbeeld de ene wiskundige enkel een deductief bewijs zou aanvaarden als reden om een bepaalde stelling te aanvaarden, terwijl een andere wiskundige strikt zou vertrouwen op zintuiglijke waarneming. Het is dan niet aannemelijk dat deze twee wiskundigen zouden samenwerken bij het bouwen aan wiskundige kennis.

---

5 Dit gebruik van het woord 'object' mag niet worden geïnterpreteerd als zou het slechts gaan om kennis van de fysieke werkelijkheid. Ook de sociale werkelijkheid, of een kwestie van moeten of mogen, kan in principe het object zijn van kennisverwerving.

6 Soeteman 2009, p. 5-13.

7 Ik denk dat het hieronder geschetste beeld van een universele methode te rijmen valt met wat Soeteman schrijft, maar dat hetzelfde geldt voor de opvatting dat er in het recht geen waarheid is en dat het spreken van juridische waarheden niet anders is dan retoriek.

8 Ik hanteer 'opvatting' hier al in een technische betekenis die ik later zal uitleggen.

Ongetwijfeld zijn er nog meer randvoorwaarden voor het bestaan van wetenschap, zelfs randvoorwaarden die kunnen worden ontleend aan de hierboven vooronderstelde definitie van wetenschap,[9] maar de twee bovengenoemde volstaan om de rol van methoden in de wetenschap duidelijk te maken. Want wat is een wetenschappelijke methode? In één betekenis is het een wijze van te werk gaan in de wetenschap. Het is een procedure die gevolgd moet worden, wil de uitkomst als 'wetenschappelijk' te boek staan. Voorbeelden van zo'n procedure zouden de empirische cyclus zijn, zoals beschreven door De Groot[10], en de methode van rechtsvinding die door Dworkin werd beschreven in het hoofdstuk 'Hard Cases' van *Taking Rights Seriously*.[11]

In een andere betekenis van 'methode'geeft een wetenschappelijke methode aan wat gelden als goede redenen voor het aanvaarden of verwerpen van een opvatting. De collectieve adoptie van een bepaalde methode in deze zin van het woord komt er op neer dat er overeenstemming bestaat (of ontstaat) over wat als dergelijke goede redenen gelden. Is bijvoorbeeld de uitkomst van een opiniepeiling onder de volwassen bevolking van een land relevant om te bepalen hoe het recht in dat land luidt? Aangezien een dergelijke overeenstemming een noodzakelijke voorwaarde is voor wetenschap, is een gedeelde methode haast per definitie een bestaansvoorwaarde voor wetenschapsbeoefening.[12]

Wetenschappelijke methoden in de zin van wijze van tewerk gaan en in de zin van identificatie van goede redenen voor het aanvaarden of verwerpen van opvattingen hangen nauw samen. In het algemeen geldt dat redenen, en dus ook redenen voor het aanvaarden en verwerpen van opvattingen, *feiten* zijn die *relevant* zijn voor datgene waar het redenen voor of tegen zijn.[13] Zo is het feit dat de Hoge Raad een wettelijke bepaling op een bepaalde manier heeft uitgelegd relevant voor de kennis dat de aldus uitgelegde bepaling deel uitmaakt van het Nederlandse recht. De aanvaarding van een methode is een keuze voor wat als relevant wordt beschouwd. Het is tevens een keuze voor het soort data dat verzameld moet worden teneinde verantwoord te kunnen redenen voor of tegen een opvatting. Als men bijvoorbeeld

9 Te denken valt aan de wijzen van publiceren van de resultaten van wetenschappelijk onderzoek (Stolker 2004; Smits 2007, par. 6.2) en aan de manier waarop de financiering is gorganiseerd.

10 De Groot 1961, hoofdstuk 1.

11 Dworkin 1978, p. 81-130.

12 Dat wetenschap een gedeelde methode veronderstelt, sluit niet uit dat deze methode grotendeels impliciet is, of dat deze in de loop der jaren aan verandering onderhevig is. Als zo'n verandering drastisch is, bijvoorbeeld als de fysica op experimenten wordt gebaseerd in plaats van op de interpretatie van gezaghebbende teksten, dan verandert de aard van de wetenschap ook.

13 De aard van redenen wordt uitvoerig besproken in Hage 1997, hoofdstuk 2.

een hermeneutische methode hanteert voor de rechtswetenschap,[14] dan is het van belang informatie te vergaren omtrent de letterlijke, of de door de opsteller (de wetgever bijvoorbeeld) beoogde betekenis van een gezaghebbende tekst. Een rechtswetenschapper zou zo'n tekst dan moeten raadplegen en deze, zo mogelijk, letterlijk ('grammaticaal' plegen Nederlandse juristen te zeggen), of wetshistorisch moeten interpreteren.[15]

De juiste wijze van het beoefenen van rechtswetenschap, de methode in de eerste zin, wordt in belangrijke mate bepaald door de erkenning van bepaalde soorten informatie als relevant voor de aan de orde zijnde onderzoeksvraag, de methode in de tweede zin. Het is deze tweede zin van 'methode' die in deze bijdrage centraal zal staan en die ik in het onderstaande zal hanteren. Wetenschap is zonder een dergelijke methode welhaast onmogelijk.

Methode en de aard van het kennisdomein

De methode van wetenschap hangt niet in de lucht; hij bestaat niet enkel omdat hij de facto wordt gehanteerd. Normaal gesproken zal een wetenschappelijke methode worden gehanteerd, omdat men vindt dat deze methode leidt tot kennis over het object van de wetenschap. Dat wil zeggen dat de methode deel uit maakt van een theorie over het kennisdomein die meebrengt dat de gehanteerde methode geschikt is om kennis te verwerven.

Neem bijvoorbeeld de natuurwetenschappen. Men veronderstelt dat de natuur 'gehoorzaamt' aan een aantal wetten en dat de gevolgen van die wetten waargenomen kunnen worden. Dit leidt tot een methode waarin waarnemingsgegevens een centrale rol spelen. Deze gegevens leiden tot formulering van theorieën aangaande de inhoud van de wetten en deze theorieën worden getoetst aan (nieuwe) waarnemingsgegevens en zo nodig bijgesteld of geheel verworpen.[16]

In de historische wetenschappen is het anders, maar toch vergelijkbaar.[17] Er wordt aangenomen dat zich in de geschiedenis een aantal gebeurtenissen heeft voorgedaan. Deze gebeurtenissen hebben een aantal 'getuigen' achter-

14 Deze methode is in veel landen waaronder Nederland nog bijzonder populair, blijkens de belangstelling voor het werk van Paul Scholten (Scholten 1974) en Ronald Dworkin (Dworkin 1986). Meer in het algemeen over de hermeneutische methode in de rechtswetenschap schrijft Smith 1997.

15 Ik wil hiermee niet hebben gezegd dat de hermeneutische methode automatisch leidt tot grammaticale of wetshistorische interpretatie, maar slechts dat deze twee interpretatiemethoden goed passen in het spectrum van technieken om betekenis aan een tekst toe te kennen dat in een hermeneutische aanpak wordt gepropageerd. Overigens geldt dat naarmate de hermeneutiek minder specifiek is over de wijze waarop moet worden geïntepreteerd, deze benadering minder een 'methode' is, omdat hij niets voorschrijft.

16 Popper 1963 hoofdstuk 1 en Harré 1985, hoofdstuk 2.

17 Voor een vergelijking tussen de geschiedwetenschap en de natuurwetenschappen, zie Nagel 1974, p. 47 e.v.

gelaten. Dat kunnen schriftelijke stukken zijn, waarin van deze gebeurtenissen verslag wordt gedaan, maar ook (andere) materiële voorwerpen waarvan het bestaan en de aard door de veronderstelde gebeurtenissen wordt verklaard. Ook hier wordt een theorie geconstrueerd op basis van materiaal dat we heden aantreffen en dat we kunnen waarnemen.

De aard van het relevante materiaal is bij de geschiedenis anders dan in de fysische wetenschappen en de te vormen theorieën hebben niet zozeer betrekking op wetmatigheden als op individuele gebeurtenissen en feiten. Voor beide gevallen geldt evenwel dat er een methode is die aangeeft wat relevante informatie is ter ondersteuning van de te vormen theorieën en dat deze methode zelf berust op een theorie over de aard van het kennisdomein en hoe deze aard leidt tot bewijsmateriaal voor of tegen te vormen theorieën.

Typen van rechtswetenschap

Het is niet ongebruikelijk om bij wetenschappelijke methoden te denken aan de methoden van een discipline, bijvoorbeeld van de rechtswetenschap, van de biologie, of van de wiskunde. Strikt genomen is dat onjuist. Wat relevante argumenten zijn voor een conclusie hangt af van het soort vraag, niet noodzakelijkerwijs van de discipline waarbinnen de vraag wordt gesteld. Als bijvoorbeeld binnen de rechtswetenschap de vraag moet worden beantwoord wat de gevolgen zullen zijn van de invoering van een bepaalde regeling, dan zal de methode in beginsel dezelfde zijn als wanneer die vraag wordt gesteld in een sociologische context. En omgekeerd zullen binnen de rechtswetenschap andere argumenten relevant zijn voor de vraag hoe een wettelijke bepaling moet worden uitgelegd dan voor de vraag hoe een bepaalde regeling is te verklaren.

In dit licht lijkt het voor de hand te liggen om onderscheid te maken tussen verschillende vraagtypen en om bij elk type vraag te bepalen welke methode binnen een discipline de facto wordt gehanteerd en welke methode gehanteerd zou moeten worden.[18] Het is dan ook denkbaar dat er binnen een discipline subdisciplines moeten worden onderscheiden, zoals bijvoorbeeld de ICT-rechtswetenschap als subdiscipline van de rechtswetenschap. Dat zou moeten als binnen de ICT-rechtswetenschap *de facto* andere argumenten als relevant zouden worden beschouwd dan in de 'gewone' rechtswetenschap, of als binnen de ICT-rechtswetenschap andere argumenten als relevant zouden *moeten* worden beschouwd. Dat dit het geval is, is in zekere zin vanzelfsprekend, want in de ICT-rechtswetenschap zullen argumenten over privacybescherming relevanter zijn dan in het recht met betrekking tot voedseladditieven, of het bestuursprocesrecht.

18 Zo pleitten Stolker (2003), De Geest (2004) en Van Rhee (2004) voor verschillende methoden, op grond van verschillende soorten onderzoeksvragen die zij als de (juiste) vraagstelling van de rechtswetenschap zagen.

De vraag is of het op een abstracter niveau ook zo is. Als wordt afgezien van de details van de informatie- en communicatietechnologie, zijn dan in de ICT-rechtswetenschap nog steeds andere soorten argumenten relevant dan in de rechtswetenschap in zijn algemeenheid.[19] Ik zal betogen dat er een niet-triviaal abstract niveau is waarop alle wetenschappen dezelfde methode hebben en dat de concretere methoden van de verschillende wetenschappen alle concretiseringen zijn van deze 'algemene' methode. Enkel in die zin heeft ook de ICT-rechtswetenschap een eigen methode, namelijk de op de ICT toegespitste concretere versie van de algemene methode.

Rechtsgeleerdheid als onderhoud aan het rechtssysteem

Alvorens in te gaan op de algemene methode van wetenschappen, wil ik kort ingaan op de mogelijkheid dat de rechtsgeleerdheid geen wetenschap is en dat ook niet aspireert te zijn. Ik heb wetenschap namelijk gedefinieerd als coöperatieve kennisverwerving en mogelijk gaat het bij de rechtsgeleerdheid, althans bij een centraal onderdeel daarvan namelijk de dogmatische rechtsgeleerdheid, helemaal niet om kennisverwerving. Een plausibele interpretatie van de dogmatische rechtsgeleerdheid is namelijk dat deze zich bezighoudt met het *onderhoud van het rechtssysteem*. Dit onderhoud houdt in dat wordt bijgehouden wat het recht inhoudt, wat de inhoud van het recht verklaart en – hetgeen in de ogen van sommigen haast op hetzelfde neer komt – welke doeleinden met het recht worden nagestreefd. Er is een continu proces gaande van het bijhouden van de inhoud van het recht door nieuwe wetgeving, jurisprudentie en literatuur te verwerken en van het bijsturen van het recht door het te systematiseen en door te evalueren in hoeverre het recht zijn functies vervult en hoe het zou moeten worden aangepast teneinde deze functies nog beter te vervullen. Dit proces van onderhoud aan het rechtssysteem, of althans het leveren van een bijdrage daaraan, zou de (primaire) taak zijn van de dogmatische rechtsgeleerdheid.

Het onderhoud van het rechtssysteem is onmiskenbaar een intellectuele activiteit die moet voldoen aan maatstaven die even streng zijn als die van een wetenschap. Sterker nog, het moet gebruik maken van rechtswetenschappelijke kennis waar die beschikbaar is. maar dat maakt deze rechtsgeleerdheid niet tot rechts*wetenschap*, want onderhoud is geen kennisverwerving.

Met excuses bij voorbaat aan zowel de tandartsen als de rechtsgeleerden, zou ik een parallel willen trekken tussen wat een dogmatische rechtsgeleerde doet en wat een tandarts doet. Een tandarts verricht onderhoud aan een gebit, zoals een rechtsgeleerde dat doet aan het rechtssysteem, met dit ver-

19 Ik neem nu maar even aan dat er zoiets bestaat als de rechtswetenschap in zijn algemeenheid en de argumenten die daarbinnen relevant zijn. Maar ik betwijfel of deze aanname correct is.

schil dat de tandarts ook daadwerkelijk ingrijpt, terwijl de rechtsgeleerde zich veelal beperkt tot adviezen aan wetgevers en rechters over hoe zou moeten worden ingegrepen. Net zoals een tandarts hooggeschoold dient te zijn om haar werk goed te doen, moet een jurist hooggeschoold zijn om zijn werk deskundig te verrichten. Beiden moeten idealiter de meest recente wetenschappelijke kennis gebruiken om het onderhoud zo goed mogelijk te verrichten. Maar geen van beiden heeft als zodanig[20] tot doel om de hoeveelheid kennis op haar of zijn vakgebied te vergroten.[21]

Het verschil tussen de aldus opgevatte rechtsgeleerdheid en wetenschappen die zijn gericht op kennisverwerving wordt nog duidelijker als we zien wat wordt gedaan met de resultaten van een rechtsgeleerde discussie. In zo'n discussie worden argumenten aangevoerd over de uitleg van de bronnen van het recht, over hoe regelingen verklaard kunnen worden en over wat een goede regeling van een bepaalde kwestie zou zijn. In zoverre zou de rechtsgeleerde discussie nog kunnen worden opgevat als een deel van de wetenschap. Maar de discussie wordt niet almaar gecontinueerd zolang er geen eenduidig antwoord op de vragen voorhanden is. Zeker als het er om gaat hoe het recht in de toekomst moet luiden, wordt de discussie na enige tijd afgebroken en neemt een gezagsdrager, een rechter of een wetgever, een besluit en vanaf dat moment geldt de inhoud van dit besluit als geldend recht. Dat is een rationele aanpak als het er om te doen is om menselijk gedrag te sturen en om de daarvoor benodigde zekerheid te bewerkstelligen. Vanuit het perspectief van kennisverwerving is het, om het voorzichtig te zeggen, ongebruikelijk dat iemand een besluit kan nemen over wat de beste opvatting over het kennisobject is.

Als men de functie van de rechts*wetenschap* identificeert met de rechts*geleerdheid* zoals hierboven omschreven, dan dient de methode van de rechtswetenschap die van een gespecialiseerde variant van rationele besluitvorming te zijn. Daar gaat deze bijdrage niet over.

Geïntegreerd coherentisme

We zullen nu verder uitgaan van de veronderstelling dat de rechtswetenschap pretendeert een wetenschap te zijn, dat wil zeggen gericht op het coöperatief verwerven van kennis over het recht. Ik zal betogen dat er een algemene 'methode' is voor kennisverwerving, waarvan de wetenschap een speciaal

20 Vanzelfsprekend kunnen zowel tandartsen als rechtsgeleerden tijdelijk uit hun onderhoudsrol stappen en wetenschap produceren. Sterker nog, hun onderhoudswerkzaamheden zullen vaak leiden tot kennis die van pas komt in de productie van wetenschap. Maar dat maakt hun onderhoudswerkzaamheden nog niet tot wetenschapsbeoefening.

21 Men zou nog kunnen tegenwerpen dat het gaat om toegepaste wetenschap. Maar ik zou toegepaste wetenschap willen onderscheiden van het toepassen van wetenschap. De eerste is gericht op praktijkgerichte kennisverwerving, terwijl de laatste niet gericht is op kennisverwerving. De grens tussen beide zal echter niet altijd eenvoudig te trekken zijn.

geval is. De rechtswetenschap en de ICT-rechtswetenschap zijn daar dan weer verdere specialiseringen van. Een paar bladzijden zijn wat krap om een algemene methode van kennisverwerving uiteen te zetten, laat staan die te rechtvaardigen. Ik zal daarom, vrees ik, nogal apodictisch moeten zijn.[22]

Volgens Plato is kennis gerechtvaardigde ware mening.[23] Omdat de waarheid van een mening niet anders kan worden getoetst dan door na te gaan of de mening is gerechtvaardigd, kunnen we de eis van waarheid binnen het kader van een methode laten rusten.[24]

Rechtvaardiging is – anders dan waarheid – relatief ten opzichte van een zekere achtergrond die de rechtvaardiging vormt. Zo is de opvatting dat het regent gerechtvaardigd voor wie al de opvattingen huldigt dat hij het ziet regenen en dat zijn ogen en de waarnemingsomstandigheden betrouwbaar zijn. Een mening is nooit op zichzelf gerechtvaardigd. In dit opzicht is gerechtvaardigd zijn dus heel iets anders dan waar zijn.

De achtergrond waartegen een bepaald kenniselement is gerechtvaardigd zal vaak bestaan uit het geheel van opvattingen van een concrete persoon. De rechtvaardiging waar het dan om gaat is de gerechtvaardigdheid van die persoon in het er op na houden van een bepaalde opvatting.[25] In dat geval is een opvatting gerechtvaardigd (voor een bepaalde persoon) als de persoon die de opvatting er op na houdt daarin gerechtvaardigd is, gegeven alle andere opvattingen die hij er niet ten onrechte op na houdt.

Een opvatting is gerechtvaardigd als de redenen voor het (als waar) aanvaarden daarvan zwaarder wegen dan de redenen die daartegen pleiten. Dat de redenen zwaarder wegen is zelf een onderdeel van de achtergrond, net als de redenen zelf. Of een opvatting gerechtvaardigd is, hangt af van *alle* redenen die daar voor of tegen pleiten. Dat wil zeggen dat de *gehele achtergrond* potentieel relevant is voor de rechtvaardiging van elke opvatting.

Een reden is een *feit* dat relevant is voor een conclusie. Een reden kan enkel dan bijdragen aan de rechtvaardiging van een opvatting als de mening dat die reden (dat feit) zich voordoet zelf ook gerechtvaardigd is. Wie als reden voor het aandoen van een regenjas opvoert dat het regent, is slechts gerechtvaardigd in haar opvatting dat ze een regenjas moet aandoen als ze gerechtvaardigd is in haar mening dat het regent.

---

22 De geïnteresseerde lezer kan meer vinden in Hage 2005 en hoewel niet uitsluitend, toch wel voornamelijk het tweede hoofdstuk daarvan: Law and Coherence.

23 Plato, *Theaetetus*, 148E.

24 Dat kennis ook 'waar' zou moeten zijn wordt relevant als het gaat om opvattingen waarvan wordt geloofd dat ze voor iedereen hetzelfde zouden moeten zijn. Zo gaan fysici er gewoonlijk van uit dat de natuur voor iedereen hetzelfde is. Literatuurcritici nemen niet standaard aan dat er maar één juiste interpretatie is van een literair werk. Juristen discussiëren erover of juridische vragen 'one right answer' (Dworkin 1978) hebben. Als men pleegt aan te nemen dat een bepaalde vraag precies één juist antwoord heeft, zal dat implicaties hebben voor wat men als goede redenen beschouwt.

25 Het is me dus te doen om wat Neta en Pritchard omschrijven als 'propositional justification'. Zie Neta & Pritchard 2009, p. 151.

Een reden is bovendien een feit dat *relevant* is voor een conclusie. Relevantie van een feit staat nooit op zichzelf. Als het feit dat het nu regent relevant is voor de kwestie of X nu een regenjas moet aandoen, zal het soort feit 'het regent' relevant zijn voor de soort conclusie 'X moet een regenjas aandoen'. De relevantie van een bepaald soort feiten voor een bepaald soort conclusies kan worden uitgedrukt in de vorm van een algemene conditionele zin:

feiten van type X pleiten voor/tegen conclusies van type Y

Als men feiten van type X als redenen aanvaardt voor conclusies van type Y, komt dat er op neer dan men deze conditionele zin aanvaardt.

Het is nuttig om een algemene term te hebben die alle mogelijke onderdelen omvat van de achtergrond waartegen opvattingen gerechtvaardigd zijn. Ik stel voor daarvoor de term 'opvatting' te gebruiken. Opvattingen omvatten niet alleen meningen omtrent de feiten, maar ook de conditionele zinnen waarvan aanvaarding bepaalde feiten relevant maakt voor bepaalde conclusies, waarden, doeleinden die moeten worden nagestreefd, beginselen, regels, 'gewichten' van redenen, prioriteiten van regels enz. Opvattingen kunnen nadrukkelijk ook worden uitgedrukt door normatieve zinnen. Ze omvatten dus ook de sfeer van het moeten, niet enkel die van het zijn.[26] De hierna voorgestelde methode is daarom evenzeer van toepassing op zuiver feitelijke, als op evaluatieve en op normatieve oordelen.[27]

Alles dat van belang is voor het gerechtvaardigd zijn van een opvatting is volgens deze omschrijving zelf ook een opvatting.

Een persoon P is gerechtvaardigd in het er op na houden van een opvatting, als deze opvatting gerechtvaardigd is tegen de achtergrond van *alle opvattingen* die P er gerechtvaardigd op na houdt.

Deze omschrijving van het gerechtvaardigd er op na houden van een opvatting is circulair, maar niet op een kwalijke manier. Het is de uitdrukking van een coherentietheorie over rechtvaardiging, die ik elders heb omschreven als 'geïntegreerd coherentisme'.[28] Het gaat om *coherentisme*, omdat alle opvattingen in beginsel voor hun rechtvaardiging met elkaar samenhangen. Het coherentisme is *geïntegreerd*, omdat de voorwaarden waaronder bepaalde opvattingen andere opvattingen ondersteunen (uitgedrukt in de eerder genoemde universele conditionele zinnen) onderdeel uitmaken van de achtergrond en niet onafhankelijk daarvan zijn gedefinieerd.

---

26 Overigens ben ik van mening dat de tegenstelling zijn/behoren (is/ought; Sein/Sollen) een schijntegenstelling is. Een betere tegenstelling (driedeling) is die tussen beweerzinnen, feiten en regels. In al deze drie categorieën kan een behoren voorkomen, maar ook een zijn dat geen behoren is. Zie Hage 2005, p. 171 e.v.

27 Een vergelijkbare uniformiteit van methode werd reeds bepleit door Popper. Zie Popper 1966, p. 369 e.v.

28 Hage 2005, hoofdstuk 2.

Het valt mogelijk op dat de omschrijving van wanneer iemand gerechtvaardigd er een bepaalde opvatting op na houdt geen verwijzing bevat naar zintuiglijke waarneming, in de ogen van velen toch de bron van kennis bij uitstek. De reden hiervoor is dat zintuiglijke waarneming leidt tot 'spontane' opvattingen die deel gaan uitmaken van het geheel van opvattingen. Dat geheel wordt onderworpen aan de kritische toets van coherentie en wat daaruit resteert is de gerechtvaardigde kennis. Opvattingen worden dus niet rechtstreeks getoetst via zintuiglijke waarneming, maar door een controle op coherentie met de opvattingen die – onder meer – via zintuiglijke waarneming ontstaan.

Hoofdlijnen van een universele methode

Uit de hierboven in heel grote lijnen geschetste theorie over de rechtvaardiging van opvattingen volgt een universele methode voor het verwerven van kennis, of meer in het algemeen gerechtvaardigde opvattingen. Ik zal twee formuleringen van deze methode geven. De eerste geeft aan wat de methode idealiter zou inhouden. Dit ideaal is praktisch niet te realiseren en daarom is er ook een tweede versie die wel realiseerbaar is en die beoogt de best mogelijke benadering op te leveren van de ideale methode. Of de tweede versie inderdaad de best mogelijke benadering is, is zelf weer een opvatting die voor revisie in aanmerking komt in het licht van alle terecht aanvaarde opvattingen.

De universele methode voor kennisverwerving in zijn ideale variant luidt:

> Aanvaard die opvattingen die tezamen met *alle* andere aanvaarde opvattingen een samenhangend geheel vormen.

Wat in dit verband samenhangend is, wordt bepaald door het geheel van aanvaarde opvattingen.[29] In zoverre is de voorgestelde universele methode 'leeg', bijna nietszeggend. Bijna, want hij zegt wel dat de maatstaven die moeten worden aangelegd bij de aanvaarding van opvattingen zelf moeten samenhangen met alle andere aanvaarde opvattingen.

Dit brengt mee dat de aard van de wetenschappelijke methode moet samenhangen met de gehanteerde opvatting over de aard van wetenschap (coöperatieve kennisverwerving, bijvoorbeeld).

Idealiter zou iedere opvatting geëvalueerd worden in het licht van alle andere opvattingen. Dat zou al een Herculeaanse taak zijn als het enkel ging om het evalueren van een opvatting over het recht in een concreet geval in het licht van alle rechtsbronnen en de opvattingen over recht en politiek,[30]

29 De technische details van wat dit inhoudt zijn weer te vinden in Hage 2005, hoofdstuk 2.
30 Vgl. Dworkin 1978, hoofdstuk 4.

maar de taak overschrijdt zelfs de capaciteiten van Hercules als daar alle overige opvattingen bij zouden komen. Wat nodig is, is een beperktere versie van de universele methode, een versie die realistisch is in het licht van de menselijke vermogens. Overigens is het hierbij niet nodig om af te gaan op de vermogens van individuele mensen. Mensen werken samen om kennis te verwerven en een vereenvoudigde methode van kennisverwerving mag een methode zijn van coöperatieve kenisverwerving, van wetenschap dus.[31]

Zo'n eenvoudiger methode kan worden gebaseerd op een combinatie van twee moderne inzichten over de rechtvaardiging van opvattingen. Het ene inzicht is dat een opvatting gerechtvaardigd kan zijn in het licht van een beperkte verzameling andere opvattingen, maar dat die rechtvaardiging niet meer opgaat in het licht van een grotere verzameling van opvattingen.[32] Het andere inzicht is dat de verzameling opvattingen die fungeert als achtergrond waartegen een bepaalde opvatting wordt geëvalueerd de uitkomst is van een proces waarin nieuwe opvattingen kunnen worden geïntroduceerd en waarin bestaande opvattingen ter discussie kunnen worden gesteld in het licht van nieuw geïntroduceerde opvattingen.[33]

Als deze twee inzichten worden gecombineerd blijkt dat de rechtvaardiging van een bepaalde opvatting in de loop van tijd kan evolueren, omdat er nieuwe opvattingen kunnen worden geïntroduceerd die impact hebben op de status van de te evalueren opvatting. Dit proces van introduceren van nieuwe opvattingen kan aan regels worden gebonden en die regels kunnen zelf weer worden geëvalueerd in het licht van alle overige opvattingen, waaronder die omtrent de relevantie van eventuele nieuwe opvattingen.[34] Overigens is het niet zo dat een aldus geïntroduceerde opvatting automatisch aanvaard wordt. Het betekent enkel dat die wordt meegenomen in het construeren van een samenhangend geheel van opvattingen. Het is dus goed mogelijk dat een opvatting wel aan het geheel van opvattingen kan worden toegevoegd, maar daar direct weer uit wordt verwijderd vanwege inconsistentie met andere opvattingen.[35]

---

31 Dit thema werd benadrukt door Popper in zijn opstel 'Epistemology Without a Knowing Subject'. Popper 1972, p. 106-152.

32 Het gaat hier om wat wel 'defeasibility' wordt genoemd. Een uitvoeriger bespreking van wat defeasibility inhoudt en hoe die samenhangt met de rechtvaardiging van opvattingen is te vinden in Hage 2005, hoofdstuk 1.

33 Meer hierover in Hage 2005, hoofdstuk 8.

34 Dergelijke regels bestaan heel nadrukkelijk binnen het procesrecht, maar impliciet ook binnen de gangbare wetenschappen als (impliciet) de eis wordt gesteld dat nieuwe argumenten gepubliceerd moeten worden in tijdschriften met een bepaalde beoordelingsprocedure.

35 Technisch bezien komt dit er op neer dat er niet alleen een inhoudelijke test is op coherentie van opvattingen, maar ook een procedurele.

De vereenvoudigde methode luidt dan als volgt:

a. Aanvaard die opvattingen die passen binnen het samenhangende geheel van opvattingen dat momenteel aanvaard wordt als relevant voor de aan de orde zijnde kwestie.

b. Het is toegestaan om nieuwe opvattingen toe te voegen aan het geheel van aanvaarde opvattingen, mits deze toevoeging voldoet aan de procedurele voorwaarden die deel uitmaken van het geheel van momentaan aanvaarde opvattingen.

Object en methode van de rechtswetenschap

Eigenlijk is hiermee alles gezegd wat er neutraal, dat wil zeggen zonder keuzes te maken, gezegd kan worden over de methode van kennisverwerving, van wetenschap in het algemeen en van rechtswetenschap in het bijzonder. De wetenschappelijke methode hangt af van wat men als wetenschap ziet, dat wil zeggen van de inhoud van het geheel van aanvaarde opvattingen. Wil de analyse van hoe rechtswetenschap zou moeten worden beoefend worden voortgezet, dan moeten we het neutrale terrein van de abstracte analyse van kennisverwerving verlaten en een bepaalde opvatting verdedigen over hoe kennis het best kan worden bereikt. Het volgende moet dan ook worden gezien als een aanzet tot zo'n inhoudelijke opvatting, die voor revisie vatbaar is.

Laten we, zoals aan het begin van deze bijdrage gepostuleerd, aannemen dat wetenschap bestaat uit coöperatieve kennisverwerving. De volgende vraag is dan wat de meest geëigende vorm is van coöperatieve kennisverwerving met betrekking tot het recht.[36] Het antwoord op deze vraag, dat ik wederom in heel grote lijnen zal proberen te schetsen in de volgende paragraaf, kan dan eventueel nog verfijnd worden tot een antwoord op de vraag wat de meest geschikte methode is om kennis te verwerven met betrekking tot het ICT-recht.

Kennisverwerving met betrekking tot het recht veronderstelt een theorie over de aard van het recht die impliceert welke methode het meest geschikt is om die kennis te verwerven. Recht heeft twee dimensies die elkaar op het eerste gezicht bijten.[37] Aan de ene kant wil het recht richting geven aan menselijk gedrag en is de vraag naar de inhoud van het recht een normatieve vraag: hoe moeten we handelen? Dat deze vraag in een juridisch kader wordt gesteld kan maken dat het juridische antwoord op de vraag anders luidt dan wanneer de vraag wordt opgevat als bijvoorbeeld een morele

36 Eigenlijk is hier nog differentiatie nodig voor wat betreft de verschillende soorten kennisvragen die mogelijk zijn met betrekking tot het recht. Ik beperk me hier tot een beschrijving van de inhoud van het recht.

37 De twee dimensies worden uitvoeriger beschreven in Hage 2009.

vraag, of als een vraag over het eigenbelang, maar dat doet niet af aan het wezenlijk normatieve karakter van de vraag.

Aan de andere kant lijkt de vraag naar de inhoud van het recht een zuiver feitelijke. Recht bestaat in de vorm van het recht van een bepaalde jurisdictie en dit recht bestaat in de vorm van een (complexe) sociale praktijk.[38] Hoe het recht luidt is een vraag die beantwoord kan worden door de bestudering van de rechtsbronnen van de jurisdictie in kwestie. In Nederland zal het dan gaan om wetgeving (formeel en materieel), richtlijnen, verdragen, jurisprudentie, in het rechtsbewustzijn levende rechtsbeginselen[39] en juridische literatuur.

Mijns inziens is de opvatting van het recht als antwoord op een (speciale variant van) de vraag hoe we moeten handelen meer bevredigend dan de opvatting van het recht als sociaal verschijnsel, of een combinatie van de twee. Als het recht zuiver een sociaal verschijnsel zou zijn, zou er geen recht zijn waar de sociale praktijk onvoldoende ontwikkeld of uniform is. Dworkin heeft mijns inziens overtuigend betoogd dat het recht zo niet werkt: ook in moeilijke gevallen redeneren juristen alsof er recht is dat moet worden 'gevonden'.[40]

De opvatting dat het recht een sociaal verschijnsel is waar er een voldoende uniforme sociale praktijk is en dat het voor de rest een normatieve kwestie is, is onbevredigend. Enerzijds omdat deze opvatting zou inhouden dat er eigenlijk twee soorten recht zijn, feitelijk en normatief, terwijl alleen sommige rechtstheoretici[41] dit zo zien en anderzijds omdat de gesuggereerde grenzen aan het feitelijk bestaande recht in praktijk niet als zodanig worden ervaren.

De opvatting dat het recht het antwoord is op een bepaald soort normatieve vraag is wel bevredigend, omdat deze opvatting goed rekening kan houden met het feitelijk bestaande recht. Het is namelijk wenselijk dat er binnen een samenleving regels bestaan die het gedrag van de deelnemers coördineren. Een dergelijke coördinerende functie kan slechts worden gerealiseerd als die regels in beginsel voor iedereen kenbaar zijn en als er geen principiële meningsverschillen mogelijk zijn over de inhoud daarvan. Het positieve recht, met duidelijk kenbare en begrijpelijke bronnen, is een manier om deze coördinerende functie te realiseren. Het is dus wenselijk om dergelijk positief recht te hebben en slechts als het positieve recht bijzonder slecht is, is het wenselijk om het niet meer als richtlijn voor gedrag te hanteren.[42]

---

38 Dat het recht bestaat als een sociale praktijk is een centraal thema in Hart 1994. Dit thema wordt nader uitgewerkt in Patterson 2009.

39 Dat de beginselen in het rechtsbewustzijn leven is hier cruciaal, want dat maakt het in beginsel mogelijk om het bestaan van die beginselen te verifiëren door sociaal-psychologisch onderzoek. Daar zal niet iedereen het mee eens zijn, maar dat komt omdat niet iedereen vindt dat het recht in wezen een sociaal – en dus feitelijk – verschijnsel is.

40 Dworkin 1978, hoofdstuk 2.

41 Zie bijvoorbeeld Brouwer 1999.

42 Rechtsfilosofen zullen in deze korte redenering ongetwijfeld argumenten uit de natuurrechtelijke sfeer (o.a. Thomas van Aquino, Fuller en Radbruch) herkennen.

Als deze opvatting over de aard en functie van het recht wordt aanvaard, is het criterium voor het al dan niet aanvaarden van een opvatting over het recht of de opvatting bijdraagt aan het realiseren van deze functie. De rechtswetenchap is dan een normatieve wetenschap, die zich ten diepste bezighoudt met de vraag hoe we moeten handelen en in dat licht met de vraag welke regels we moeten hanteren om een aantrekkelijke vorm menselijk samenleving mogelijk te maken. Binnen dat kader speelt het positieve recht een wezenlijke rol.

ICT-recht

Wat betekent dit voor de methode van de ICT-rechtswetenschap? Bij het vaststellen van welke regels we moeten hanteren moet in sterke mate rekening worden gehouden met de aard van het te regelen domein. Inzicht in het domein is daarom een factor die van cruciaal belang is bij het bepalen van wat het recht voor dat domein inhoudt.[43] Er is geen duidelijke scheiding tussen domeinkennis en juridische kennis; de methode van de rechtswetenschap is domeinafhankelijk.

Dit brengt mee dat de rechtswetenschap op het gebied van informatie- en communicatietechnologie een grondige kennis van dit domein veronderstelt, al was het maar om de praktische consequenties van regelgeving op dit gebied te kunnen inschatten. In deze – het zij toegegeven, zeer beperkte – zin heeft de ICT-rechtswetenschap een eigen methode, net zoals de rechtswetenschap eigen methodes heeft voor alle gespecialiseerde domeinen. Maar al deze methodes zijn specialisaties van de methode van de rechtswetenschap, die weer een speciale variant is van de wetenschappelijke methode en de algemene methode van kennisverwerving.

Verwijzingen

Austin 1954
J. Austin, *The Province of Jurisprudence Determined*, herdruk van de Weidenfeld & Nicholson editie van 1954, Indianapolis: Hacket 1998. Origineel uit 1832.

Brouwer 1999
P.W. Brouwer, 'Onvermijdelijke rechtsonzekerheid?', *Rechtsfilosofie en Rechtstheorie* 1999, p. 188-209. Ook in Hol en Hage 2008, p. 177-204.

Cliteur 1997
P.B. Cliteur e.a. (red.), *Rechtsfilosofische stromingen van de twintigste eeuw*, Deventer: Gouda Quint 1997.

43 Let op: omdat de aard van de rechtswetenschap in de hier voorgestane visie normatief is, gaat het om de vraag naar de inhoud van het recht en niet – zoals Austin zou stellen – om de vraag naar wat wenselijk recht zou zijn. Vgl. Austin 1954, p. 184.

Dworkin 1978
R. Dworkin, *Taking Rights Seriously*, 2e druk, Londen: Duckworth 1978.

Dworkin 1986
R. Dworkin, *Law's Empire*, Londen: Fontana 1986.

Franken 2004
H. Franken, 'Rechtsgeleerdheid in de rij der wetenschappen', *NJB* 2004, p. 1400-1408.

De Geest 2004
G. de Geest, 'Hoe maken we van de rechtswetenschap een volwaardige wetenschap?', *NJB* 2004, p. 58-66.

De Groot 1961
A.D. de Groot, *Methodologie*,'s-Gravenhage: Mouton 1961.

Hage 1997
J.C. Hage, *Reasoning with Rules*, Dordrecht: Kluwer 1997.

Hage 2005
J.C. Hage, *Studies in Legal Logic*, Dordrecht: Springer 2005.

Hage 2009
J.C. Hage, 'Recht als sociaal feit en recht als praktische rede', *Rechtsfilosofie en Rechtstheorie* (38), 2009, p. 27-36.

Hage en Von der Pfordten (2009)
J.C. Hage en D. von der Pfordten (red.), *Concepts in Law*, Dordrecht: Springer 2009 (in druk).

Harré 1985
R. Harré, *The Philosophies of Science*, 2e druk, Oxford: Oxford University Press 1985.

Hart 1994
H.L.A. Hart, *The Concept of Law*, 2e druk, Oxford: Clarendon Press 1994.

Hol en Hage 2008
A. Hol en J. Hage (red.), *Coherentie, rechtszekerheid en rechtspositivisme. Verspreide opstellen van prof. mr. P.W. Brouwer (1952-2006)*, Den Haag: BJu 2008.

Langemeijer 1956
G.E. Langemeijer, *Inleiding tot de studie van de wijsbegeerte des rechts*, Zwolle: Tjeenk Willink 1956.

Nagel 1974
E. Nagel, *The Structure of Science*, 4e druk, Londen: Routledge & Kegan Paul 1974.

Neta en Pritchard 2009
R. Neta en D. Pritchard (red.), *Arguing About Knowledge*, Londen: Routledge 2009.

Patterson 2009
D. Patterson, *'After Conceptual Analysis. The Rise of Practice Theory'*, te verschijnen in Hage en Von der Pfordten 2009.

Popper 1966
K.R. Popper, *The Open Society and its Enemies.. Volume 2: Hegel & Marx*, 5e druk, Londen: Routledge & Kegan Paul 1966.

Popper 1972
K.R. Popper, *Objective Knowledge*, Oxford: Clarendon Press 1972.

Van Rhee 2004
C.H. van Rhee, 'Geen rechtsgeleerdheid, maar rechtswetenschap!', *Rechtsgeleerd Magazijn Themis* 2004, p. 196-201.

Schmidt 1987
A.H.J. Schmidt, *Pallas ex machina. Informele systemen in verband met het recht*, Lelystad: Vermande 1987.

Scholten 1974
Asser-Scholten (Algemeen deel), Zwolle: Tjeenk Willink 1974.

Smith 1997
C.E. Smith 'Hermeneutiek', in: Cliteur 1997, p. 233 e.v.

Smits 2007
Naar prestatie-indicatoren voor rechtswetenschappelijk ondezoek. Rapport van de Commissie Prestatie-indicatoren en ranking ('commissie Smits'), ingesteld door het Disciplineoverleg Rechtsgeleerdheid (DRG) van de VSNU.

Soeteman 2009
A. Soeteman, *Rechtsgeleerde waarheid*, afscheidsrede Vrije Universiteit Amsterdam 2009.

Stolker 2003
C.J.J.M. Stolker, '"Ja, geléérd zijn jullie wel!" Over de status van de rechtswetenschap', *NJB* 2003, p. 766-778.

Stolker 2004
C.J.J.M. Stolker, 'Wat maakt een juridisch tijdschrift wetenschappelijk?', *NJb* 2004, p. 1409-1418.

Van registratie naar verwerking

Jaap van den Herik■

Samenvatting

Drieëntwintig jaar heb ik met Aernout Schmidt mogen samenwerken. In die tijd heeft zich een stormachtige ontwikkeling in de juridische wereld voltrokken. Wij hebben daar aan deelgenomen samen met Hans Franken en vele anderen. Een volledig overzicht is moeilijk te geven, want er is veel gebeurd. In deze bijdrage wil ik de stimulerende rol van Aernout belichten. Van *Pallas ex Machina* tot ANITA. Van Mr. tot Dr. tot Professor. Twee conclusies zijn onlosmakelijk aan deze periode verbonden. (1) Informatica-toepassingen zijn ongelooflijk veelzijdig in de rechtspraak. (2) Dankzij de nieuwste ontwikkelingen op het gebied van automatische computermodellen zijn we nu op weg naar het nemen van juridisch correcte beslissingen.

Introductie

In onze samenleving zijn computers op geheel verschillende manier ontvangen. Bij de rekencentra werden ze met open armen ontvangen, omdat ze zo goed konden rekenen (optellen, aftrekken etc.). Dat gold ook voor de geheime dienst. Zo gebruikte de MI 5 (Bletchley Park, Engeland) een computer voor het breken van de code van de Duitse onderzeeboten, en de onderzoekers in Los Alamos spendeerden hun vrije tijd aan het ontwikkelen van een schaakprogramma op de nieuwste, zojuist binnengereden computer. Oppenheimer vond het goed. De techniek schreed voort. De mogelijkheden waren onvoorzienbaar.[1]

In het begin van de jaren tachtig van de vorige eeuw ontmoette ik Ernst Enschedé (van de schaakclub DD in Den Haag) bij een wedstrijd DD 2 – Overschie. Hij wist dat ik met onderzoek op het gebied van computerschaak bezig was en zei: "Die computers van jou, wat zou mijn vader daar veel aan gehad hebben. Hij had al zijn jurisprudentie in grote kaartenbakken en wist daar tot op hoge leeftijd zijn weg goed in te vinden. Maar het werd steeds moeilijker."[2] Ik begreep het: de registratie van de jurisprudentie in een com-

■ Jaap van den Herik is hoogleraar bij eLaw@Leiden, Universiteit Leiden en bij TiCC, Tilburg University.

1 Van den Herik 1983.

2 Cf. Enschedé 1966.

puter zou het zoeken daarin vergemakkelijken. De volgende stap zou dan zijn: het verbeteren van de zoekprocessen. Ik droomde verder: als de programma's dan gevonden hadden wat ze zochten, konden ze misschien wel een beslissing nemen. Vervolgens bedankte ik Ernst voor zijn goede ideeën.

In 1987 ontmoette ik Aernout Schmidt. Hij was in de afrondende fase van zijn proefschrift onder de bezielende leiding van Professor Melai. Laatstgenoemde belde me op – stellig op instigatie van Aernout – en vroeg : "Zoudt u niet eens mee willen kijken bij een geheel nieuwe ontwikkeling binnen het recht?" Aernout was bezig met een interessant programma dat zou kunnen/ moeten/ mogen (de modaliteit was in die tijd nog niet in discussie) beslissen over voorwaardelijke invrijheidsstelling. Hij had het programma de mooie naam *Pallas ex Machina* meegegeven. Het zou ook de titel van zijn proefschrift worden.[3] Het was het begin van onze samenwerking. Het proefschrift was een doorbraak, waarbij het me opviel dat een aantal juristen tegen me zei: "dat had ik ook al eens bedacht". "Het kan zijn, maar Aernout heeft het opgeschreven, als eerste", was mijn steevaste antwoord. Jammer voor hem werd spoedig daarna *voorwaardelijke* invrijheidsstelling omgezet in *voorlopige* invrijheidsstelling met alle veranderingen van dien. Maar hoe dan ook, de juridisch wereld had geroken aan de mogelijkheden van een computer.[4]

Recht en Informatica

In 1985 had Aernout tijdens zijn promotieonderzoek een groep Recht en Informatica opgericht. Hij had hiervoor gehoor gevonden bij het faculteitsbestuur en spoedig daarna bij het LUF (Leids Universiteits Fonds). Ik voelde me vereerd dat ik gevraagd werd om deze groep te leiden als bijzonder hoogleraar Juridische Informatica. Hans Franken sloot zich vervolgens bij ons aan. Samen met Jaap Hage, Franke van der Klaauw en Corien Prins hadden we een prachtteam.

We onderzochten van alles binnen de rechtsinformatica en binnen het informaticarecht. Aernout was de verbindende schakel. Als een bedrijvig baasje verklaarde hij de informaticatermen aan juristen en de juridische noties aan informatici. Er werden jaarverslagen gepubliceerd, aio's aangetrokken, gespecialiseerde colleges gegeven en proefschriften geschreven. Voor mijn inaugurele rede[5] ondervond ik veel juridische steun van Aernout. Hij kwam naar Maastricht, legde me uit hoe het juridisch precies zat, bleef slapen en ging de volgende dag monter verder. Ik bedank hem hier nogmaals met de woorden die ik toen uitsprak: "Jouw onderzoek wekte ooit mijn belangstelling voor de rechtsinformatica. Samen zijn we toen in 1987

3 Schmidt 1987.
4 Schmidt 2007.
5 Van den Herik 1991.

met Juridische Kennissystemen aan de slag gegaan. Onze toepassing was rechtsgeleerd onderzoek. Beiden hadden we een grote mate van wetenschappelijke nieuwsgierigheid, waarbij onze rollen langzaam maar zeker verwisselden. Ten slotte wilde jij alles van informatica weten en was ik alleen maar benieuwd of de computerbeslissing juridisch verantwoord was. Door je inzet en je vermogen een bijna onbegrensde belasting blijvend te torsen, heb je je in onze afdeling de ideale *waarnemer* betoond, in alle betekenissen van het woord."

Probleemstelling

Intussen ging de wereld verder. Na 10 jaar (1998) nam Aernout het leiderschap van Recht en Informatica over. Enkele jaren later werd hij benoemd tot hoogleraar. De groei en bloei van de groep was zo duidelijk dat wij reorganisatie op reorganisatie glansrijk overleefden. Wij verdienden onze eigen projecten – Aernout was een crack in het binnenhalen – en zorgden voor voortdurende uitstraling.

Een van de projecten was het ANITA-project (Administrative Normative Information Transaction Agents). We vonden de heren Hugo Kielman en Wouter Koelewijn bereid om het juridische deelonderzoek samen met ons en Laurens Mommers uit te voeren. Een korte samenvatting van de ideeën die ten grondslag lagen aan de toekenning van het project is te zien in Figuur 1: Hoofdknelpunten van informatie-uitwisseling.

Onderzoeksdomeinen	**Hoofdknelpunten**
Juridisch	1. Moeilijk toegankelijke juridische kennis 2. Ontoereikende privacywaarborgen
Bestuurlijk	3. Ontoereikende gegevenscontrole 4. Gesloten bedrijfscultuur
Technologisch	5. Onvoldoende standaardisatie

Figuur 1: Hoofdknelpunten van de informatie-uitwisseling.

Het onderzoek had vele dimensies, zoals ook reeds uit Figuur 1 blijkt. Wij kiezen in deze bijdrage voor de volgende probleemstelling: *Hoe kunnen we ondanks ontoereikende gegevenscontrole toch goede beslissingen nemen?*

Privacy en politiegegevens

De discussie tussen Aernout en Hans aan de ene kant en Jaap aan de andere kant ging niet zelden over computerrechtspraak (*Kunnen Computers* Recht*spreken*?). We konden ons alle drie vinden in het volgende compromis: *Computerrechtspraak bevindt zich (nog) in de ondersteunende fase.* Jaap las die zin zonder haakjes. Aernout en Hans vonden dat wat tussen haakjes stond er niet bij hoorde en dat de zin verder altijd zijn geldigheid zou bewaren.

De ontwikkeling van de computerrechtspraak komt bijvoorbeeld heel duidelijk tot uitdrukking in de voorbereidende fase van een strafprocedure. Daarmee bedoelen we de fase die voorafgaat aan een zitting van de rechtbank. Het traject is: Politie → OM → Rechtbank. Voor onze probleemstelling ontwikkelen we twee onderzoeksvragen, te weten:

OV 1: Op welke wijze heeft de wetgever de uitwisseling van criminele inlichtingen genormeerd?

OV 2: Op welke wijze is de huidige uitwisseling van criminele inlichtingen ingericht en wat zijn daarin de (juridische) knelpunten?

Wat bij deze onderzoeksvragen in het oog springt is de spanning tussen rechtsbescherming en rechtshandhaving. Voor de politie is een groot probleem gelegen in het gebruik van computermogelijkheden. Vroeger (in de tijd van Ernst Enschedé) was er sprake van registratie van gegevens (cf. Wpolr). Tegenwoordig (2010) zijn computers in staat om gegevens te verwerken (Wpolg, ingegaan 1 januari 2008). Je zou bijna zeggen dat het probleem van de rechtsbescherming versus rechtshandhaving zich dus binnen de computer afspeelt. Als we die gedachte even doortrekken is het dan met behulp van allerlei slimme AI-technieken (Artificial Intelligence) misschien ook mogelijk dat computerprogramma's zichzelf normatief gedrag opleggen. Dit is precies het onderzoek van Wouter Koelewijn,[6] waarbij Aernout een van de promotores was.

Van Classificatie naar *Ranking*

Het gebruik van computers is mooi, het gebruik van supercomputers is nog mooier[7] en het gebruik van Grid-technologie is vooralsnog het meest geavanceerde. Het concept van de toekomst luidt *Cloud Computing*. Zover zijn we nog niet maar het is goed als de onderzoekers in recht en informatica weten wat de komende ontwikkelingen zijn.

Laat ik het zo eenvoudig mogelijk voorstellen. Als een juridische onderzoeker meer geheugenruimte ter beschikking heeft dan nu en ook de te gebruiken computer een grotere snelheid kan ontwikkelen om herhaaldelijk allerlei beslissingen te nemen die relevant zijn voor het classificeren van een casus (b.v. gevaarlijk versus niet gevaarlijk), dan is het beter om af te zien van classificatie en over te gaan op *ranking*. Het volgende voorbeeld is ontleend aan het ToKeN-project IPOL (Intelligence-led Policing) dat uitgevoerd is door Theo de Roos (toen nog UL), Jaap van den Herik, Thijs Vis en Stijn Vanderlooy (2009). Stel dat we een verzameling van 7 voorvallen hebben, die geclassificeerd moeten worden in *gevaarlijk* en *niet-gevaarlijk*.

6 Koelewijn 2009.

7 Zie Aerts en Michielse 2009.

We hebben twee classifiers: f1 en f2. Voor beide classifiers zijn de resultaten hetzelfde en wel:

	x1	x2	x3	x4	x5	x6	x7
f1, f2:	+	+	+	+	–	–	–

Laten we aannemen dat f1 en f2 het volledig eens zijn over x1 en x2 alsmede over x6 en x7. Laten we vervolgens aan f1 en f2 de voorvallen x3, x4 en x5 voorleggen om te evalueren (d.w.z. een waarde toekennen tussen 0 en 1). Neem aan dat de uitkomst van deze procedure het volgende beeld vertoont:

	x1	x2	x3	x4	x5	x6	x7
f1:	1.0 +	1.0 +	0.52 +	0.4 +	0.5 –	0.0 –	0.0 –
f2:	1.0 +	1.0 +	0.82 +	0.4 +	0.5 –	0.0 –	0.0 –

Twee zaken vallen hierbij op. Allereerst classificeren f1 en f2 het voorval x4 als *gevaarlijk*, maar zij kennen aan deze classificatie de waarde van 0.4 toe, terwijl zij voorval x5 met een waarde van 0.5 als *niet gevaarlijk* classificeren. Kortom, beide beoordelaars zijn het eens over de classificaties van x4 en x5 en zelfs over de bijbehorende waarden. Toch zou een waarnemer van buiten (wie beoordeelt de beoordelaar?) opmerken dat f1 en f2 eigenlijk zouden moeten zeggen dat x5 *gevaarlijk* is en x4 *niet gevaarlijk*, of misschien wel dat x4 en x5 beide *niet gevaarlijk* zijn (of beide wel *gevaarlijk*).

De tweede opmerking ligt iets subtieler. Classifier f1 beoordeelt voorval x3 als *gevaarlijk* met een waarde van 0.52, classifier f2 is het met hem eens maar beoordeelt dit veel hoger, nl. met 0.82. Voor f1 zit dit voorval bijna in het bereik van *niet gevaarlijk* (namelijk vergelijkbaar met x5 die zowel f1 als f2 als *niet gevaarlijk* beschouwen). Let op, dit is een lineaire vergelijking voor één variabele, maar het gaat om het idee: *ranking* leidt tot betere beslissingen dan classificeren.

Drie casus

Om onze bewering over *ranking* en het gebruik van computers te substantieren geven we hieronder drie casus.

Casus 1: terroristische dreiging (Amsterdam, 12 maart 2009)
In 2009 werd de gemeente Amsterdam opgeschrikt door een telefonische aankondiging van een terroristische aanslag op IKEA op 12 maart. Van diverse kanten werd er door de driehoek (burgemeester, officier van justitie, korpschef) om informatie gevraagd. De controle van de gegevens diende op korte termijn te gebeuren. De classificatie van de driehoek was*: ernstig*, *zeer ernstig*.

Deze classificatie werd gevolgd door stringente maatregelen: het oppakken van mensen (als er dan een tand verloren gaat is er wel 'iets' gebeurd). We weten intussen hoe het afgelopen is. (Er was geen sprake van een echte dreiging. Het gaat hier niet om de details.) De overblijvende vraag is wel: is er iets misgegaan bij de gegevenscontrole? Daar zijn argumenten voor en argumenten tegen aan te voeren. Maar als we hier een *ranking*-procedure hadden uitgevoerd in plaats van een classificatieprocedure dan was het oordeel ongetwijfeld geweest: *niet gevaarlijk*, *niet ernstig*.

Casus 2: bedreiging van scholen in Breda (Rijsbergen, 12 maart 2009)
Op internet verschenen berichten dat er iemand op een school in Breda de volgende dag gedood zou kunnen worden. De classificatie van het OM is *zeer ernstig*. Er worden stevige maatregelen genomen: de minister bemoeit zich met de zaak, de FBI wordt ingeschakeld, het IP-nummer wordt nagegaan, de omgeving van het IP-nummer wordt nagegaan (voor het geval de problematiek was gelegen in onbeschermde internettoegang in een huiskamer, waardoor van buiten ingelogd kon worden op het IP-adres van de buurman. Let wel: (a) de gegevenscontrole was meer dan toereikend uitgevoerd met als resultaat dat de eigenaar van het IP-nummer redelijkerwijs niet verdacht kon worden van het plaatsen van zulke berichten op internet en (b) er vond een *ranking* van de acht verdachte huizen plaats – hulde aan Henk van Brummen die deze zaak leidde).

Vervolgens vindt er een inval plaats in het eerste verdachte huis; dat levert niets op. De bewoners krijgen excuses aangeboden. Daarna is er een inval in het als tweede *gerankte* huis. Hier blijkt de zaak volledig duidelijk, inloggen bij de buren, een bericht met verschrikkelijke strekking posten en dan kijken wat er gebeurt. De doortastende oplossing van het OM is een compliment waard. Met deze actie werd ook eigenlijk de actie van Cohen in Amsterdam (mensen oppakken) gelegitimeerd. Het is evenwel niemand duidelijk waarom hij geen excuses aanbood voor een verkeerde actie. In deze tijd van razendsnelle technologische ontwikkelingen moeten we over durven gaan op *ranking* van gebeurtenissen (i.p.v. classificatie) en dan op grond daarvan actie ondernemen. Als we het daarover eens zijn dan kunnen we het er ook over eens zijn dat als de actie verkeerd is excuses op hun plaats zijn.

Casus 3: Hillsborough
Op 15 april 1989 vond tijdens de FA Cup Semi-Final Liverpool-Nottingham Forest een grote ramp plaats. Veel te veel mensen waren toegelaten in één toeschouwersvak. Er ontstond gedrang en velen vonden de dood. Na 20 jaar werd deze ramp herdacht. Er zijn veel foto's en verhalen gepubliceerd en waar het allemaal om draait is het volgende: "What they [parents of victims] want is simply recognition that mistakes were made by people entrusted with the safety of the public. They want to hear, on official lips, the phrase 'we are sorry'." Deze casus is toegevoegd als een bijzondere interpretatie van de titel: 'van registratie naar verwerking'. Voortschrijden van de techniek zou ook moeten leiden tot voortschrijden van het onderkennen van elkaars gevoelens.

Moderne ontwikkelingen

Natuurlijk wordt met *ranking* niet alles opgelost. Overigens, wat we hierboven beschreven hebben betreft een overgang van binaire classificatie naar *bipartite ranking*. Dat geldt voor één variabele en zoals we gezien hebben met het voorbeeld van de classifiers f1 en f2 zijn er ook dan nog veel open vragen. Er moeten technieken komen om niet alleen te genereren wat we doen maar ook te visualiseren. Een aantal van deze technieken is reeds ontwikkeld, zoals de ROC-ruimte, de ROC-curve en de AUC.[8] Verder zal het theoretisch raamwerk van de multi-classificatie gegeneraliseerd moeten worden en dan geschikt gemaakt moeten worden voor de overgang naar een *multipartite ranking*. We blijven dan natuurlijk het probleem tegenkomen van f1: x3=0.52 en f2: x3=0.80. Derhalve is het goed om naar nieuwe technieken te kijken die ons hierbij kunnen helpen, zoals *adaptive voting* (aangepast stemmen) of *abstention* (het onthouden van een waardeoordeel).

Conclusies

De conclusies die bij dit betoog van ICT-ontwikkelingen binnen het recht behoren zijn geïnspireerd door het beginwerk van Aernout Schmidt. Zij luiden als volgt:

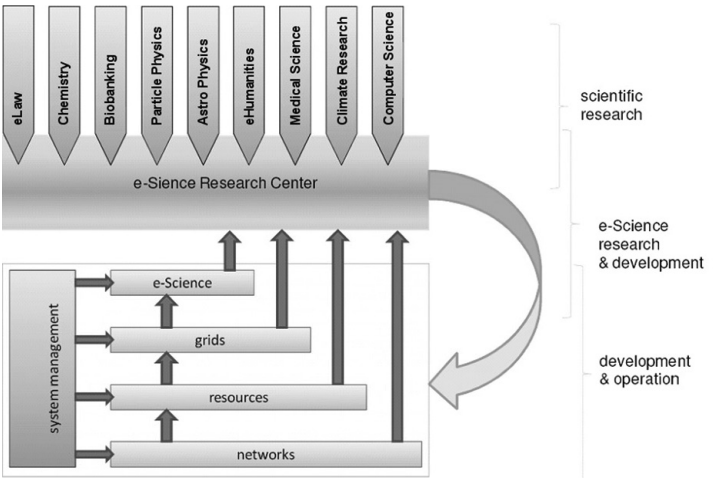
(1) Informatica-toepassingen zijn ongelooflijk veelzijdig in de rechtspraak.

(2) Dankzij de nieuwste ontwikkelingen op het gebied van automatische computermodellen zijn we nu op weg naar het nemen van juridisch correcte beslissingen.

De toekomst van eLaw

Toen Aernout Schmidt in 1998 de leiding van Recht en Informatica overnam, begreep hij dat er een nieuwe periode was aangebroken. Zoals omstreeks 1950 computers een nieuw fenomeen waren, zo was internet omstreeks 2000 een nieuw fenomeen in het recht. Recht en Informatica diende (1) internationaal te zijn, (2) geavanceerdheid uit te drukken en (3) kort, krachtig en kernachtig te zijn. Daarom werd het eLaw en voor onze groep in het bijzonder eLaw@Leiden. Hoe eLaw past in eScience is helder aangegeven in Figuur 2. Daarmee is tevens de toekomst van eLaw vastgelegd: mee in de vaart der wetenschappen, tezamen met de grote ontwikkelingen.

8 Zie Vanderlooy 2009.



Figuur 2: eLaw gezien als onderdeel van eScience Research.

Dankwoord

Het ANITA-onderzoek is in 2002 van start gegaan. Er wordt interdisciplinair onderzoek gedaan naar de mogelijkheden van multi-agentsystemen. Het ANITA-project (administrative normative information transaction agents) vindt plaats in het kader van het NWO ToKeN-project en is een samenwerkingsverband tussen de UL, de UU (J.J. Meijer) en de RUG (De Vey Mestdagh, projectleider) Het IPOL-onderzoek is gestart in 2005. Het is eveneens een NWO ToKeN-project en kent een samenwerkingsrelatie tussen de UL, UM, en UvT (zie tekst). De volgende mens wordt ten zeerste bedankt voor de jarenlange samenwerking: Aernout Schmidt. De andere mensen: Hans Franken, Joke Hellemons, Hugo Kielman, Franke van der Klaauw, Wouter Koelewijn, John-Jules Meyer, Laurens Mommers, Eric Postma,Theo de Roos, Stijn Vanderlooy, Kees de Vey Mestdagh en Thijs Vis bedank ik voor hun samenwerking met Aernout en mij. Ik weet zeker dat Aernout terugkijkt op vele prettige contacten.

Verwijzingen

Aerts & Michielse 2009
P. Aerts en P. Michielse P. (eds.), *De Rekenmeesters*, Nationale Computerfaciliteiten (NCF) en SARA Reken- en Netwerkdiensten, Amsterdam, 2009.

Enschedé 1966
Ch. Enschedé, 'Bewijzen in het strafrecht', *RM Themis* 1966, p. 516.

Van den Herik 1983
H.J. van den Herik, *Computerschaak, Schaakwereld en Kunstmatige Intelligentie* (diss. TUD), Delft, Academic Service Den Haag 1983.

Van den Herik 1991
H.J. van den Herik, *Kunnen Computers* Rechts*preken* (oratie UL), Gouda Quint bv Arnhem 1991.

Kielman 2010
H.H. Kielman, *Politiële Gegevensverwerking en Privacy. Naar effectieve waarborging* (diss. UL), Leiden 2010.

Koelewijn 2009
W.I. Koelewijn, *Privacy en politiegegevens, Over geautomatiseerde normatieve informatie-uitwisseling* (diss. UL), Leiden University Press, 2009.

Schmidt 1987
A.H.J. Schmidt, *Pallas ex Machina, Informele systemen in verband met het recht* (diss UL), Koninklijke Vermande BV Lelystad 1987.

Schmidt 2007
A.H.J. Schmidt, Ought Computers Adjudicate?, in: J.Donkers e.a., *Liber Amicorum ter gelegenheid van de 60e verjaardag van Prof. dr. Jaap van den Herik*, Maastricht 2007, pp. 132-147.

Vanderlooy 2009
S. Vanderlooy, Ranking and reliable classification (diss. UM), Maastricht, 2009.

Limits and Dimensions

Gerben Wierda■

Abstract

The digital revolution is in the end based on a massive application of classical logic. Classical logic, however is dimensionless, there is no time, no space, no becoming, no uncertainty. No amount of dimensionless facts can create the dimensions of the real world, and this is a barrier that returns in many guises, be it the impossibility to have AI on digital computers or the problems modelling the human values underlying law systems into digital systems. On the other hand, existing law systems face a seemingly unsurmountable mass of dimensionless facts (digital data), can they cope, and how? Is A.H.J. Schmidt's suggestion to model law quality on a more scientific footing, comparable to the way economics is grounded in mathematics these days, feasible?

Logic

We use the word 'not' for more than one thing. "It is not true that Pete is in the room" uses the word not, but so does "it is not true that 2+2=5". Though the word is the same and the meaning is clearly related, there are differences. A difference between the first 'not' and the second 'not' is that the second is intended as never, while the other does not exclude that at some point in time the statement will be true. The truth-value of '2+2=5' cannot change over time, while the truth-value of 'Pete is not in the room' may.

The same sort of aspect holds for the opposite: logical truisms or tautologies. Logical truisms of the type '2+2=4' are always true. There is no way they can be 'not true' at any point in time. The cannot become true or false. There is no time aspect in their meaning. Tautologies are always true, regardless of circumstances or context. When the truth of *b* follows always (by logical necessity) from the truth of *a*, and *a* is true then it must be the case that *b* is true also. This is for instance the case when doing algebra.

■ Gerben Wierda is IT Lead Architect, APG, http://www.apg.nl/, formerly IT Lead Architect for the Judiciary in The Netherlands. The opinions in this article do not reflect opinions of APG.

Mathematical proofs are statements by which one statement of mathematics is proven by transforming it into other statements that in the end can be seen as true directly. Let us take a very simple example. Let us take the following statement: $(a+b)(a-b)=a^2-b^2$. How do we know that the two sides are equivalent? Well, we can start transforming the left side using logical rules that do not affect the meaning of the left side until it is the same as the right side. So, we apply the rule of associativity: $x(y+z)=xy+xz$, and the rule of commutativity: $xy = yx$. These rules are transformation rules. Apply them and the meaning stays the same. 3 times 4 is the same as 4 times 3. 3 times 6 is the same as 3 times 4 plus 3 times 2. We could ask ourselves why we know that these rules are true, but that question is misleading. Following Wittgenstein: asking ourselves why we know this may syntactically look like a question, with a question mark and all, but it only is a question if there are multiple answers possible[1]. Because if we ask ourselves why we know something to be true or false, we are asking for the reason we choose between the truth and falsehood of something. But such a choice is not available in logic and mathematics. We might say: since it cannot be false, it is senseless to ask why we know it, as there is no reason, no explanation. "2+2=4" is an internal, logical, timeless, relation between 2, +, = and 4, not something testable. Testability requires the possibility of being true or false and of our knowledge of true- or falsehood 'becoming'. Mathematical statements are therefore fundamentally different from testable statements. As Wittgenstein argued: If you ask a question without the uncertainty, you are breaking the rule of what a question can be. Such a statement is 'senseless'. Trying to answer senseless questions, often sentences that get there question-status purely from their grammatical form (e.g. a question mark at the end in many languages or stating both opposites in a statement as in Chinese[2]), is a dead end, he argued.[3] [4]

1 Wittgenstein's important later work can be seen as addressing the question: "when is a statement a question?" to which the answer is "if it can be used in a setting where it is used as a question". This is why he starts showing us statements that look like questions but are orders, etc.. In the beginning of the *Philosophical Investigations* (Wittgenstein 1973) Wittgenstein looks at how statements are used and shows us that the meaning of a statement lies hidden in its use and not its form, or, that the meaning of a statement is its correct use, where correctness in all but purely logical situations depends on circumstances (context).

2 "You can not can speak Chinese".

3 With such a question we have entered a room which has no exits but the one we entered through. The only valid solution in such a situation is to leave the room. In Wittgenstein's view, philosophy should often be just that: a remedy against asking senseless questions instead of a by definition futile attempt to answer them at all cost.

4 Actually, if we allow statements becoming true or false, and thus allow for them a state where they are neither we end up in constructivist mathematics of the L.E.J. Brouwer kind. In his seminal paper (Brouwer 1908), which started intuitionist mathematics, he does just that.

Assuming the validity of those rules of transformation for now, we can transform the left hand side into the right hand side. This is far from interesting and it is very simple algebra. The issue here is to show that at no point, there is freedom to say the step is invalid. There is nowhere an aspect of choice or decision. This proof is valid whatever the values *a* and *b* have, whenever it is performed. It is always true, and that, in fact, is what we call a truism, a tautology. Never along the road of mathematical transformations should we be surprised, it must be so. Nowhere is there something new. This is why Wittgenstein finally decided that for him mathematicians must be inventors and not discoverers. They invent new rules of transformation among the infinite number of possibilities. But they do not discover something new. This is also why he argued that all valid mathematical proofs have to be tautologies as they have to be undoubtable transformations.

What holds for time in the previous paragraphs also holds for space. Classical logical statements and their relatives on the side of mathematics have a value that does not depend on space. '2+2=4' is true, irrespectively of where the statement is made.

Classical logic, therefore, can be characterized by its freedom from aspects like time and space. We might say: *classical logic is dimensionless*.

The reader may wonder what this lengthy exposé has to do with IT and the Law. The answer to that question is that, since classical logic is the mechanism by which modern computers and networks work[5], we could (and should) wonder if this aspect of classical logic being 'without' time and space has consequences for what the effects of the ongoing digital revolution are on our culture and our laws, which are 'within' time and space. Two questions lie before us:

1. Can the legal profession itself (partly) be executed by computer programs?

2. How must the legal profession cope with the explosion of subject matter from the dimensionless domain[6]?

The first question has received a lot of attention from the advent of digital computers in the 1950's. Examples from our own Dutch academic system are for instance Van de Herik[7] and Schmidt[8]. The second question is more recent and follows form the exponential growth of the use of computers and networking from the 1990's and onward. Here, Schmidt has recently been focusing his attention[9].

---

5 This is independent of the level of abstraction that tooling like computer languages may have added. The abstractions may be reduced to the basic operations of a digital computer which at its lowest level is known as a 'Turing Machine'.

6 E.g. the bits and bytes on the internet and connected computer systems.

7 Van den Herik 1991.

8 Schmidt 2007.

9 E.g. Schmidt, Dolfsma & Keuvelaar 2007.

Digitizing the legal profession

Law and IT superficially have something in common: they both try to model aspects of human behaviour with rules. But the likeness ends fairly quickly, because the rules of Law are part of the dimensional, real, world. The computer is pure embodied classical logic, the law only looks like (dimensionless) logic, but is built from many terms which do require interpretation (e.g. 'good', 'enough', 'reasonable', etc.).

As an example we may take the many Dutch court cases that have been the result of the way the forerunner of Dexia bank sold leveraged investment portfolios to its customers. When these portfolios tanked during the dot-com bust, customers — often to their surprise — found out they had huge debts. Most of the litigation centered around the question if the bank had fulfilled its legal obligations to its prospective clients when selling them these leveraged portfolios. These obligations were of various types, but generally they fall in two categories:

1. The form was faulty. This for instance happened when a legally required signature was missing, e.g. from a spouse.

2. The content was faulty. Had the bank warned its clients enough for the risks as it was legally bound to do?

The first are obligations of a type that can be formalized in a discrete question. Has the speed of the car exceeded 54 km/h? Is the signature available on the contract? The physical appearance of a signature on a contract can become a context-free dimensionless fact of the type that a computer program needs to be able to function[10]. It is however wrong to say that the program itself 'decides' anything, as a decision requires choice and choice is not available in the dimensionless domain of the digital computer. What happens is that the actual decision is made when the program is *designed*, e.g. the decision to always make ruling X when dimensionless fact Y is the case[11]. In individual legal cases, rulings are coupled to decisions, and the two terms are often used as synonyms. I would suggest that the influence of the digital world separates them in many cases as the one above. We should therefore talk about 'the decision on how to rule'. Hence, the word decision (just as the word not) has multiple, different roles to play[12]. When we do separate 'decision' and 'ruling' in the legal world, we can be clearer about what happens.

10 In this case a logical true or a logical false.

11 It is decided to use the rule $\forall X \Rightarrow Y$.

12 Assuming that both uses of the word decision are the same is exactly the sort of trap Wittgenstein tried to warn us for. Language sometimes bewitches us, indeed. The world changes and language needs to play catch-up.

When facts can be made context-free[13] (e.g. breaking the speed limit, a missing signature), we can decide to rule always in the same way on the basis of that fact. If we decide that, we can fully automate the ruling on the basis of the facts[14].

The second type of obligations of the bank in the foregoing example are however far less tractable. Schmidt[15] calls this the incommensurability trap. Here in the end a judge decides by weighing all facts and circumstances if it was indeed 'enough'. According to Schmidt, this incommensurability trap holds for human judges as well (and thus is not a valid argument against computer adjudication). And indeed, it is not possible to make a dimensionless, context-free, account of many human decisions, be it chess moves by chess masters or decisions by judges[16]. It is however not clear that the fact that incommensurability holds for human judges means they are in the same situation as digital computer programs. After all, it is not necessary to assume that the decisions themselves have to be rule-like for a law system to work. In fact, ample corroboration is available for the opposite: it seems we can have decent working law systems, like the one in The Netherlands, without having full commensurability of adjudications. The fact that different judges may make different decisions in — what appears to be — the same case, the fact that judges make errors, may well be the Wittgensteinian 'rough ground' that is needed for a human law system to function at all.

Decision making itself has proven to be untractable for discrete systems, which is unsurprising taken the fundamental choicelessness of the discrete world. Optimism that enough dimensionless facts put together may create dimensions, somehow, has not been supported by results of the AI-communities in the last 60 years[17]. Mathematically, even an infinite amount of dimensionless facts will not be enough to create real world dimensions[18] and assumptions about a certain massive amount providing enough 'precision' to mimick the dimensional world have not been supported by evidence. Hence, as long as computers are digital, it is highly unlikely from a mathematical

13 The context-free fact is created when a reliable (dimensional) 'truthmaker' situation in the world (speed measurement, signature detection) can be used to remove the real world dimensions from the question at hand. The truthmakers from analytic philosophy therefore need to have the same dimensionality as the question they are meant to strip from its dimensions. E.g. a truthmaker 'an hour ago' can not be used to remove the dimensions from a question about location, e.g. 'is the signature on the contract?', because the dimensions do not match.

14 *Decide* once, *rule* many times.

15 Schmidt 2007.

16 Or design decisions by IT architects, for that matter.

17 See for instance Dreyfus 1991.

18 The insistence of the main body of the AI crowd is reminiscent of the supposed insistence of the Pythagoreans that the world should be commensurable (rational). The world, however, seems not to be rational but real, both in the mathematical as in the every day meaning of the terms.

point of view that any real AI-like system will be built.[19] However in cases where the result of a decision is again enumerable[20], computer systems may be used to build a lot of the wording of the ruling from standard building blocks, thus freeing the judge from a lot of the tedious work following the decision itself. Here, we can partly automate the ruling on the basis of facts in combination with an interaction with the adjudicator for the decision[21]. This use of computer support has its risks too. Automated rulings do for instance carry the risk of adjudicators 'going autopilot' too much and — in effect — let the decision to be made depend on the ease of use of an automated ruling already available. However, given the fact that parties will always scrutinize each ruling to see if appeal is possible, such behaviour is self-limiting. Trust in the Judiciary is also at risk, as it depends on the rulings being recognized as being personal. Hartendorp writes: "people go to court to be heard and the ruling should relate to their situation"[22].

Both types of digital computer support:

- fully automated rulings based on preprogrammed decisions based on dimensionless facts, and
- partly automated wording of rulings from an enumerable set based on interaction with an adjudicator for the decisions are being developed all over the world. Neither of these include the decision-parts of adjudication and neither are signs that digital adjudication is on its way.

Summarizing:

1. Classical logic is dimensionless;
2. In a dimensionless settings, decisions do not exist, only transformations;
3. Digital systems work on the basis of classical logic and are therefore also dimensionless and independent of their complexity incapable of choice and thus of decision;
4. When we think of decisions taken by computers, we should instead be aware of the decision taken by the programmer of the computer, given that the computer has no choice;

19 When new technologies like quantum computing become succesful, a whole new chapter needs to be added, because those potential developments have quite different advantages and drawbacks than the discrete dimensionless systems of the current digital revolution.

20 E.g. only a certain number of law articles come into play and are referenced in the ruling.

21 Such a system has in fact been built by the court of Amsterdam for the aforementioned Dexia cases.

22 Hartendorp 2009, p.49.

5. In computer support for the law, we should separate clearly our use of the word 'decision' and the word 'ruling'; the IT support of both are quite different subjects.

A new world emerges

Computers have become immensely powerful logic machines. But just as artists have not been replaced by computers with the advent of computer graphics[23], judges are far from being replaced by computers[24]. Still, just as the world of graphics has been changed, the legal world is being changed by:

- Using the power of computers for (semi-)automatic rulings[25];
- An enormous increase in digital data, traffic which affects real life and with that affects the demands being put on the legal systems.

The overwhelming amount of dimensionless data and dimensionless processing — i.e. the digital revolution — is creating its effects on the world. Without digitized music being the norm since the introduction of the CD, and without the abundancy of cheap and powerful computers and networks, copyright infringement would not be a problem of the size it is today. Without massive use of a rather unsafe environment, identity theft and fraud would be less of a problem[26]. And the digital tracks people leave all over the place are both a boon for criminals but also a danger for the precarious balance between individual freedom and state power.

So, how must the legal system cope with this massive influx of problems, or more precisely with the problems that come with the massive rise in discrete dataprocessing?

Schmidt[27] follows 'futurologist' Kurzweil in expanding the notion of exponential growth to the idea that a 'singularity point'[28] is near. Schmidt does not follow Kurzweil in that we are close to being overwhelmed by changes in our society and that we will have to transform in some new eter-

---

23 A conviction held by many in the field during the 80's and 90's of the previous century. As it turned out, companies like Pixar were succesful because their artists were given powerful new tools which not replaced the artist, but enabled them to 'paint' good stories differently, comparable to the development of lens technology halfway the previous century. The reaction of the existing profession to the new tools are comparable to the reaction of many in the legal field.

24 Nor should they be if Hartendorp 2009 is correct to state that the judiciary is about 'acceptable rulings', more than just legal rules and facts, and that 'acceptable rulings' also means for parties to know they had a fair hearing in their case.

25 This is the above mentioned equivalent of new tools for the artists in our computer graphics example.

26 And we have not seen the full impact yet, in my opinion.

27 Schmidt 2009a.

28 The actual idea has been coined by SF-writer and mathematician Vernor Vinge.

nal nanotech based species, but he worries that innovation will result in a society where one individual will have the means to destroy the entire civilization. Protecting society against such an event will require the perfect e-justice system. Schmidt[29] concludes that legal systems will have enormous difficulty to cope, for one, because our society will need many new rules and it lacks the science to find out which legal rules are 'good' rules. He suggests a more scientific approach is needed, an approach leading to an empirical investigation to the quality of law systems:

> "In the approach chosen I do not look for knowledge akin to 'laws of nature' of the $e = mc^2$ type, rather for knowledge like the models of price-forming mechanisms and of market-failure effects of economists and models of survival of the fittest mechanisms of biologists."[30]

To my — admittedly limited — knowledge of discussions about law system quality, Schmidt might have been the first to suggest this approach for the legal field. It is an interesting idea, that has a merit of its own, and that does not depend on pseudo-scientific arguments, like those from the aforementioned Kurzweil. It does not even need the extra pressure on the law systems of the world that Schmidt expects.

Before we move to Schmidt's interesting suggestion of basing law system quality on a scientific model and scientific procedure (i.e. empirical tests of the model of what constitutes 'good laws'), let us shortly address if Schmidt is right to worry about new developments 'overwhelming' the law systems of the world. The question is, can we cope?

Yes, we can!

Initially, the prospect for humans seems bleak. After all, humans are rather bad at logic and the amount 'physically' thrown at us by means of the digital revolution is staggering. As Andy Clark writes: "Humans are better at frisbee than at logic" [31]. Though we are the best in the animal kingdom when it comes to logic, we are still rather bad at it. Our minds never developed to handle massive amounts of dimensionless data. When confronted with larger amounts of logic, only a few of us can cope. Take for instance chess. Compared to the amount of dimensionless data and processing now confronting our societies, chess is extremely simple. There are only 6 types of pieces, each with a limited set of allowed movements. The field is only 64 squares. The basic of chess are far from complicated, though it explodes into many discrete possible positions. Still, many of us can learn to play a decent game of chess. As Dreyfus reports, based on research by De Groot, decent players

29 Schmidt 2009b, p 3.
30 Schmidt 2009b, p 4.
31 Clark 1992.

hardly seem to use strict logical skills when playing chess. Most of their skill has the form of some sort of non-discrete pattern recognition enabling them to limit the number of discrete steps investigated to a minimum. 'Calculating chess' to a depth that beats humans 'estimating chess' does not mean that computers have in any way become more intelligent or better at estimation.

But looking at the amount of digital events in the world may be a misleading way to look at it. It is only when these dimensionless digital events encounter the real human world that there is an issue for human law systems at all. Human law systems are in the end about humans, not about anything else. The knife is not an interesting artefact for law until it is used to kill a human. The hedge is not important until it becomes part of a civil law dispute between neighbours who have ceased to be friends. Uncountable bits fly around these days, infringing on rights that our societies have granted to owners of intellectual works. The amount of data may be staggering and a reason for us to notice, but it is their effect on humans or human organisations (artists, companies) that makes the bits of data interesting and suddenly the huge problem is just a massive cumulation of many times the same problem. Is the amount of data (the stuff that grows exponentially so far) a good measure of the number of types of problems to expect? It seems not, as it is the number of types of problems that confronts law makers.[32]

Luckily, therefore, though the actual amount of legal facts grows with computer and network use, the number of types of facts grow less rapidly. Besides, since (paraphrasing Protagoras) 'man is the measure of human law systems',[33] the amount of possible effects on law systems are limited as well. And thirdly, while we get accustomed to the new technology, some rules will only be needed temporarily, such as the UK Locomotives Act 1865 ('Red Flag Act') that required a crew of three with one holding a red flag walking in front of the car.[34]

The exponential rise in digital data and processing may present us with a challenge, but there is no reason to worry that we will not in one way or another be able to cope. However, Schmidt is right to worry about the effects of these new rules on society, in that important current values like privacy and personal security are under threat by the growth of IT. The jury is still out on the question if these dangers to privacy and security are inherent in IT or if we can learn to mitigate them effectively at the human level.

---

32 For an example of a typology, see for instance Schmidt & Wierda 2000.

33 With some notable exceptions, e.g. animal welfare, though some of the animal welfare discussions do look like extending some of the rights of man to other animals and we are then still talking about the rights of man.

34 The red flag part was revoked in 1878 and from 1896 on cars under 3 tons were exempt from the 3-crew rule.

'Legistics'

For the new field of model-based empirical research into the quality of human law systems, I would like to suggest the name 'legistics'. Legistics is to law systems what economics is to economical systems[35]. According to Schmidt, legistics should ideally be populated with formulas with commensurable values as economics is today.

Given that a situation as in economics is Schmidt's goal, we can first look at the state of affairs for economics to see what we are aiming at. We see then that in almost a century a large body of models and formulas has grown, often based on complicated mathematical models. For instance, the 'Nobel Prize'[36] winning original[37] Black-Scholes model for an equity and the Black-Scholes partial differential equation for the price of a derivative of an equity and the Black-Scholes formula for option pricing that results from solving that equation.

As economic tides (and certainly the current credit crisis) show, even such elaborated models may fail spectacularly. That is because these models are often based on several simplifying assumptions to make them usable or mathematically solvable. In case of the Black Scholes model, for instance, some assumptions are:

- There are no transaction costs;
- The stock does not pay dividend;
- There are no restrictions on short selling;
- It is possible to buy/sell any fraction of a share;
- Stock price follows a Brownian Motion[38] with constant drift and volatility;
- The risk free interest rate is known and stable.

35 And physics to the natural world. Schmidt is mistaken to think he is not looking for laws like e = mc2, because the epistemological status of that law is not so much different than the status of the economic laws he has in mind. Even $e = mc^2$ may turn out to be not exactly right in the future.

36 There exists no Nobel Prize for Economics, but there is the *The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel*, which by most is considered the 'Nobel' prize for Economy.

37 The model has been extended since in various ways.

38 The randomness of dust specks that move in the air. According to Wikipedia on 15/08/2009, it was interestingly enough already used in an economic setting in 1900 by Louis Bachelier in his Ph.D. thesis, *The Theory of Speculation*. One is reminded of the use of the Law of Pythagoras being part of the curriculum of schools for scribes in ancient Babylonia, almost two millennia before Pythagoras.

These limitations make the Black-Scholes model a useful approximation, but following it entails various risks, not all of which may be hedged or even hedgeable.

Current mainstream economic models are also generally based on assumptions like 'rational individual' behaviour with full information disclosure. Not so much the information availability is the main problem, but, as more and more research has shown, we are only partly rational and we are far from individual.

So, why does the entire investment world use a model like the Black-Scholes formula for derivatives valuation? There are various reasons: it is easy to calculate, it can be used as a basis to do what-if analyses on, e.g. with Monte Carlo type calculations differing inputs to see what happens, etc.. In fact, the model is not used as a physics model would[39], but it is used as an indicator. In the end, the models of economics are mainly useful for professionals as input for their human-like intelligence.

In the real world, these humans may not all understand what they are dealing with (we are not all Nobel Prize winners), and they may start to trust models like the Black-Scholes and other models blindly. And, even if they do understand the uncertainties, they may err.

Financial constructs like Collateralized Loan Obligations and Mortgage Backed Securities which lie at the basis of the current credit crisis and the models on which they were built were beyond most of the sellers and buyers, and the products were still massively created, bought and sold. Add to this an amount of automation which made certain that everybody was using roughly the same formulas and systems and we have a system setup that neither is understood and which is instable *because* everybody uses the same rules, making sure that when it goes wrong, it goes massively wrong[40]. That is a scenario which may not be acceptable in the field of law.

Prospects for a field of 'Legistics'

Schmidt proposes the following initial model:

- Law system quality is divided in 6 different 'natural' qualities: 'freedom', 'fairness', 'welfare', 'security', 'legitimacy' and 'autonomy'[41]. These values are not commensurable, they cannot be directly measured.

---

39 In that sense, Schmidt is right to make a difference between $e = mc^2$ and economic models like Black-Scholes, but from his goal to be more 'scientific' about law system quality, I think that is not what he had in mind.

40 Massive automation does (by its nature of being exactly the same instead of roughly the same) have this rather distressing effect. The Wittgensteinian 'rough ground' that results from human adjudication may function as a guard against this effect.

41 Schmidt 2009b, p 8.

- Behaviour of stakeholders in a law system is measured via actual behaviour by stakeholders of a law system. They are expressed in a percentage. For those on the inside the behaviours are: use (*u*), comply with (*c*), evade (*e*), leave (*l*) and revolt against (*r*) the system and for those on the outside: join (*j*), team up with (*t*) and fight (*f*) the system.[42] Schmidt proposes a function *W(u, c, e, l, r, j, t, f)* that expresses willingness to participate with regard to a law system for the stakeholders as a function of observed behaviours.

- Schmidt proposes a function *R* (for Radbruch) of *W* that produces *Q*, which is the overall quality of the law system: *Q = R(W)*.

To get to *Q* via the averaged numbers for the natural values like 'fairness' etc. of the examples (and thus to a *Q* he wants to link *W* to, via the to be determined function *R*), Schmidt has to resolve to an (in this case his own) estimate for *Q* based on averaging estimates for the 'natural' values. Schmidt starts with some answers (a value for *Q*) to see what the function *R* on the variables of *W* should look like. This, by the way, is a dangerous procedure[43].

In the future, one could imagine a line of inquiry where the natural values are estimations by legal professionals. As such, the Radbruch function *R*, would be a test of professional assessment of quality by measuring actual stakeholder behaviour. Since the stakeholder behaviour is a physical manifestation of stakeholder opinion, *R* is therefore a relation between opinions of two separate groups[44].

In terms of using *R* to create an independent measurement of the natural values of law systems, however, it is hard to see how any such model could be constructed without being effectively (and mathematically) equivalent to the impossible dream of rational AI or a rational foundation of what good law is, instead of the measured opinion of professionals on those natural values.

If *W* is instead only used to bring a certain model-like subjective order to measurements of (public) opinion, we seem to have changed nothing fundamentally to the practices of current democracies except for a more detailed 'vote' for the population. Such fragmentation has its own problems, like

42 Schmidt 2009b, p 11.

43 I am reminded of a draft environmental study that I reviewed once for a friend and that concluded that the effects of noise on work performance was a 5th order function, which fitted the numbers perfectly. But the situation was that the range had been split into 5 intervals (and thus there were 5 data points) for which a 4th [sic] order function would have been enough. Had the researchers used 10 intervals, they would have found a perfect 9th-order (or in their misguided case: a 10th-order) function for the influence of noise on productivity.

44 And as such possibly useful for professional groups like the Judiciary to measure stakeholder behaviour (e.g. how many stakeholders do not bother to go to court when they have an issue for which the courts are meant?) to get to a measure for perceived quality of their system, instead of the current default method of surveys.

allowing people to vote for more education and against taxes to fund them. But, since the *W*-function is coupled with physical manifestations of stakeholders, it does bring something essentially new and valuable to the table (with respect to opinion polls and the like), namely the effective[45] inclusion of the effects of all the vague and contradictory values of stakeholders.

Closing remarks

- Models of Physics and Economics, like $e = mc^2$ or the Black-Scholes formula (or any other model in a scientific approach), are meant to be testable through their predictive value. For new law systems, there is no such thing in Schmidt's approach. A truly scientific model would therefore require (unavailable) rational foundations for the natural values.
- One important difference between the economy and the legal profession must be mentioned. In the economy, it is in the end about economic value, which can be expressed in hard numbers (money, volatility). Though Schmidt gives such numerical values for natural values like 'freedom', 'fairness', 'welfare', 'security', 'legitimacy' and 'autonomy'[46], it is unclear what such numbers mean with respect to real world human values.
- Schmidt concludes from his examples that a combination of high *r* and high *f* are indicative of low *Q*. But working with percentages for the behavioural variables (*u,c,e,l,r,j,t,f*) automatically undervalues the importance of minorities. E.g. if there is low *r* or low *f* as in the case of the Chinese occupation of Tibet, it does for me not follow that this occupation has a high *Q*.

References

Brouwer 1908
L.E.J. Brouwer, 'De onbetrouwbaarheid der loogische principes', *Tijdschrift voor Wijsbegeerte*, 2: 152-158, Groningen: Noordhoff, 1908

Clark 1996
A. Clark, *Being there : putting brain, body, and world together again*, Cambridge: MIT Press, 1996

Dreyfus 1992
H.L. Dreyfus, *What Computers (Still) Can't Do*, Cambridge: MIT Press, 1992

Hartendorp 2009
R. Hartendorp, 'Alledaagse rechtspraak, een pragmatische kijk op oordeelsvorming', *Rechtstreeks*, 2:11-51, Den Haag: Raad voor de rechtspraak, 2009.

45 And non-commensurable.
46 Schmidt 2009b, p. 12.

Schmidt & Wierda 2000
A.H.J. Schmidt and G.C.Th. Wierda, 'Communicatierechten in de grondwet', *Rechtsgeleerd Magazijn Themis*, (9), pp. 323-224, 2000.

Schmidt, Dolfsma & Keuvelaar 2007
A. Schmidt, W. Dolfsma and W. Keuvelaar, *Fighting the War on File Sharing*, Cambridge University Press, 2007.

Schmidt 2007
A.H.J. Schmidt, 'Ought computers adjudicate?', in: J. Donkers, L. Mommers, E.O. Postma & A.H.J. Schmidt (eds.) (2007), *Liber amicorum ter gelegenheid van de 60e verjaardag van Prof. dr. H. Jaap van den Herik*, Maastricht: MICC, 2007.

Schmidt 2009a
A.H.J. Schmidt, 'E-justice, no ground for optimism', in: Proceedings of the 7th Eastern European e|Gov Days: eGovernment & eBusiness Ecosystem & eJustice April (22) -23 – 24, 2009, Prague Czech Republic.

Schmidt 2009b
A.H.J. Schmidt, 'Radbruch in cyberspace: about law-system quality and ict innovation', in: *Masaryk University Journal of Law and Technology*, Forthcoming.

Van den Herik 1991
H.J. van den Herik, *Kunnen computers rechtspreken?*, Arnhem: Gouda Quint BV, 1991.

Wittgenstein 1973
L. Wittgenstein, *Philosophical Investigations*, Oxford: Wiley-Blackwell, 1973.

DEEL IV

PRAKTIJK

Towards a Preliminary Knowledge Management Reasoning System to Improve Consistency of Sentencing

Martin Apistola■

Introduction

From the perspectives of equality before the law and legal certainty, a uniform application of law is crucial for the functioning and image of the judiciary.[1] Yet, many researchers have shown that there are inexplicable differences in sentencing of comparable cases.[2] All research together offers sufficient confirmation of the hypothesis that judges too often sentence inconsistently.[3]

This situation has become even more complex as the increase in availability and use of technology has contributed to an information overload in the judiciary; it is relatively simple to publish enormous amounts of sentencing knowledge.[4] The amount of sentencing information available to judges is so huge that it is hardly possible for them to become acquainted with all relevant sentencing knowledge. Furthermore, this situation grows worse as judges are often not aware of the possibilities of technology and it is often not clear to them how technology can be used to manage their knowledge. These are just a few examples of knowledge related problems in sentencing.

Different solutions to the problem have been proposed.[5] Some have suggested the establishment of a sentencing court. However, it is questionable whether this solution does not have the same objections as known to the existing jurisprudence-culture. Others have argued for the restriction of the judges' discretionary power by introducing guidelines and criminal sentencing rules. Empirical research shows that although many judges use guidelines for sentencing, the use of guidelines in verdicts is fragmented and the interpretation of the concept 'guideline' varies locally.[6] Others aim at developing information systems to make sentencing knowledge generally accessible. Empirical research, however, has shown that such systems are hardly being used.[7]

■ Martin Apistola is a researcher at the Hogeschool van Amsterdam.

1 Rapport Visitatie Gerechten 2006.
2 Tulder & Diephuis 2007, Schoep & Schuyt 2005; Duker 2003; Oskamp 1998.
3 Schoep & Schuyt 2005, Duker 2003, Oskamp 1998, Brenninkmeijer 1992, Schmidt 1992.
4 Oskamp, Apistola & De Mulder 2002, p. 167.
5 Oskamp 1998.
6 Schoep & Schuyt 2005.
7 *Idem.*

And so, developing a solution to decrease disparate sentencing remains an important point of interest, certainly now that the recent extension of the number of criminal court judges increases the risk of unjustified divergence.[8] The article aims at contributing to this goal; it focuses on the use of Case Based Reasoning principles to support Knowledge Management (KM) in courts. A provisional Knowledge Management Based Reasoning (KMBR) approach is presented as the first step of transforming the idea of a KM problem solving paradigm based on CBR approaches into reality. The aim of the paper is to organize ideas regarding CBR and KM and provide a preliminary basis for future research.

Knowledge Management and Sentencing

The agenda of the Council for the Judiciary in 2003 considers administering justice as a knowledge-intensive activity.[9] Based on this assumption, we introduce a new perspective on sentencing: considering sentencing as a knowledge-based activity.[10] From this knowledge-based perspective, inconsistent sentencing is seen as the result of differences in knowledge or knowledge-use. An important reason for differences in sentencing is that judges appear to have insufficient knowledge of judgements passed by their colleagues, who work in other courts of law.[11] By approaching sentencing from a knowledge-based perspective, taking away those differences becomes an activity of knowledge management.[12]

Since the nineties scientific research has much attention for studying an organisation as a "collection of knowledge". Or, in other words: there is a focus on the knowledge available within an organisation.[13] For that reason, organisations are being approached more and more from a knowledge-based perspective: the perspective which considers knowledge the strategically most important resource of an organisation. From this knowledge-based view, researchers try to get more grip on the knowledge of organisations. The most important subject of knowledge management is to optimize performance by managing knowledge.[14]

Knowledge management consists of different processes:[15] judges for example can – amongst others – collect, develop, share, evaluate and apply sentencing knowledge. These processes are also called knowledge processes. Tools such as information systems, sentencing guidelines, knowledge maps,

8 *Idem.*
9 Jaarplan 2003.
10 Schmidt 2005.
11 Oskamp 1998.
12 Schmidt 2005.
13 Spender 1996, Grant 1996, Kogut & Zander 1992, Alavi & Leidner 2001.
14 Van Engers 2001.
15 Apistola 2007, Weggeman 1997, Schreiber e.a. 2001, Boersma 2002.

courses and training, and expertise centres can support the deployment of knowledge processes. Other examples are meetings, reviews and feedback. Environmental factors such as the autonomy of judges, the organisational culture, the communication climate, motivation and management involvement also determine how knowledge processes are executed and how tools are being used.

Knowledge management concerns the management of knowledge, knowledge processes, tools and environmental factors and their mutual relationships.[16] The success of KM not only depends on whether some tool supports knowledge type 'explicit', but it depends on the whole package: do we have an optimal fit between the type of knowledge we want to manage, the knowledge processes we want to apply to that type of knowledge, the tools we want to use to support knowledge processes and, moreover, does our culture and management support the investment in tools and time needed to deploy the knowledge processes?

Most research and practice lacks attention for these mutual relationships. However, without insight in the KM elements and their mutual relations it is unclear how well knowledge processes are executed, what the use of tools is and how environmental factors influence knowledge management in the judiciary. Because of insufficient insight in the relationship between the core elements of knowledge management in the judiciary, it is hard to support the investment in new tools to support sentencing. For example: does a specific tool really support a knowledge process and is it supported by influential environmental factors? Instead of independently researching just a few KM elements, sentencing should be approached from a holistic KM point of view.

Even though many (scientific) publications about sentencing *or* knowledge management – and just a handful on *legal* KM – have appeared, there are hardly any (scientific) publications about the contribution of knowledge management to consistent sentencing. Amongst researchers, judges and within courts there seems hardly to be any urge to document KM cases and to develop a KM case base. Moreover, as yet, there are no computer programs to support the use of KM cases in courts. A well-known concept that could be used is the legal database that legal professionals use to search for case law. Besides that the concept of Case Based Reasoning could be deployed to support the use of KM cases. CBR is a technology for the development of knowledge based systems for amongst others the legal domain.

A lot of research has been done on the subjects of sentencing, KM and CBR, but their mutual relations have not been well studied. In opposite to many other knowledge management and sentencing research, this paper will take a first step towards a holistic approach of the core elements of sentencing and knowledge management such as knowledge, knowledge processes, tools, environmental factors and their mutual relationship.

16 Oskamp 2002, Holsapple & Joshi 2000.

Knowledge Management Based Reasoning[17]

There are a number of reasons why Knowledge Management Based Reasoning (KMBR) deserves more research and development in law practice and the AI&Law community:

Sentencing practice
By developing a Knowledge Management case base, a judge may become aware of the existence of different types of knowledge. Raising awareness is an important first step towards optimal knowledge management.[18] A KM case base can be used as a starting point for classification. By documenting a KM case a judge can get an idea of what knowledge he uses or needs, and how he can organize his knowledge. We see that judges often have trouble retrieving and storing the right knowledge. The structure of databases is often not based on the knowledge used and needed by individual judges. By documenting KM cases, it becomes possible to adjust and refine the structure of technology to the way judges work instead of the other way around. Further, by comparing KM cases of various judges, it becomes clearer what knowledge is really needed in courts.

On the basis of a KM case base, a judge might get an idea of the possible knowledge processes he can deploy. Based on his sentencing task, the judge may find out what knowledge processes are already important to him. A judge could also decide to pay more attention to a knowledge process that is documented in the KM case base. A collection of KM cases enables comparing knowledge processes of various judges and focusing on the support of knowledge processes that need more attention.

Currently, technology can support more than one knowledge process, but there is no overview in sentencing practice of what knowledge processes are important to judges. Much money and effort are invested in the introduction of technology, but it is not clear which technology supports what kind of knowledge process. So it seems that technology is used quite randomly to support knowledge processes. With the help of a KM case base it becomes clearer which knowledge processes are important to judges. As a consequence, more specific investments in technology support can be made.

A KM case base also provides a judge with a general overview of various means of technology support. Based on such an overview, the lawyer gets a first impression of the technology already used by colleagues, or technology that might turn out profitable to him. Currently we see that there is usually a whole range of technology support available in courts. This makes it hard for a judge to select the right type of technology. Different forms of technology support in KM cases make it easier for judges to select the right type of support.

17 This section is based on and inspired by Apistola & Lodder 2005, Aleven 1999 & Aleven 2002.

18 Apistola & Lodder 2005.

AI & law research

Just like the interaction between case law and legislation, documented KM cases offer clues to gaps in legal KM research. KM cases are useful for qualifying the facts of a KM case. They help to bridge the gap between abstract KM concepts and concrete KM facts. This may help to develop systems to support judges dealing with KM. Such systems aim to help judges in analyzing a KM problem and to use KM cases in argumentation to improve their knowledge management.

A Knowledge Management Based Reasoning (KMBR) application uses a collection of KM cases, called the KM case database. When a new KM problem is entered, the program selects the most relevant KM cases and generates argumentation fragments on the basis of these cases. In these arguments, the KM problem is compared with possibly conflicting KM cases that support different positions. The program also shows which objections can be put forward. This information helps to evaluate a KM problem and is therefore useful for a judge.

KMBR also helps to gain a better understanding of knowledge and reasoning of judges with regard to knowledge management. This is achieved by developing computer models and computer programs that simulate aspects of these reasoning processes. KMBR research should focus on the development of simplified models of argumentation on the basis of past KM cases in courts. Such a model describes how judges improve their knowledge management by using the most relevant KM cases, relevant similarities and differences between KM approaches, how the relevance of KM approaches can be estimated, etc.

KMBR is able to utilize general and specific knowledge of previously experienced, concrete KM situations (KM cases). A new KM problem is solved by finding a similar past KM case and reusing it in the new KM problem situation. KMBR is also an approach to incremental, sustainable knowledge development, since a new KM experience is retained each time a KM problem has been solved, making it immediately available for future problems. A better understanding of KM in courts can lead to better supporting sentencing programs.

KMBR problem solving[19]

What is KMBR? In essence, it means solving a new KM problem by remembering a previous similar KM situation and by reusing knowledge and knowledge of that KM situation. A judge, for example, who has had trouble finding knowledge in a database is informed about a judge who had the same problem but who was able to retrieve the knowledge he was looking for.

19 Based on Aleven 1999, Aleven 2002.

In KMBR terminology, a KM case denotes a KM problem situation. A previously experienced KM situation which has been captured and learned in such a way that it can be reused in the solving of future KM problems, is referred to as a past KM case, previous KM case, stored KM case, or retained KM case. Correspondingly, a new KM case or an unsolved KM case is the description of a new KM problem to be solved. KM-based reasoning is in effect a cyclic and integrated process of solving a KM problem, learning from this KM experience, solving a new KM problem, etc.

The KMBR system generates information that helps a judge to evaluate his KM case and to develop a new approach on the basis of relevant KM cases. When a new KM case is entered, the KMBR system selects the most relevant KM cases from its case base. For each KM case, it generates arguments. First, the system generates an argument based on analogy in which it compares the facts of the given KM case with those of the KM case found. This way it supports a position: the judge can use a certain KM approach or not. Secondly, the system constructs an argument a contrario. It show which drawbacks there are with regard to a KM approach. Where possible, the system shows the relevant differences between the new KM case and the previous KM cases. The system also generates arguments with regard to the importance of different KM approaches, seen in the light of (scientific) knowledge of knowledge management.

Representation of KM cases with factors[20]

An important question in modelling argumentation based on past KM cases is: how does the model describe or represent KM cases? In other words, what knowledge is stored about each KM case in a form accessible to the KMBR system? First of all, the KMBR system is concerned with the comparison of KM cases on basis of facts. The KM cases are represented with the help of factors. These are patterns of facts that make a KM approach stronger or weaker. The idea behind this is that it is often hard to define KM concepts in terms of necessary and sufficient conditions.

KM experts and judges will have different opinions about that. It is possible, though, to indicate which factors (should) play a role in the assessment of whether a KM concept is applicable or not. In KM literature there is, for example, no agreement on a definition of knowledge management. It does provide a list of five relevant factors: knowledge, knowledge processes, tools, environmental factors and their mutual relationship. In developing KMBR, this list may be extended on the basis of more research and experiences in sentencing practice. The correlation between these factors strengthens or weakens a KM approach.

20 Aleven 1999, Aleven 2002.

To store a KM case in the case database of the KMBR system, it first needs to be analysed to determine which of those factors are applicable. This information is stored in the KM case database. When a new KM case is added to the KMBR system, first the relevant factors need to be established. The following factors are based on the core elements of knowledge management: knowledge, knowledge processes, environmental factors, technology and the correlation between these elements.

- Knowledge Factors: Sentencing knowledge can be categorized as follows: (F1) administrative data, (F2) declarative knowledge, (F3) procedural knowledge, and (F4) analytical knowledge.[21] This taxonomy is only one possible classification and clearly needs to be refined for practical use. The value of these types of knowledge can be explicit or implicit.

- Knowledge Process Factors: A distinction can be drawn between the judge at work using his legal skills and knowledge, and how these activities can be supported by, for example, technology.[22] The latter activity is what the knowledge processes of this section refer to. These knowledge processes do not constitute the core knowledge work of a judge, but deal with organising and structuring his activities and the legal content necessary for performing sentencing. Basically, knowledge processes are activities of a judge that help him to manage his knowledge. The main knowledge processes for judges are (F5) developing (developed – not developed), (F6) sharing (shared – not shared) and (F7) evaluating (evaluated – not evaluated) knowledge.[23] This is a rather broad classification of knowledge processes and probably needs to be refined or extended to be of practical use in courts.

- Environmental Factors: Literature on legal knowledge management mentions a number of environmental factors that influence the success of knowledge management in courts: (F8) autonomy of judges (autonomous – not autonomous), (F9) organisational culture (open – closed), (F10) motivation (motivated – not motivated) and (F11) management commitment (commitment – no commitment).[24]

- Technology Factors: Courts have invested in technology support. In combining several existing distinctions, I introduce the following taxonomy of different types of IT support: (F12) word processors, (F13) databases, (F14) communication systems, (F15) knowledge-based systems (not used – used).[25] This classification of technology factors is rather gen-

21 Edwards & Mahling 1997.
22 Apistola & Lodder 2005.
23 Probst, Raub & Romhardt 2000; Oskamp 2000; Weggeman. 1997; Schreiber, Akkermans, & Anjewierden. 2001; Florijn, Van Gurchom & Van der Meulen 2000.
24 Terrett 1998; Gottschalk 1999; Rusanow 2002; Onwusah 1997; Parsons 2004.
25 De Mulder & Oskamp 1999; Matthijssen & Weusten 1999; Matthijssen, Voermans & Weusten 2002; Voermans & Van Kralingen 1999.

eral and clearly needs to be refined for practical use in courts. With the taxonomy I want to illustrate that it is possible to give a clear overview of technology used by, or is of interest to, judges. Each application has characteristics that can be used to evaluate how knowledge or knowledge process can be supported.

- Correlation factors: Three core factors relevant for knowledge management can be distinguished: knowledge, knowledge processes, technology and environmental factors. I used general taxonomies for each of these factors. In this paper the focus is on the role of technology in relation to knowledge processes. My classification of the relation between technology factors and knowledge factors, knowledge process factors and environmental factors is rather general and clearly needs to be refined for practical use in sentencing practice. With the taxonomy, I wish to illustrate that it is possible to give a clear overview of the relationship between all KM factors. Each technology has characteristics that can be used to evaluate how knowledge or knowledge process can be supported.
  - (F16) *Knowledge – Knowledge Process – Technology* (correlated – not correlated): Develop analytical knowledge: With the help of a word processor, a judge can study and combine analytical knowledge that has been made explicit. When analytical knowledge can be made explicit it may be stored in and retrieved from a database in a particular court. Analytical knowledge is a combination of declarative knowledge applied to a particular fact setting. Because it is so specific it may be hard to find on the internet. On the other hand, courts can gather this knowledge amongst their own judges and publish it on their intranets. Analytical knowledge is usually complex and it may be difficult to formulate and sent questions with the help of e-mail and groupware. Usually personal contact makes it easier to get feedback. Knowledge systems try to reach conclusions about the course of action in a specific situation and so help a judge to develop analytical knowledge.
  - (F17) *Environmental Factor – Technology* (correlated – not correlated): Powell and Dent-Micalleff notice that an open organisation and an open communication are variables most linked to the performance of information technology.[26] In an open culture, communication plays an important role. Especially IT-applications such as internet and intranet, e-mail and groupware could support that communication. In closed cultures managing and controlling information and IT-applications are more important.
  - (F18) *Environmental Factor – Knowledge Process* (correlated – not correlated): According to various authors, managing knowledge is related to the culture within an organisation. Wong notices that a culture

26 Powell & Dent-Micallef 1997.

which supports knowledge management usually is a culture in which knowledge is highly appreciated and in which the development, sharing and application of knowledge is strongly encouraged.[27] Uit Beijerse observes that knowledge use mainly depends on the organisational culture.[28]

Application

By applying the KMBR approach it is determined whether a knowledge management approach is useful for a judge. First of all the core KM-factors that play a role need to be inventoried, for example:

1. Knowledge: (F4) analytical knowledge
2. Knowledge process: (F6) sharing
3. Environmental factor: (F9) organisational culture
4. Correlation: (F18) Environmental Factor – Knowledge Process (correlated)

Next, research will have to show which combinations of factors lead to successful knowledge management.[29] When for example the factors 1-4 are respectively explicit, shared, open and correlated, the chance of success of the knowledge management approach increases. The next step is to collect previous KM cases (KMC1-4) and a case which must be decided upon (KMCn) (see table). In each case, it must be decided which factors and values played a role and the outcome of the KM approach used.

Case name	**Factor 1**	**Factor 2**	**Factor 3**	**Factor 4**	**Successful KM approach**
KMC 1	Explicit / implicit	Shared / not shared	Open / closed	Correlated / not correlated	Yes / no
KMC 2	Explicit / implicit	Shared / not shared	Open / closed	Correlated / not correlated	Yes / no
KMC 3	Explicit / implicit	Shared / not shared	Open / closed	Correlated / not correlated	Yes / no
KMC 4	Explicit / implicit	Shared / not shared	Open / closed	Correlated / not correlated	Yes / no
KMC n	Implicit	Shared	Open	Correlated	?

27 Wong 2005.
28 Beijerse 2000.
29 Apistola 2007.

To answer the question whether a knowledge management approach can be used in KMCn we look for identical factors. When for example the factors 2-4 are identical, KMC2 can be used to argue that a knowledge management approach is useful. On the other hand it may be argued that a knowledge management approach is not useful because in KMC4 not only the factor 2 and 4 are identical but also factor 1.

Conclusion

Inconsistency of sentencing is a societal problem. Sentencing has a great impact on the suspect and the sentence is for society the most recognisable part of the entire process of sentencing.[30] The sentence is also the signal towards society that indicates what the consequences are of certain actions. It is also often the subject of the first question the public asks when there is a verdict. Nowadays the public is better informed about sentencing decisions because the media often extensively report about criminal cases and sentencing decisions. As a consequence of the research of inconsistency in sentencing and the greater familiarity of the public with verdicts in concrete cases, inconsistencies in sentencing have become a subject of the public debate.[31] So it is of great importance for the judge to arrive at a well-thought sentencing decision. By developing a KM method to stimulate consistent sentencing this societal problem may be reduced.

Sentencing is not just a cultural or technological or economical problem. All these problems are related. The KM approach should take into account that these core aspects as well as some other aspects of sentencing are related. Inconsistency of sentencing may be improved by a holistic approach of knowledge management support and sentencing.

In the near future, parts of the research results may be implemented in the work of judges. In the far future, the entire KM-method may become part of the sentencing practice. When the KM method helps to improve consistency of sentencing decisions, this may have a great impact on the practice of sentencing. This proposed research helps to make clear whether investing in knowledge management within the Administration of Justice and more specific, sentencing, is justified. Studying the relationship between sentencing and knowledge management helps to make clear how a vague subject can be measured in practice.

The proposed research also offers the possibility to further develop the research discipline of legal knowledge management which is still in its infancy. For that the research can make clear on which points knowledge management, Case Based Reasoning need to be developed to contribute to consistent sentencing. Research in the area of knowledge management and sentencing

30 Schoep & Schuyt 2005.
31 *Idem*.

must be brought together in one overview. This way it should become clear to what extent the various research results fit together.

The new research approach may be more effective than existing approaches, as it takes into account all core knowledge management elements *and their mutual relations* to support sentencing instead of just one or a few elements or relations.

References

Alavi & Leidner 2001
M. Alavi and D.F. Leidner, 'Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues', *Mis Quarterly* (25) 2001-1.

Alavi & Tiwana 2003
M. Alavi and A. Tiwana, 'Knowledge Management: The Information Technology Dimension', In M. Easterby-Smith & M. Lyles, *Handbook Of Organizational Learning and Knowledge Management*, 2003.

Apistola & Lodder 2005
M. Apistola and A.R. Lodder, 'Law Firms and IT – Towards Optimal Knowledge Management', *The Journal Of Information, Law And Technology (Jilt)*.

Apistola 2001
M. Apistola, Een kwalificatie van kennistypen in domeinmodellen voor straftoemeting. Afstudeerscriptie Haagse Hogeschool, 2001.

Apistola 2007
M. Apistola, *Advocaat en Kennismanagement*, Diss. Vu University Amsterdam, 2007.

Apistola, Mommers & Lodder 2001
M. Apistola, L. Mommers and A. Lodder: A Knowledge Management Exercise In The Domain Of Sentencing: Towards An Xml Specification, Jurix 2001.

Apistola, Warnier, Oskamp & Brazier 2007
M. Apistola, M. Warnier, A. Oskamp and F.M.T. Brazier, 'Towards A Conceptual Framework for Digital Dossier Management in Criminal Proceedings', in: *Proceedings Of The Fifth International Conference On Law and Technology* (Lawtech 2007), 2007.

Boer 2005
N.I. Boer, *Knowledge Sharing Within Organizations. A Situated and Relational Perspective*, Dissertation Erasmus University Rotterdam, 2005.

Boersma 2002
S.K.Th. Boersma, *Management Van Kennis. Een Creatieve Onderneming*, Assen: Koninklijke Van Gorcum 2002.

Carine 2003
H. Carine (2003), 'Applying Knowledge Management In Law Firm Alliances', *10th Asia Pacific Special Health And Law Librarians Conference*, Adelaide.

Commissie Leemhuis 1998
Commissie Leemhuis (Commissie Toerusting En Organisatie Zittende Magistratuur), Rechtspraak Bij De Tijd, Den Haag, 1998.

De Mulder & Oskamp 1999
R.V. De Mulder and A. Oskamp. Juridisch Kennismanagement, in A. Oskamp and A.R.Lodder (eds.), *Informatietechnologie Voor Juristen – Handboek Voor De Jurist In De 21ste Eeuw*, Kluwer, Deventer, 1999.

Disterer 2003
G. Disterer, 'Fostering Knowledge Sharing: Why and How?', In: Reis, A.P.D., Isaias, P. (eds.), *Proceedings Of The Iadis International Conference E-Society 2003*, Lissabon: Iadis, 2003.

Disterer 2005
G. Disterer, *Results Of An Empirical Study, Knowledge Management In International Professional Services Firms* (Kmipsf 2005), Workshop, 2005.

Du Plessis 2004
T. Du Plessis, *Information and Knowledge Management In Support Of Legal Research In A Digital Information Environment* (Diss. Rand Afrikaans Universiteit) 2004.

Dublin 2005
M. Dublin, *Creating An Environment In Law Firms Where Knowledge Management Will Work*, Http://Www.Articlecity.Com/Articles/Legal/Article_165.Shtml.

Duker 2003
M. Duker, *Legitieme Straftoemeting*, Boom Juridische Uitgevers, Den Haag, 2003.

Edwards & Mahling 1997
D.L. Edwards and D.E. Mahling, *Toward Knowledge Management Systems In The Legal Domain*, Acm, 1997.

Florijn, Van Gurchom & Van Der Meulen 2000
R. Florijn, M . Van Gurchom, and M. Van Der Meulen. *Kennis Leren Managen – De Theorie En Praktijk Van Kennismanagement*. Ten Hagen & Stam, 2000.

Forstenlechner 2005
I. Forstenlechner, *Impact Of Knowledge Management On Law Firm Performance. An Investigation Of Causality Across Cultures* (Dissertation) School Of Industrial and Manufacturing Science 2005.

Gerechtshof Arnhem Jaarplan 2007
Gerechtshof Arnhem, Jaarplan 2007.

Gerechtshof Arnhem, Jaarverslag 2006
Gerechtshof Arnhem, Jaarverslag 2006.

Gore & Gore 1999
C. Gore and E. Gore, Knowledge Management: The Way Forward, Total Quality Management, Vol. 10, Nos 4&5, 1999.

Gottschalk 1999
P. Gottschalk, 'Use Of It For Knowledge Management In Law Firms', The Journal Of Information, Law And Technology (Jilt) 1999-3.

Gottschalk 2005
Gottschalk, P., Brekke, K., Pedersen, H.C., Incentives For Knowledge Sharing Through Information Technology In Law Firms, Virtual Law Journal, 2005.

Grant 1996
R.M. Grant, 'Toward A Knowledge-Based Theory Of The Firm', *Strategic Management Journal* (17), 1996, p. 110.

Gurteen 1999
D. Gurteen, 'Creating A Knowledge Sharing Culture', *Inside Knowledge*, 1999-2 (5).

Hall 2001
H. Hall, 'Input-Friendliness. Motivating Knowledge Sharing Across Intranets', *Journal Of Information Science* (27), 2001-3.

Hansen Et Al. 2002
M.T. Hansen, N. Nohria and T. Tierney, 'Wat is jouw strategie voor het managen van kennis?, in: *Harvard Business Review On Organizational Learning*, Zaltbommel: Thema 2002.

Hartendorp 2008
R. Hartendorp, Praktisch gesproken. Alledaagse civiele rechtspleging als praktische oordeelsvorming , Dissertatie Erasmus Universiteit Rotterdam, 2008.

Hinds & Pfeffer 2001
P.J. Hinds and J. Pfeffer, 'Why Organizations Don't "Know What They Know". Cognitive And Motivational Factors Affecting The Transfer Of Expertise', *Research Paper Series Graduate School Of Business*, Stanford University 2001.

Hinds & Pfeffer 2003
P.J. Hinds and J. Pfeffer, 'Why Organizations Don't Know What They Know. Cognitive And Motivational Factors Affecting The Transfer Of Knowledge', in: M. Ackerman, V. Pipek, V. Wulf (eds.), *Beyond Knowledge Management. Sharing Expertise*, Cambridge: Mit Press 2003.

Holsapple & Joshi 2000
C.W. Holsapple and K.D. Joshi, 'An Investigation Of Factors That Influence The Management Of Knowledge In Organizations', *Journal Of Strategic Information Systems*, 2000, p. 239-240.

Hunter et al. 2002
L. Hunter, P. Beaumont and M. Lee (2002), "Knowledge Management Practice In Scottish Law Firms", Human Resource Management Journal, 12 (2), pp. 4-21.

Huysman & De Wit 2000
M. Huysman and D. De Wit, *Kennis Delen In De Praktijk. Vergaren, Uitwisselen En Ontwikkelen Van Kennis Met Ict*, Assen: Van Gorcum, 2000.

Huysman & De Wit 2002
M. Huysman and D. De Wit, *Knowledge Sharing In Practice*, Dordrecht: Kluwer 2002.

Inkpen 1996
A.C. Inkpen, 'Creating Knowledge Through Collaboration', *California Management Review* (39), 1996-1.

Jaarplan voor de Rechtspraak 2004
Jaarplan voor de Rechtspraak 2004.

Jaarplan voor de Rechtspraak 2003
Jaarplan voor de Rechtspraak 2003.

Jaarverslag 2004 Rechtbank Utrecht
Jaarverslag 2004 Rechtbank Utrecht.

Jongedijk & Matthijssen 2004
S. Jongedijk and L. Matthijssen, *Stand Van Kennismanagement In De Advocatuur*, Rotterdam, 2004.

Khandelwal & Gottschalk 2003
K. Khandelwal and P. Gottschalk, *A Knowledge Management Survey Of Australian Law Firms*, 2003.

Kogut & Zander 1992
B. Kogut and U. Zander, 'Knowledge Of The Firm, Combinative Capabilities, And The Replication Of Technology', *Organization Science* (3), 1992-3.

Matthijssen & Weusten 1999
L. Matthijssen And M.C.M. Weusten. Typologie Van Juridische Informatietechnologische Toepassingen, in A. Oskamp And A.R. Lodder, Editors, *Informatietechnologie Voor Juristen*, Kluwer, Deventer, 1999.

Matthijssen, Voermans & Weusten 2002
L. Matthijssen, W. Voermans, And M.C.M. Weusten. *Informatietechnologie Voor Juristen – Handboek Voor De Jurist In De 21ste Eeuw*, Chapter It-Toepassingen In De Juridische Praktijk. Kluwer, 2002.

Mintzberg 1992
H. Mintzberg, *Organisatiestructuren*, Schoonhoven: Academic Service 1992.

Nahapiet & Ghoshal 1998
J. Nahapiet and S. Ghoshal, 'Social Capital, Intellectual Captial, And The Organizational Advantage', *Academy Of Management Review* (23) 1998-2.

Onwusah 1997
B. Onwusah, 'The Investment Conundrum', The Journal Of Information, Law And Technology (Jilt) 1997-2.

Oskamp & Lauritsen 2003
A. Oskamp and M. Lauritsen, 'Ai And Law In Practice? So Far Not Much', in *AI And Law And Practice*, Artificial Intelligence And Law, Volume 10, 2003.

Oskamp 2000
A. Oskamp, *Onderneming En Ict*, Chapter Beheer Van Juridische Kennis In Het Ittijdperk. W.E.J. Tjeenk Willink, 2000.

Oskamp e.a. 1999
A. Oskamp, M. Tragter and A.R. Lodder, 'Mutual Benefits For Ai & Law And Knowledge Management', *Proceedings Of The Seventh International Conference On Artificial Intelligence And Law*, Acm, New York, 1999.

Oskamp e.a. 2002
A. Oskamp, M. Apistola and R.V. De Mulder, 'Kennismanagement Voor Juristen', in: A. Oskamp & A.R. Lodder (eds.), *Informatietechnologie Voor Juristen*, Deventer: Kluwer 2002.

Oskamp, Apistola & De Mulder 2002
A. Oskamp, M. Apistola and R.V. De Mulder, 'Kennismanagement Voor Juristen', in: A. Oskamp & A.R. Lodder (eds.), *Informatietechnologie Voor Juristen*, Deventer: Kluwer 2002.

Osterloh & Frey 2000
M. Osterloh and B.S. Frey, 'Motivation, Knowledge Transfer, And Organizational Forms', *Organization Science* (11), 2000-5.

Parsons 2004
Parsons, M. (2004), *Effective Knowledge Management For Law Firms*, Oxford University Press.

Powell & Den-Micallef 1997
T.C. Powell and A. Dent-Micallef, 'Information Technology As Competitive Advantage: The Role Of Human, Business, And Technology Resources', *Strategic Management Journal* (18), 1997-5.

Probst, Raub & Romhardt 2000
G. Probst, S. Raub and K. Romhardt. *Effectief Omgaan Met Kennis*, Scriptum Management, 2000.

Programma Strafsector 2010
Programma Strafsector 2010, *Deskundigheidsbevordering En Kennisinfrastructuur.*

Rapport Visitatie Gerechten 2006
Rapport Visitatie Gerechten 2006.

Rusanow 2002
G. Rusanow, *Global Law Firm Knowledge Management Survey Report*, Curve Consulting 2002.

Rusanow 2003
G. Rusanow, *Knowledge Management And The Smarter Lawyer*, New York: Alm Publishing 2003

Rusanow 2006
G. Rusanow (2006), *Global Law Firm Knowledge Management Survey*, http://www.llrx.com/node/1705/.

Scarbrough & Swan 2001
H. Scarbrough and J. Swan, 'Explaining The Diffusion Of Knowledge Management. The Role Of Fashion', *British Journal Of Management* (12), 2001.

Schmidt 2005
A.H.J. Schmidt, 'De Cirkel Is Rond', in: *Trema Bulletin* 2, 2005, p. 43-47.

Schoep & Schuyt 2005
A. Schoep, P. Schuyt , *Instrumenten Ter Ondersteuning Van De Rechter Bij De Straftoemeting*, E.M. Meijers Instituut, Leiden 2005.

Schoep 2008
A. Schoep, *Straftoemetingsrecht en Strafvorming*, Diss. Leiden University, Deventer: Kluwer 2008.

Schreiber et al. 2001
G. Schreiber, H. Akkermans and A. Anjewierden, Knowledge Engineering And Management, MIT Press, 2001.

Schulz & Klugmann 2005
M. Schulz and M. Klugmann, 'Creating A Culture Of Knowledge Sharing In Law Firms. Some Obstacles And Solutions', in: K.D. Althoff E.A. (eds.), Wm 2005, Lnai 3782, Berlin: Springer-Verlag 2005.

Spender 1996
J.C. Spender, 'Making Knowledge The Basis Of A Dynamic Theory Of The Firm', *Strategic Management Journal* (17), 1996.

Susskind 1998
R. Susskind, *The Future Of Law. Facing The Challenges Of Information Technology*, Oxford: University Press 1998.

Terret 1998
A. Terrett, 'Knowledge Management And The Law Firm', Journal Of Knowledge Management (2), 1998-1.

Tjaden 2007
T. Tjaden (2007), *The Role Of Law Firm Culture In Knowledge Management*, http://www.Slaw.Ca/2007/06/29/The-Role-Of-Law-Firm-Culture-In-Knowledge-Management.

Uit Beijers 2000
R.P. Uit Beijerse, 'Knowledge Management In Small And Medium-Sized Companies.Knowledge Management For Entrepreneurs', *Journal Of Knowledge Management* (4), 2000-2.

Valente 1999
V. Valente, Case-Based Reasoning, In: A. Oskamp & A.R. Lodder (eds.), *Informatietechnologie Voor Juristen*, Deventer: Kluwer 1999.

Valente 2002
V. Valente, Case-Based Reasoning, In: A. Oskamp & A.R. Lodder (eds.), *Informatietechnologie Voor Juristen*, Deventer: Kluwer 2002.

Van Den Brink 2003
P. Van Den Brink, *Social, Organizational, And Technological Conditions That Enable Knowledge Sharing* (Dissertation) Technical University Delft, 2003.

Van Den Hooff & De Ridder 2004
B. Van Den Hooff and J.A. De Ridder, 'Knowledge Sharing In Context: The Influence Of Organizational Commitment, Communication Climate And Cmc Use On Knowledge Sharing', *Journal Of Knowledge Management* (8), 2004-6.

Van Den Hooff, Ridder & Vijvers 2002
B. Van Den Hooff, J. De Ridder and J. Vijvers, 'Knowing What To Manage. The Development And Application Of A Knowledge Management Scan', *Third European Conference On Organisational Knowledge*, Learning And Capabilities, Athens: Greece, 2002.

Van Engers 2001
T.M. Van Engers, *Knowledge Management. The Role Of Mental Models In Business Systems Design* (Diss. Amsterdam VU), Belastingdienst 2001.

Van Tulder & Diephuis 2007
F. Van Tulder and B. Diephuis, Afgewogen Straffen. Analyse en verbetering van de databank consistente straftoemeting, *Research Memoranda Raad Voor De Rechtspraak*, Nr. 4, Jaargang 3, 2007.

Voermans & Van Kralingen 1999
W. Voermans and R.W. Van Kralingen. Informatie- en communicatietechnologie in de juridische praktijk, in: A. Oskamp and A.R. Lodder (eds.), *Informatietechnologie voor Juristen*, Kluwer, Deventer, 1999.

Weggeman 1997
M. Weggeman. *Kennismanagement – inrichting en besturing van kennisintensieve organisaties*, Scriptum Management, 1997.

Wong 2005
K.Y. Wong, 'Critical Success Factors For Implementing Knowledge Management In Small And Medium Enterprises', *Industrial Management & Data Systems* (105), 2005-3.

E-discovery

Hans Fokker■

Inleiding

Het gebruik van elektronische documenten heeft in arbitrage geleid tot aanvankelijk niet voorziene ontwikkelingen op het gebied van 'discovery', een zo dadelijk toe te lichten begrip uit het Engelse en Amerikaanse procesrecht. Deze hebben onlangs tot een discussie in de beroepsgroep geleid, waarover hierna eveneens meer.[1]

Susskind en de ontwikkeling van 'discovery'

Richard Susskind, o.a. IT-adviseur van de Britse Lord Chief Justice, publiceerde in 1996 het boek 'The Future of Law'. Dat was in de tijd dat e-Bay en Amazon nog in de kinderschoenen stonden en dat Google en de BlackBerry nog moesten worden uitgevonden. Hij voorspelde dat informatietechnologie binnen twintig jaar de rechtspraktijk fundamenteel zou veranderen, onder andere door de intrede van elektronische post (e-mail). Zijn voorspelling kwam al binnen tien jaar uit.

In The Times schreef dezelfde Susskind in 2006 dat sommige rechtshelpers intussen de mogelijkheden van Internet hebben ontdekt: van on-line juridisch advies tot het veilen van juridische dienstverlening, van multimediale kennissystemen tot virtuele case rooms. Toch zijn deze initiatieven nog betrekkelijk zeldzaam. Men mag denken dat men de revolutie heeft doorstaan, maar het echte werk moet nog komen. Susskind voorspelt dat de komende tien jaar een stijgende lijn in de snelheid van de ontwikkelingen te zien zal geven. Geavanceerde systemen op het gebied van het verzamelen van documenten zullen naar zijn mening een elementaire omslag veroorzaken bij het geven van maatadvieswerk. De grondslagen van geschillenbeslechting zullen drastisch veranderen door een combinatie van elektronische 'discovery' of 'disclosure', elektronische aanlevering van dossiers aan rechterlijke instanties en on-line geschillenbeslechting. Juridische scholing en post-academische opleiding zullen op een andere basis worden opgezet, zoals e-learning en on-line communiceren. Tegelijkertijd zal de relatie tussen

---

■ Hans Fokker is vice-president van het Gerechtshof Arnhem.

1 Fragment uit Fokker 2009.

advocaat en cliënt onherkenbaar veranderen, doordat zij zullen opereren onder hetzelfde virtuele dak, in on-line samenwerking en communicatie, aldus Susskind.

Wie om zich heen kijkt ziet dat Susskind gelijk krijgt, bijvoorbeeld op het gebied van 'discovery". Eerst een paar opmerkingen over 'discovery', daarna iets meer over 'e-discovery'. Het uit het Engelse burgerlijk procesrecht[2] en de USA bekende begrip 'discovery' houdt globaal in dat partijen, voordat de procedure bij de rechter begint, elkaar om informatie kunnen en mogen vragen die mogelijk van dienst kan zijn in die procedure.[3] De andere partij is in beginsel verplicht die informatie te leveren. De rechter kan zonodig op verzoek van een partij ingrijpen. Het idee is dat partijen open kaart spelen en dat de feiten aan het begin van de procedure meteen op tafel liggen. Misschien, zo is de gedachte, is de procedure voor de rechter zelfs niet eens meer nodig is als de zaak voor partijen helder is geworden door de 'discovery'.

Een nadeel is dat in de praktijk zo'n onderneming kan ontaarden in een 'fishing expedition', doordat partijen elkaar het hemd van het lijf vragen in de hoop iets belastend op te vissen wat tegen de wederpartij gebruikt kan worden. Op de geheime agenda staat dan bijvoorbeeld: als we nu eens álle notulen van vele jaren van álle bestuursvergaderingen van de onderneming gaan doorspitten, misschien komen we dan wel iets van onze gading tegen.

Een ander nadeel is dat dergelijke zoektochten hoge kosten meebrengen, niet in het minst aan rekeningen van de advocaten. Worden de woorden 'discovery' en 'fishing expedition' vaak in één adem genoemd, daaraan kan de term 'lawyers paradise' zonder omwegen worden toegevoegd.

Discovery in Nederland

De Nederlandse wet kent niet een dergelijke algemene exhibitieplicht, in die zin dat partijen jegens elkaar of ten opzichte van de rechter verplicht zijn en gedwongen kunnen worden tot het verschaffen van informatie en documenten, zoals in de USA. Wel hebben wij art. 843a Rv, dat een bijzondere exhibitieplicht regelt. Het slaat, aldus de beraadslaging in de Eerste Kamer,[4] op de situatie dat de inhoud van een schriftelijke bewijsmiddel aan een partij in beginsel wel bekend is, maar dat zij het niet in haar bezit heeft.

Lid 1 luidt: "Hij die daarbij rechtmatig belang heeft, kan op zijn kosten inzage, afschrift of uittreksel vorderen van bepaalde bescheiden aangaande een rechtsbetrekking waarin hij of zijn rechtsvoorganger partij zijn, van degene die deze bescheiden te zijner beschikking of onder zijn berusting heeft. Onder bescheiden wordt mede verstaan: op een gegevensdrager aangebrachte gegevens". Dat woord 'bepaalde' moet 'fishing expeditions' uit-

2 Zie Van den Reek, p. 111 e.v.
3 Zie ook Krzeminski 2008, p. 47.
4 Algemene beraadslaging Eerste Kamer, *Parlementaire geschiedenis bewijsrecht*, p. 417.

sluiten. Volgens lid 2 bepaalt de rechter zo nodig de wijze waarop inzage, afschrift of uittreksel zal worden verschaft. Lid 3 ontheft 'geheimhouders' van de exhibitieplicht, terwijl het vierde en laatste lid degene die de bescheiden onder zijn berusting heeft vrijstelt, indien daarvoor "gewichtige redenen zijn, alsmede indien redelijkerwijs aangenomen kan worden dat een behoorlijke rechtsbedeling ook zonder verschaffing van de gevraagde gegevens is gewaarborgd".

Een partij kan slechts inzage etc. vragen van een met name genoemd document. Men moet daarbij bovendien een rechtmatig belang hebben, de enkele interesse is niet genoeg. Al met al dus een veel beperktere exhibitieplicht dan in de USA.

Discovery en arbitrage

Voor arbitrage geldt dat in art. 1039 lid 4 Rv wordt bepaald, dat het scheidsgerecht bevoegd is overlegging van 'stukken' te bevelen. Het scheidsgerecht kan dat ambtshalve doen (al dan niet op initiatief van een partij). Het verschil met art. 843a lid 1 Rv is dat art. 1039 lid 4 Rv niet beperkt is tot bepaalde aangeduide genoemde stukken, al zal ook daar een belang bij de overlegging aanwezig moeten zijn.[5] Vergelijk art. 22 Rv dat de rechter de bevoegdheid geeft te bevelen bepaalde, op de zaak betrekking hebbende stukken, over te leggen. Partijen kunnen dit weigeren indien daarvoor gewichtige redenen zijn. De rechter beslist of de weigering gerechtvaardigd is, "bij gebreke waarvan hij daaruit de gevolgtrekking kan maken die hij geraden acht". Deze dreigende toevoeging betekent dat de rechter een ongegronde weigering in het nadeel van de weigerende partij mag uitleggen. Ditzelfde geldt ook allemaal voor het scheidsgerecht.

Verhouding Verenigde Staten – Nederland

Deze Nederlandse wettelijke bepalingen leveren weliswaar geen 'discovery' naar Amerikaans recht op, maar dat neemt niet weg dat het toch nuttig is stil te staan bij de speciale problemen die, naar Amerikaanse ervaring met 'discovery', het produceren van elektronische bewijsstukken kunnen meebrengen.

Dit geldt te meer waar niet uitgesloten is dat bewijs, verkregen in een Amerikaanse 'discovery'-procedure, gebruikt kan worden in procedures voor de Nederlandse rechter[6] en niet valt in te zien waarom dat niet zou gelden voor een Nederlands scheidsgerecht. Bovendien wordt ook in Neder-

5 Zo eist artikel 28 lid 2 NAI arbitragereglement dat het scheidsgerecht bevoegd is bepaalde, door het scheidsgerecht relevant geachte stukken over te laten leggen.

6 Zie Krzeminski 2008, p. 47 e.v.

land gedacht over de vraag of de huidige regeling van de exhibitieplicht van art. 843a Rv aanpassing behoeft en, zo ja, op welke wijze. Verwezen kan worden naar de Adviescommissie voor het Burgerlijk Procesrecht. Deze commissie, door de Minister van Justitie gevraagd om advies naar aanleiding van het eindrapport Fundamentele Herbezinning van de Commissie Asser-Groen-Vranken, heeft bij brief van 14 juli 2008 haar advies over gegevensverstrekking in burgerlijke zaken ('discovery') aangeboden aan de Minister.[7]

De Adviescommissie doet voorstellen voor een wettelijke regeling, op te nemen in het Wetboek van Burgerlijke Rechtsvordering.[8] Zij neemt een medewerkingsplicht aan de waarheidsvinding tot uitgangspunt, waarop een correctief past dat geen medewerking kan worden verlangd waar dat kennelijk – dus: beoordeeld aan de hand van een marginale toetsing – disproportioneel zou zijn. Zij stelt voor vier artikelen (155a tot en met d) aan Rv toe te voegen, waarin aan een ieder die de beschikking heeft over bepaalde gegevens de plicht wordt opgelegd die gegevens, na deze zonodig te hebben opgespoord, op de voet van de nieuwe regeling te verstrekken, op kosten van degene die aanspraak maakt op de verstrekking. De rechter gelast de gegevensverstrekking, na hoor en wederhoor, slechts dan wanneer dat niet in strijd is met de belangen van betrokkenen. Daaronder worden mede begrepen het gewicht van de burgerrechtelijke rechtsbetrekking waarop de aanspraak betrekking heeft, de belasting die van de tot verstrekking aangesprokene of van anderen gevergd wordt en gerechtvaardigde aanspraken op het inachtnemen van vertrouwelijkheid of het respecteren van de persoonlijke levenssfeer. In dit advies wordt geen speciale aandacht besteed aan elektronisch opgeslagen gegevens. In de USA bestaan daarover al wel regels.

In de USA hebben de federale gerechten met ingang van 1 december 2006 de bestaande regels voor procedures op het gebied van 'discovery' (Federal Rules of Civil Procedure) aangepast aan het bestaan van elektronische documenten (in de wandeling: 'the amended Federal Rules' of '2006 amendments').[9] Staten als New York, Californië en Illinois zijn gevolgd. Verder heeft een werkgroep van een invloedrijke Amerikaanse denk-tank genaamd The Sedona Conference de wijdverbreide 'Sedona Principles Adressing Electronic Document Production' het licht doen zien, waarin prin-

7 Asser, Groen & Vranken 2006.

8 Het advies is gepubliceerd in het Tijdschrift voor Civiele Rechtspleging, 2008, nr. 4, p. 123.

9 Zie E-discovery Amendments to the Federal Rules of Civil Procedure and Committee Notes, www.uscourts.gov/rules/congress0406.html. The Advisory Committee on Civil Rules of the US Judicial Conference was reeds in 1999 begonnen met het ontwerpen van de regels. Het ontwerp werd goedgekeurd door de Judicial Conference in 2005. Toen bleek dat de US Senate en het Supreme Court geen bezwaren hadden traden zij op 1 december 2006 in werking. Het gaat om de Federal Rules 16, 26, 33, 34, 37 en 45.

cipes van e-discovery worden weergegeven en van commentaar worden voorzien.[10]

In deze 'Federal Rules' is de benadering van 'e–discovery' deze, dat 'discovery' van elektronisch opgeslagen materiaal is "now on equal footing with discovery of paper documents", voorts dat de beginselen die gelden voor gewone 'discovery' ook van toepassing worden verklaard op de elektronische variant en ten slotte dat speciale regels voor de elektronische 'discovery' daaraan zijn toegevoegd. Partijen in een gerechtelijke procedure voor een federale rechter zijn in beginsel gerechtigd tot alle elektronische informatie, net als bij 'hard copy'-materiaal, mits binnen de perken (het materiaal moet zijn: "reasonably calculated to lead to the discovery of admissible evidence at trial").

Men wilde de nieuw toegevoegde regels flexibel houden, om toekomstige ontwikkelingen bij te kunnen benen zonder de regels te hoeven veranderen. Ook hier is het streven dus naar zoveel mogelijk technologie-onafhankelijke regels. Dat heeft als keerzijde dat nogal wat open normen zijn toegevoegd. Zo wordt in de nieuwe Rule 26 (a)(2) onder B de beperking gesteld dat een partij geen elektronisch opgeslagen informatie behoeft te verschaffen uit bronnen "that the party identifies as not reasonably accessible because of undue burden or cost". De buitensporige belasting en kosten dienen te worden bewezen door de partij van wie de informatie wordt gevraagd. Bij onenigheid beslist de rechter, al dan niet met daaraan door hem verbonden voorwaarden ("The court may specify conditions for the discovery"). Volgens de Toelichting ("Committee Notes") hangt de beslissing van de rechter niet alleen af van de belasting en de kosten voor de responding party, maar ook van de vraag of deze gerechtvaardigd worden door de omstandigheden van het geval. Overwegingen daarbij kunnen bijvoorbeeld zijn: (1) of het verzoek tot discovery voldoende gespecificeerd is, (2) of elders de gewenste informatie aanwezig is in gemakkelijker toegankelijke bronnen, (3) het antwoord op de vraag of de 'responding party' met goede reden nalaat gevraagde informatie te verstrekken die waarschijnlijk wel heeft bestaan maar niet meer eenvoudig beschikbaar is te stellen, (4) welke voorspelling valt te geven over het belang en het nut van de informatie, (5) het belang van de onderwerpen die in geschil zijn, en (6) de middelen waar-

10 The Sedona Principles: Best Practices recommendations and Principles for Adressing Electronic Document production (2nd ed. June 2007), www.thesedonaconference.org. In het voorwoord van de Principles omschrijft de Sedona Conference zichzelf als een verzameling van "the nation's finest lawyers, consultants, academics and jurists to address current problems in the areas of antitrust law, complex litigation and intellectual property rights that are either ripe for solution or in need of a 'boost' to advance law and policy". De eerste werkgroep is ontstaan in oktober 2002 en was gewijd aan de ontwikkeling van richtlijnen voor behoud en produceren van elektronische documenten. In maart 2003 werd een ontwerp van de Principles gepubliceerd, die meteen werden geciteerd in een rechterlijk adviescomité betreffende electronic discovery en in een van de eerste beslissingen van een rechterlijke instantie over het onderwerp e-discovery (Federal District Court in New York), aldus Appendix D bij de Principles.

over partijen beschikken.[11] De verzoekende partij moet zo nodig aantonen, eventueel steekproefsgewijs, dat de noodzaak van 'discovery' opweegt tegen de belasting en kosten die gepaard gaan met het opsporen en tevoorschijn brengen van de informatie. Ook kan de rechter als voorwaarde stellen dat de verzoekende partij de kosten van het opsporen en produceren van de informatie voor zijn rekening neemt.

Veel zal dus afhangen van de omstandigheden van het geval en van de beslissing van de rechter, als partijen het niet eens kunnen worden.

Daar komt bij dat de omschrijving "elektronisch opgeslagen informatie" zeer ruim is. In de Committee Notes valt te lezen dat men het niet mogelijk achtte de verschillende soorten technologische mogelijkheden te definiëren die van invloed kunnen zijn op de problemen en de kosten, die het toegang verkrijgen tot elektronisch opgeslagen informatie mee kunnen brengen.

Partijen worden door de Rules gedwongen voor aanvang van de 'discovery' eerst met elkaar stil te staan bij de problemen die zich kunnen voordoen en hoe zij deze willen oplossen, zoals: wordt de gevraagde informatie geprint op papier of wordt deze elektronisch aangeleverd (bijvoorbeeld in Portable Document Format, PDF). Daarbij moeten zij elkaar over en weer inlichten over de met het een en ander gemoeide inspanning en kosten. Op de wederpartij ligt in dit verband ook de verplichting naar categorie en type de bronnen op te geven waar *niet* wordt gezocht (maar wel zou kunnen worden gezocht), zodat de verzoekende partij kan beoordelen of het de moeite waard is daar toch nader op in te gaan.

De Sedona Principles

De werkgroep van de Sedona Conference, die de Sedona Principles het licht heeft doen zien, onderscheidt eveneens tussen het wel of niet toegankelijk zijn van de informatie. Zodra het gaat om niet gemakkelijk toegankelijke informatie ("disaster recovery back-up tapes and other sources of electronically stored information that are not reasonably accessible") moet de verzoekende partij de noodzaak en het belang van het ophalen van deze informatie aantonen tegenover de belangen van de wederpartij om niet te hoeven voldoen aan het verzoek, "including the disruption of business and information management activities" (Principle 8). Bij afwezigheid van gebleken noodzaak kan de wederpartij van de verzoeker niet worden gedwongen "deleted, shadowed, fragmented, or residual stored information" te bewaren of te produceren (Principle 9).

De 14 Principles zelf passen op één A4. Het gehele rapport van de Werkgroep beslaat echter 73 pagina's tekst, waarin per Principle commentaar en verwijzingen worden gegeven.

11 Advisory Committee Notes to Fed. R. Civ. P 26(b)(2).

De Sedona Principles zijn ontstaan uit ervaringen van 'e-discovery'-practici, die zich hebben verenigd in deze denktank. Tegelijkertijd was er een beweging gaande die is uitgemond in de zojuist genoemde, in 2006 gewijzigde, Federal Rules. Deze bewegingen hebben elkaar over en weer beïnvloed, al zijn er ook verschillen,[12] waarover straks meer.

Eerst iets over een zaak die voor een Amerikaanse rechter heeft gespeeld, waarin naar een balans is gezocht tussen voor- en nadelen van 'e-discovery'. Het is de zaak Zubulake v. UBS Warburg.[13] Rechter Shira A. Scheindlin van het US District Court for the Southern District of New York heeft in een aantal uitspraken in deze zaak voor het eerst vijf categorieën elektronische informatie onderscheiden:

(1) 'active, online data', die in de dagelijkse gang van zaken worden gebruikt en gemakkelijk beschikbaar zijn, bijvoorbeeld computer hard drives;

(2) 'near-line data', die zijn opgeslagen op optische of magnetische schijven in een geautomatiseerde bibliotheek en snel toegankelijk zijn met behulp van een robot of op andere geautomatiseerde wijze;

(3) 'offline storage archives', dat wil zeggen optische of magnetische schijven die 'op een plank in het magazijn' liggen en door mensenhand tevoorschijn moeten komen;

(4) 'back-up tapes', die louter een computerstructuur weerspiegelen en niet erop ingericht zijn dat zij zich laten doorzoeken op individuele dossiers, en

(5) 'erased, fragmented or damaged data', die alleen door grote inspanning en met veel kosten kunnen worden teruggehaald.

De rechter heeft alleen de eerste drie categorieën gekwalificeerd als toegankelijk, omdat het daarbij gaat om informatie die op een gemakkelijk te gebruiken format zijn opgeslagen. De twee andere categorieën beoordeelde de rechter als redelijkerwijs niet toegankelijk.

De Sedona Principles maken hetzelfde onderscheid. Dit onderscheid heeft navolging gevonden in de USA, onder andere in de Toelichting op Rule 26 (b)(2), een van de eerder genoemde toevoegingen uit 2006 aan de Federal Rules.

'Discovery' kan ook plaatsvinden in het kader van internationale arbitrage. "If 'discovery' is a dirty word in international arbitration, 'e-discovery' promises to be downright obscene", aldus Robert H. Smit en Tyler B. Robinson, advocaten respectievelijk te New York en Londen in een artikel getiteld "E-disclosure in International Arbitration" in het tijdschrift Arbitration International.[14]

---

12 Verwezen zij naar de Inleiding, pagina 6, punt 4: 'What is the Relationship Between The Sedona Principles and Court Rules?'.

13 Zubulake v. UBS Warburg, 217 FRD 309 (SDNY 2003); Zubulake v. UBS Warburg LLC, 229 FRD 422 (SDNY 2004); Zubulake v. UBS Warburg LLC, 220 FRD 212 (SDNY 2003); Zubulake v. UBS Warburg LLC, 216 FRD 280 (SDNY 2003).

14 Smit & Robinson 2008.

Volume, verspreiding, duurzaamheid, vluchtigheid en dynamiek

Smit en Robinson wijzen erop dat de ongekende mogelijkheden tot het elektronisch ontwerpen, communiceren en opslaan van documenten de betekenis van het woord 'document' hebben gewijzigd, en daarmee het proces van 'document discovery' in de USA en onvermijdelijk ook in internationale arbitrage. Elektronisch opgeslagen documenten, vooral e-mails, zijn in hoog tempo misschien wel de meest belangrijke bron van bewijs in handelsgeschillen geworden, aldus de schrijvers.

Zij zetten de kenmerken voor de overzichtelijkheid op een rij. In de eerste plaats: het volume van elektronische documenten in een rechtsgeding is vaak veel groter dan dat van papieren documenten. Dat is niet alleen omdat deze documenten gemakkelijker aangemaakt worden, vermenigvuldigd worden en verzonden worden dan papier, maar ook omdat mensen tegenwoordig e-mail gebruiken waar vroeger de telefoon werd gebruikt (soms juist om te voorkomen dat een gesprek op papier werd gezet).

Dat is een ervaring die de Nederlandse rechter ook heeft. Waar vroeger gebeurtenissen of uitspraken van personen in getuigenverhoren soms met de grootste moeite aan het licht konden worden gebracht, omdat getuigen zich de gang van zaken niet meer precies konden herinneren of niet meer wisten wat iemand precies gezegd had, doet zich dat probleem tegenwoordig in mindere mate voor, omdat de hele gang van zaken regelmatig vast ligt in overgelegde e-mails, soms met kopie aan velen, al dan niet met allerlei bijlagen. E-mail wordt gemakkelijker verspreid over tal van plekken: de eigen harde schijf, de eigen netwerk server, laptops, blackberries of andere draagbare apparaten en elektronische reserve-opslag en is daar te achterhalen.

Aan deze twee verschillen, te weten meer *volume* en gemakkelijker *verspreiding* kan worden toegevoegd: *duurzaamheid*. Elektronische informatie is veel moeilijker te vernietigen dan papier. Een druk op de 'delete'-knop betekent niet dat de informatie voor de eeuwigheid wordt geschrapt, maar alleen dat deze in de computer ruimte moet maken voor andere informatie. Het is onder omstandigheden mogelijk de geschrapte informatie boven water te krijgen. Er bestaan forensische computerspecialisten die daartoe in staat zijn. Misschien kan dit vergeleken worden met de kunstschilder van een eeuw geleden die geen geld had om een nieuw doek te kopen of ontevreden was met zijn werk en zijn schilderij overschilderde met een andere afbeelding; met behulp van een technische ingreep als röntgenstraling kan de kunsthistorische onderzoeker van nu de oude afbeelding weer tevoorschijn toveren.

Vluchtigheid is een volgend kenmerk. Voortdurend wordt nieuwe computertechnologie geïntroduceerd. Elektronische informatie kan weliswaar voor eeuwig worden opgeslagen, maar de techniek om deze toegankelijk te maken kan verouderen.

Elektronische informatie is ook *dynamischer.* Papier is statisch, het is doorgaans opgeborgen in een dossier. Elektronische informatie echter kan gemakkelijk worden gewijzigd, geactualiseerd, kortom veranderd, soms

zonder menselijke tussenkomst. Samengevat: meer volume, meer verspreiding, grotere duurzaamheid, vluchtigheid en meer dynamiek.

Zo kan men zich met de schrijvers afvragen wanneer er sprake is van het produceren van een document. Is de laatste versie waarin het is opgeslagen voldoende of moeten ook eerdere versies te voorschijn worden gehaald? Soms bevat een document verwijzingen, links, naar andere documenten; moeten die worden gehandhaafd? Mag volstaan worden elektronische informatie te produceren die met de tegenwoordige programmatuur en hardware niet meer kan worden gelezen?

Aan de andere kant: met zoektermen kan sneller worden gezocht. Mag worden geëist dat dit gebeurt? Met behulp van computers kan het zoekproces worden gestroomlijnd en vereenvoudigd; elektronische informatie behoeft niet meer te worden geprint en in verhuisdozen of zelfs vrachtwagens bij de wederpartij te worden bezorgd. Volstaan kan worden met het aanleveren van schijven of USB-sticks (flash drives) met behulp waarvan alleen de interessante documenten worden geprint.

e-Disclosure

Smit en Robinson bepleiten in hun artikel de komst van – nu nog ontbrekende – richtlijnen voor 'e-disclosure' in internationale arbitrage. Arbiters in internationale arbitrage hebben vaak de bevoegdheid documenten of bewijs te eisen. Regels over het bewaren, verzamelen en presenteren van dat bewijs ontbreken nu, zeker wat betreft elektronische informatie. De International Bar Association kent weliswaar "Rules on the Taking of Evidence in International Commercial Arbitration" ('IBA Rules'), maar ook deze bevatten geen speciale regels over het bewaren, verzamelen en de 'disclosure' van elektronische informatie.[15]

De schrijvers doen ook een voorstel voor een aantal (22) richtlijnen op dit gebied. Zij doen dat in het besef dat in internationale arbitrage, waar diverse juridische culturen kunnen samenkomen, de behoefte aan regels op het gebied van 'e-disclosure' niet door iedereen gevoeld zal worden. Het is immers mogelijk dat er mensen zijn die vrezen dat speciale regels over e-documenten alleen maar het onwelkome fenomeen van de 'discovery' in internationale arbitrage vergroten. Van partijen, raadslieden en arbiters uit civil-law-culturen, waar weinig of geen discovery bestaat, kan men niet verwachten dat zij openstaan voor het overnemen van de Federal Rules. Maar dat neemt volgens de schrijvers niet weg dat men niet de ogen kan sluiten voor het aangebroken elektronische tijdperk.

Zij hebben zich daarbij laten inspireren door zowel de in het voorgaande aangeduide '2006-amendments' op de Federal Rules als door de Sedona Principles, maar hebben ook gekeken naar de IBA Rules. Deze laatste gaan vol-

15 www.ibanet.org.

gens de daarbij behorende Preambule uit van de gedachte dat "each Party shall be entitled to know, reasonably in advance of any Evidentiary Hearing, the evidence on which the other Parties rely" en hebben, zo zou men geneigd zijn te denken, dus toch wel iets gemeen met de gedachte achter 'discovery'. Toch zijn zij daarmee niet geheel vergelijkbaar: "There shall be no U.S.-style pre-trial discovery (....) Pre-trial discovery and fishing expeditions by one party against another are out of place in international arbitration", aldus de werkgroep die verantwoordelijk is voor de IBA-Rules.[16]

Het is hier niet de plaats dieper in te gaan op de 22 voorstellen van Smit en Robinson. Volstaan kan worden met de kenschets dat daarin veel uit de Federal Rules en de Sedona Principles terugkomt. Zij concluderen dat de bestaande IBA Rules ruim genoeg lijken te zijn om daaronder elektronische informatie te begrijpen en scheidsgerechten in staat te stellen om op ad hoc basis verstandige resultaten te bereiken. Maar zij achten een speciale regeling van e-disclosure richtlijnen noodzakelijk om voorspelbaarheid, uniformiteit en eerlijkheid te bereiken in internationale arbitrage.

Rond de conferentie van de IBA in 2008 in Argentinië heeft een internetdiscussie plaatsgevonden naar aanleiding van een conferentie waar e-document production aan de orde kwam. Eén ervaren arbitragedeskundige, Martin Hunter, maakte, samengevat aan het slot, de volgende waardevolle opmerkingen:

(i) Er is in beginsel geen verschil tussen het produceren van 'hard copy' documenten en elektronische documenten in internationale arbitrage;

(ii) In beide gevallen moeten de arbiters, als partijen daarover zelf geen afspraken maken, orders ter regeling van de procedure uitvaardigen, waarbij zij zich laten leiden door het beginsel van proportionaliteit. Dat betekent dat zij een afweging moeten maken tussen enerzijds de kosten en moeite die het produceren van documenten meebrengen en anderzijds de vruchten die partijen en de arbiters op grond van die eventuele documenten kunnen plukken ten behoeve van de beslechting van het geschil;

(iii) De beoordeling of in een bepaald geval aan de eisen van proportionaliteit wordt voldaan is aan de arbiters. Gedetailleerde regelingen op dit gebied kunnen alleen maar ten koste gaan van de flexibiliteit en voorspelbaarheid van de arbitrale procedure;

(iv) Met de bestaande IBA-Rules (3.1, 3.2 en 3.3.) kan worden volstaan voor het uitvaardigen van procedurele orders betreffende documenten, zij werken in de praktijk uitstekend;

(v) Het gebruik van termen als e-discovery en e-disclosure werkt niet verhelderend, want zij betekenen niet in elk land hetzelfde.

Deze opmerkingen laten zich van harte onderschrijven.

16 Zie noot 60 in het artikel van Smit en Robinson voor verdere verwijzing.

Aan het voorgaande valt toe te voegen dat het Chartered Institute of Arbitrators een 'Protocol for E-Disclosure in Arbitration' kent. Daarin wordt een evenwicht gezocht tussen kosten en baten op vergelijkbare wijze als in de bovengenoemde regelingen. Daaraan bestaat in de praktijk ook behoefte.

Het valt te hopen dat de arbitrage-practici oog hebben voor de ontwikkelingen en valkuilen die hierboven zijn geschetst.

Verwijzingen

Asser, Groen & Vranken
W.D.H. Asser, H.A. Groen en J.B.M. Vranken (met medewerking van mevrouw mr. Tzankowa), *Uitgebalanceerd: eindrapport fundamentele herbezinning Nederlands burgerlijk procesrecht*, Den Haag: Boom Juridische uitgevers 2006.

Fokker 2009
J.P. Fokker, *E-arbitrage*, proefschrift Leiden (promotores: A.H.J. Schmidt en H.J. Snijders), 2009.

Krzeminsky 2008
K.J. Krzeminski, 'US discovery for use in Dutch civil proceedings', *TCR* 2008/2.

Van den Reek 1997
W.A.J.P. van den Reek, *Mededelingsplichten in het burgerlijk procesrecht*, Tjeenk Willink, 1997.

Smit & Robinson 2008
Robert H. Smit en Tyler B. Robinson, 'E-disclosure in International Arbitration', in: *Arbitration International* 2008(24), no. 1, p. 105.

E-Justice: nieuwe kansen voor onderzoek naar ICT en recht

Ronald van den Hoogen■

Inleiding

In 1996 verscheen de bundel '*10 jaar IT & Recht: verleden, heden en toekomst*' ter gelegenheid van het tienjarig bestaan van de Nederlandse Vereniging voor Informatietechnologie en Recht.[1] Schmidt geeft in zijn bijdrage aan deze bundel, 'Expertsystemen & juridische informatisering' de belangrijkste – en nog altijd relevante – vragen op het gebied van rechtsinformatica en informaticarecht:[2]

1. Hoe kan het recht het maken van bindende afspraken over het verrichten en/of verrekenen van informatie-uitwisseling, -bewerking, -openbaarmaking, -verveelvoudiging, -bescherming en dergelijke ondersteunen?
2. Hoe kan het recht daarbij de vereisten van de rechtsstaat ondersteunen?
3. Hoe kan de techniek deze afspraken/regelingen ten aanzien van informatie-uitwisseling zoveel mogelijk vormgeven in automatiserings(deel) processen (apparatuur en programmatuur)?
4. Hoe kunnen recht en techniek de benodigde berichten en functies zodanig standaardiseren dat samenwerking (interoperabiliteit) en vrije mededinging tussen dienstverleners mogelijk blijft en wordt gestimuleerd?

Ik heb deze vragen altijd bijzonder gevonden, omdat zij uitgaan van *ondersteuning* van de techniek door het recht en van *ondersteuning* van het recht door de techniek. Waar anderen vaak vanuit het recht de risico's van de techniek benadrukten of onderzochten of juist te ver doorschoten in de mogelijke ondersteuning die de techniek kan bieden aan het recht, heeft Schmidt hierin altijd zijn eigen koers gekozen, zoals het een onafhankelijk wetenschapper betaamt. Ik heb het artikel echter vooral gekozen vanwege zijn constatering dat deze vragen ook op internationaal niveau onder ogen moeten worden.

■ Ronald van den Hoogen werkt als programmamanager eRechtsbestel (e-Justice) bij de directie Rechtsbestel van het Ministerie van Justitie. Hij schrijft op persoonlijke titel.

1 NVVIR 1996.

2 Schmidt 1996.

Hij formuleert dat als volgt:

> "In dat licht is misschien nog het meest klemmende het vinden van mogelijkheden om internationale afspraken op uitvoeringsniveau te kunnen maken binnen een aannemelijk tijdsbestek en in een kader van toezicht en controle dat recht doet aan de eisen van de rechtsstaat. Europese informatisering en integratie van administratieve procedures (…) laten zien dat de vragen nog lang niet zijn opgelost."

Het heeft even geduurd, maar de afgelopen jaren is daadwerkelijk een begin gemaakt met Europese informatisering. Dat is gebeurd in het programma *European e-Justice*.[3] Op 15 december 2009 is het eerste resultaat van dit programma zichtbaar geworden bij de opening van het *e-Justice portaal* in Stockholm. Het portaal zal de komende jaren uitgroeien tot hét centrale punt voor informatie-uitwisseling en communicatie tussen justitiële organisaties uit de Europese Unie. De vragen die Schmidt stelt, zijn daarmee echter nog lang niet allemaal beantwoord. Voor onderzoekers op het gebied van de rechtsinformatica en het informaticarecht biedt het e-Justice programma dan ook nieuwe (financiële) bronnen, nieuwe mogelijkheden voor het vinden van praktische toepassingen van onderzoeksresultaten en – vooral – nieuwe inspiratie.

In deze bijdrage schets ik de totstandkoming van dit programma en geef ik de belangrijkste onderdelen waaruit het bestaat.

E-Justice:[4] de start

In 2006 organiseerde Oostenrijk, als voorzitter van de Europese Unie en als voorloper op het gebied van de elektronische overheid, een congres over *e-Law* en *e-Justice* in Wenen. Het bleek de start van een boeiend politiek-bestuurlijk traject dat uiteindelijk heeft geleid tot het e-Justice programma zoals dat thans bestaat en de komende jaren zal blijven bestaan. Duitsland heeft het Oostenrijkse initiatief een jaar later op de Europese politieke agenda geplaatst. Op 12-13 juni 2007 besloot de JBZ-Raad[5] dat op Europees niveau de inzet van informatie- en communicatietechnologie binnen het justitiële domein dient te worden bevorderd.[6] Vijf prioriteiten zijn daarbij nadrukkelijk benoemd:

---

3 Zie voor een uitvoerig dossier over dit onderwerp: http://www.justitie.nl/onderwerpen/internationaal/european-e-justice/.

4 Voor de term '*European e-Justice*' is gekozen om het onderscheid duidelijk te maken voor lidstaten die hun digitaliseringsprojecten op nationaal niveau ook e-Justice noemen. Omdat wij dat in Nederland niet doen, handhaaf ik hier de term *e-Justice*.

5 De JBZ-Raad is de raadsformatie Justitie en Binnenlandse Zaken. Hij bestaat uit de ministers van justitie en/of binnenlandse zaken van de lidstaten van de Europese Unie. De JBZ-Raad vergadert ongeveer zes keer per jaar en heeft daarnaast geregeld informele bijeenkomsten.

6 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/nl/jha/95060.pdf.

- het inrichten van een e-Justice portaal;
- het inzetten van ICT voor de communicatie tussen justitiële autoriteiten, juridische beroepsbeoefenaren en burgers;
- het gebruik van videoconferentie;
- het gebruik van ICT voor bijzonder procedures zoals het Europees betalingsbevel;
- toegang tot nationale registers, zoals insolventieregisters, handelsregisters, kadastrale registers en strafregisters.

De JBZ-Raad heeft de Raadswerkgroep Juridische Informatica een mandaat gegeven om activiteiten te starten in het kader van e-Justice. Nederland participeert thans in een aantal projecten, waaronder de projecten ter verbinding van de insolventieregisters en strafregisters. Ik kom daar later op terug. Portugal en Slovenië spraken met Duitsland af in 2007 en 2008 eveneens prioriteit te geven aan e-Justice. Conferenties volgden in Bremen, Lissabon en Portoroz.

Op 2 juni 2008 besloot de Europese Commissie nadrukkelijk om partij te worden in het e-Justice programma. Niet alleen door financiële middelen ter beschikking te stellen, maar door met een eigen strategie te komen: 'Naar een Europese strategie inzake e-Justice'.[7] De Commissie wilde de leiding over het e-Justice project naar zich toe trekken. Veel lidstaten, waaronder Nederland,[8] protesteerden hiertegen en een impasse dreigde. Frankrijk is er echter als voorzitter van de Europese Unie in de tweede helft van 2008 in geslaagd een compromis te vinden tussen het standpunt van de Commissie en dat van de belangrijkste lidstaten. Het *European e-Justice action plan*[9], dat onder Franse leiding tot stand is gebracht, is nu leidend voor de toekomstige plannen. Voordat ik dat actieplan beschrijf, geef ik de context van het e-Justice programma waarbinnen het werk plaatsvindt: de uitgangspunten, de afbakening en de functies van e-Justice.

E-Justice: context

Een van de doelstelling van het e-Justice programma is het vereenvoudigen van juridische procedures. De Europese Commissie heeft berekend dat ongeveer 10 miljoen personen op dit moment betrokken zijn bij een grensoverschrijdende civiele procedure. Dit aantal zal de komende jaren ongetwijfeld toenemen. Het gebruik van moderne technologie beoogt de administratieve lasten voor burgers, juridische beroepsbeoefenaren en justitiële organisaties te verminderen.

---

7 http://www.justitie.nl/onderwerpen/internationaal/european-e-justice/documenten-european-e-justice/.

8 *Kamerstukken II*, 2007-08, 22 112, nr.673.

9 http://register.consilium.europa.eu/pdf/en/08/st15/st15315.en08.pdf.

Uitgangspunten
Eerste uitgangspunt bij de ontwikkeling van E-Justice is, dat men rekening houdt met het werk dat op Europees niveau al is verricht, met de websites van de Europese instellingen, met het Europees Justitieel Netwerk in burgerlijke en handelszaken en strafzaken en met initiatieven die door de juridische beroepsgroepen al zijn gestart, zoals het Europees testamentenregister.

Een tweede uitgangspunt is dat bij de ontwikkeling van e-Justice rekening wordt gehouden met de ontwikkelingen in de e-government context. Binnen de Europese Commissie is veel werk verricht in het kader van de zorg voor een beveiligde infrastructuur en in de authenticatie van documenten. Het European Interoperability Framework (EIF), dat door het IDABC-programma[10] is ontwikkeld, dient te worden bevorderd. Het Europese werk op het gebied van elektronische handtekeningen en e-Identity wordt zeer belangrijk geacht voor de juridische omgeving waar e-Justice betrekking op heeft.

Een derde uitgangpunt is dat voor het bevorderen van e-Justice een horizontale, rechtsgebiedoverstijgende aanpak nodig is. Zowel in civielrechtelijk, strafrechtelijke en administratiefrechtelijke procedures bestaat de wens om procedures te digitaliseren of door toepassingen van ICT te laten ondersteunen.

Afbakening
Bespreking van het e-Justice programma vindt voornamelijk plaats in de raadswerkgroep e-Justice. Deze werkgroep heeft geen wetgevende bevoegdheid. Dat betekent dat voor de activiteiten op het terrein van e-Justice in beginsel geen (nieuwe) wettelijke aanpassingen vereist zijn.

Lidstaten zijn vanzelfsprekend vrij om eigen projecten op het terrein van e-Justice te starten. Om voor financiering door de Europese Commissie in aanmerking te komen, moeten deze projecten echter een Europese dimensie hebben en betrekking hebben op grensoverschrijdend rechtsverkeer. In elk geval moeten zij de potentie hebben om alle lidstaten van de Europese Unie erbij te betrekken. Projecten die toegevoegde waarde voor de burger hebben, hebben prioriteit.

Functies
E-Justice heeft drie functies: toegang tot informatie op het terrein van justitie, virtualisering en communicatie tussen justitiële autoriteiten. Toegang tot informatie op het terrein van justitie betekent vooral toegang tot Europese wetgeving en jurisprudentie, zoals die op dit moment via EUR-Lex[11] en N-Lex[12] plaatsvindt. Een bijzonder initiatief om jurisprudentie beter te ontsluiten komt uit Nederland. De Raad voor de rechtspraak streeft er naar om,

10 http://ec.europa.eu/idabc.
11 http://eur-lex.europa.eu/nl/index.htm.
12 http://eur-lex.europa.eu/n-lex/.

op vergelijkbare manier als bij het Nederlandse Landelijk Jurisprudentie Nummer (LJN) gebeurd is, een 'European Case Law Identifier' te creëren.[13]

'Virtualisering' of 'dematerialisatie' van procedures omvat elektronische communicatie tussen een rechtbank en procesdeelnemers, maar ook procedures die virtueel verlopen, zonder dat daadwerkelijk een zitting plaatsvindt, bijvoorbeeld via een elektronische mediation.

De functie 'communicatie' heeft tot doel de communicatie tussen justitiele autoriteiten van verschillende lidstaten te verbeteren en te vereenvoudigen. Bijvoorbeeld via het gebruik van videoconferentie of via beveiligde elektronische netwerken.

Het e-Justice portaal is één van de resultaten waar de JBZ-Raad nadrukkelijk om heeft gevraagd. Het vormt ook het eerste en belangrijkste resultaat dat het e-Justice programma heeft opgeleverd. Het portaal dient in de toekomst toegang te verschaffen tot het gehele e-Justice systeem. Bijvoorbeeld tot Europese en nationale rechtsbronnen en diensten. Het zal, door middel van een uniforme identificatie- en authenticatieprocedure, te benaderen zijn door juridische beroepsgroepen op basis van de rechten die zij hebben. Het streven is voor burgers een vergelijkbare identificatie- en authenticatieprocedure in te richten.

Techniek

In het kader van e-Justice is afgesproken dat er geen nieuwe centrale systemen worden gemaakt, maar dat ernaar wordt gestreefd decentrale systemen in te richten die verbonden zijn met bestaande systemen in de lidstaten. Om informatie-uitwisseling en communicatie mogelijk te maken, is het noodzakelijk om de hoogst mogelijke graad van compatibiliteit na te streven tussen de verschillende systemen. Afspraken en standaarden zullen, waar zij nog niet bestaan, dienen te worden ontwikkeld om interoperabiliteit te bewerkstelligen.

Van een goed functionerend e-Justice systeem kan bovendien geen sprake zijn als er geen voorzieningen bestaan voor identificatie en authenticatie. Het zal een van de belangrijkste uitdagingen worden om hier goede voorzieningen voor in te richten. Ook een goede beveiliging van netwerken en gegevens is cruciaal voor het slagen van het programma.

Taal

Het systeem dient toegang te verschaffen tot nationale functionaliteiten door middel van een gebruikersvriendelijke, meertalige interface. De Europese Unie kent 23 officiële talen. Vertaling en interpretatie spelen daarom een zeer belangrijke rol bij de ontwikkeling van het programma. Er wordt daarom (ook) nagedacht over mogelijkheden voor automatische vertalingen.

13 http://www.legalaccess.eu/spip.php?article47.

E-Justice: inhoud[14]

In de inleiding bij dit artikel gaf ik aan dat het e-Justice programma nieuwe kansen biedt voor onderzoekers op het terrein van de rechtsinformatica en het informaticarecht. Daarom beschrijf ik hieronder de inhoud van het programma voor de komende jaren. Ik doe dat in het kader van het e-Justice portaal, omdat dit portaal een centrale rol zal vervullen in het programma.

In de eerste fase (die loopt tot eind 2009) zal het portaal niet veel meer bevatten dan informatie over procedures en links naar andere websites. Toch geeft de beschrijving van de inhoud van dat portaal een goed beeld van waar e-Justice betrekking op heeft. Omdat ik via dit artikel onderzoekers op het terrein van de rechtsinformatica en het informaticarecht wil informeren over de e-Justice thema's die de komende jaren op de agenda staan, wil ik vrij uitvoerig op de afzonderlijke (21) onderwerpen in gaan.

a. Informatie over wetgeving
Dit onderdeel van het portaal bevat informatie over wetgeving van de Europese Unie, nationale wetgeving, links naar internationale organisaties en internationale en nationale jurisprudentie. Discussie over dit onderdeel vindt plaats in de zogenaamde eLaw-werkgroep van de Raad van de Europese Unie.

b. Informatie voor verdachten en slachtoffers in strafzaken
Het portaal bevat *fact sheets* over de rechten die een verdachte en een slachtoffer hebben in een strafzaak en over de compensatie die slachtoffers kunnen ontvangen in alle lidstaten. Veel van deze informatie is al beschikbaar via de website van het EJN-netwerk en de *Judicial Atlas*.[15]

c. Informatie over civielrechtelijke procedures
Op dit onderdeel is algemene informatie over rechtssystemen verzameld, staan de belangrijke beginselen van een civielrechtelijke zaak in alle lidstaten, en staat informatie over de rechterlijke organisatie en over de juridische beroepen. Het bevat ook informatie over de bevoegde rechtbanken en algemene informatie over Europese procedures.

d. Kosten van civielrechtelijke procedures
De Europese Commissie heeft in december 2007 een studie laten verrichten naar de kosten van civielrechtelijke procedures. De resultaten van dat onderzoek zijn op het portaal gepubliceerd, in een gebruikersvriendelijk *format*.

14 Informatie afkomstig van: European Commission, Description of Services/Technical annex, version 0.8, 4 February 2009 (niet openbaar).

15 Zie: http://ec.europe.eu/justice_home/judicialatlascivil/html/index_en.htm.

e. Europese *small claims* procedure
Op 10 juni 2009 is de uitvoeringswet verordening Europese procedure voor geringe vorderingen van kracht geworden.[16] In eerste instantie zal het e-Justice portaal slechts algemene informatie over deze *small claims* procedure bevatten. In 2009 is de Europese Commissie een haalbaarheidsstudie gestart naar een elektronische applicatie voor deze procedure. De verwachting is dat tussen 2009 en 2013 een groep lidstaten samen met de Commissie een *dynamisch formulier* zullen ontwikkelen dat het mogelijk maakt een elektronische applicatie te gebruiken. In Engeland maakt men hier al langere tijd gebruik van bij een elektronische *small claims* procedure (Money Claim Online).[17]

f. Vertaling
Een belangrijk knelpunt bij het grensoverschrijdend verkeer is het taalprobleem. Op het gebied van vertalingen zijn dan ook diverse activiteiten voorzien. Er bestaat een pilot die tot doel heeft databases van juridische tolken en vertalers te verbinden. Eventueel zal deze interconnectie tussen de databases in het e-Justice portaal worden opgenomen. Er zijn ook andere initiatieven: het ontwikkelen van een *legal glossary* dat definities van bepaalde juridische termen bevat, het bevorderen van *semantische operabiliteit* (Semic.eu)[18] en de financiering van software ten behoeve van het geautomatiseerd vertalen.

g. Justice Forum
Sinds 30 mei 2008, wellicht heeft u het gemist, bestaat er een *Justice Forum*. Dit forum bestaat uit deskundigen en betrokkenen uit nationale lidstaten op het terrein van Justitie. Het heeft ook tot doel afstemming en transparantie te bewerkstelligen op het terrein van e-Justice. Het portaal bevat een onderdeel dat ten dienste staat van de samenwerking binnen het Justice Forum.

h. Interconnectie tussen insolventieregisters
Nederland (Raad voor de rechtspraak) neemt deel aan het project van 11 lidstaten dat tot doel heeft de insolventieregisters te verbinden. Een subproject heeft tot doel interface-specificaties te ontwikkelen voor het verbinden van civiele registers in brede zin en deze specificaties te testen op de insolventieregisters. Aanvankelijk was het de bedoeling om de interconnectie te realiseren binnen de eerste versie van het portaal, maar het project is niet in staat gebleken de specificaties tijdig op te leveren.

i. Interconnectie tussen kadastrale registers (EULIS)
Het portaal bevat een link naar het *European Land Information Service* (EULIS), het project van (op dit moment) zes Kadasters binnen de Europese Unie, dat tot doel heeft de kadastrale registers met elkaar te verbinden.[19] Ook het

16 *Staatsblad* 2009, 234. Zie ook: http://www.eerstekamer.nl/behandeling/20090609/publicatie_wet_2/f=/vi6pbflwmdnc.pdf.
17 Zie: https://www.moneyclaim.gov.uk/csmco2/index.jsp.
18 Zie: http://www.semic.eu/semic/view/snav/About_SEMIC.xhtml.
19 Zie: http://www.eulis.org/.

Nederlandse Kadaster doet hier aan mee. Na 2009 kan EULIS eventueel worden geïntegreerd in het e-Justice portaal.

j. Interconnectie tussen handelsregisters (EBR)
Het portaal bevat ook een link naar *European Business Register* (EBR), het project van (op dit moment) 22 landen, ook van buiten de Europese Unie, dat tot doel heeft handelsregisters met elkaar te verbinden. Ook hier is Nederland via de Kamer van Koophandel een partner. Op termijn zal het EBR worden geïntegreerd in het e-Justice portaal, indien hierover goede afspraken kunnen worden gemaakt met het EBR zelf.

k. Europees Betalingsbevelprocedure (EPO)
Op 10 juni 2009 is de Uitvoeringswet verordening Europese betalingsbevelprocedure van kracht geworden.[20] In het portaal zullen, naast een algemene beschrijving van de procedure en een link naar de regelgeving, ook de elektronische formulieren kunnen worden gedownload. Met behulp van de EPO kan een Nederlander die een vordering in een andere lidstaat van de Europese Unie wil innen, met behulp van een standaardformulier bij de rechter in die andere lidstaat om een Europees betalingsbevel verzoeken. Hij heeft daarvoor geen bijstand van een advocaat in die lidstaat nodig.

Op dit moment zijn Duitsland en Oostenrijk met een pilot bezig die tot doel heeft een elektronische variant van de betalingsbevelprocedure in te richten. Naar verwachting zullen applicaties die hieruit voortvloeien tussen 2010 en 2013 in het portaal worden opgenomen.

l. Mediation
In eerste instantie komen er op het portaal slechts links naar en informatie over mediation. Tussen 2010 en 2013 zal naar verwachting de eerste mogelijkheid in het portaal worden opgenomen om door middel van een systeem van online mediation geschillen op te lossen. Het zou aansluiten bij het onderzoek dat de Raden voor rechtsbijstand in Nederland zijn gestart in samenwerking met de Universiteit van Tilburg naar mogelijkheden om via online mediation geschillen over echtscheiding op te lossen.[21]

m. Rechtsbijstand
Ook over rechtsbijstand blijft het in eerste instantie bij algemene informatie en links. Na 2010 start de Europese Commissie een haalbaarheidsstudie die betrekking heeft op het aanvragen en verkrijgen van rechtshulp via het internet. De resultaten ervan zullen op hun bruikbaarheid voor het e-Justice portaal worden getoetst.

n. Videoconferentie
Het e-Justice portaal zal algemene informatie en documenten over videoconferentie bevatten. Ook wordt gepubliceerd welke locaties op dit moment

20 *Staatsblad* 2009, 232.
21 Zie: http://www.rvr.org/nl/subhome_rz/mediation/ON.

geschikt zijn voor het houden van videoconferenties in alle lidstaten. Op termijn is het de bedoeling om een online boekingssysteem in het portaal op te nemen. Nederland is op dit moment partner bij een onderzoek dat wordt uitgevoerd onder leiding van de Universiteit van Surrey (Verenigd Koninkrijk) dat tot doel heeft te onderzoeken aan welke vereisten het tolken via het internet dient te voldoen om bruikbaar te zijn in het strafrecht. Resultaten van dit onderzoek worden in de loop van 2010 verwacht.

De prioriteit die aan videoconferentie wordt gegeven, sluit aan bij initiatieven die in Nederland plaatsvinden om videoconferentie bij alle rechtbanken, alle detentiecentra voor vreemdelingen en de grootste Huizen van bewaring in te voeren.[22]

o. Interconnectie tussen databases van tolken en vertalers

Op dit moment vindt een pilot plaats tussen twee landen die tot doel heeft databases van tolken en vertalers met elkaar te verbinden. Op termijn zal het mogelijk zijn deze database te doorzoeken via het e-Justice portaal.

p. EJN-netwerken

Beide Europese Justitiële Netwerken (strafrecht en burgerlijke en handelszaken) hebben een eigen website.[23] Omdat het e-Justice portaal beoogt een '*one stop shop*' te zijn, valt het niet uit te sluiten dat deze websites op termijn worden geïntegreerd in het portaal. Ook de Justitiële Atlas zal in overeenstemming moeten worden gebracht met het portaal.[24]

q. Europese betekeningsverordening

De Europese Commissie start tussen 2010 en 2011 een haalbaarheidsstudie naar mogelijkheden om de betekening van documenten via elektronische middelen te laten plaatsvinden.

r. Online betaling van procedurele kosten

In 2013 moet het mogelijk zijn om procedurele kosten online te betalen. Ook deze mogelijkheid dient via het portaal te kunnen verlopen.

s. Strafregisters

Op 6 april 2009 is het Europees Kaderbesluit Europees Strafregister Informatiesysteem (ECRIS) van kracht geworden. Dit besluit vormt de basis voor geautomatiseerde uitwisseling van gegevens uit strafregisters. In Nederland is het strafregister het Justitieel Documentatie Systeem dat door de Justitiële Informatiedienst wordt beheerd.[25]

---

22 Zie: http://www.justitie.nl/actueel/persberichten/archief-2008/80317landelijke-invoering-videoconferentie.aspx?cp=34&cs=21205.

23 Zie: http://ec.europa.eu/civiljustice/index_nl.htm.

24 Zie: http://ec.europa.eu/justice_home/judicialatlascivil/html/index_nl.htm.

25 Zie: http://www.justid.nl/producten_en_diensten/jds/.

t. Interconnectie tussen testamentenregisters
België en Frankrijk hebben in een pilot aangetoond dat het mogelijk is testamentenregisters met elkaar te verbinden. Het is mogelijk voor andere lidstaten om bij dit initiatief aan te sluiten. Op termijn kan de mogelijkheid worden geboden om deze gegevens via het e-Justice portaal op te vragen.

u. Juridische opleiding
Het portaal moet kunnen worden gebruikt als instrument bij het organiseren van Europese justitiële opleidingen.

E-Justice: kansen voor onderzoek naar ICT en recht

Uit het bovenstaande overzicht blijkt dat het gebruik van ICT op het justitiële domein de komende jaren veel aandacht krijgt, dat tal van projecten zijn en worden gestart en dat e-Justice behoort tot de prioriteiten binnen de Europese Unie. Ook het Nederlandse kabinet steunt dit initiatief. Minister van Justitie Hirsch Ballin heeft de ambitie uitgesproken dat Nederland ernaar streeft te behoren bij de kopgroep van landen die zich inspannen op het terrein van e-Justice.[26]

Schmidt beweerde in 1996 dat het gebrek aan voortgang in Europese informatisering laat zien dat de relevante vragen voor het informaticarecht en de rechtsinformatica 'nog lang niet zijn opgelost'. Het is daarom misschien wel enigszins teleurstellend te moeten constateren dat de voortgang die de laatste jaren is geboekt in Europese informatisering niet of nauwelijks is te herleiden tot voortgang die is geboekt in het wetenschapsgebied van informaticarecht of rechtsinformatica. Het lijkt er zelfs op dat de kennis binnen de Europese rechtspraktijk van de mogelijkheden van ICT voor het recht de kennis van veel onderzoekers ver te boven gaat. Dat is geen goed nieuws. Vooral niet voor het onderzoeksdomein van de rechtsinformatica, waar Nederland in internationaal opzicht een naam heeft hoog te houden. Onderzoekers op het terrein van de rechtsinformatica zouden, meer nog dan zij nu doen, moeten participeren in het e-Justice programma. Zij kunnen dat zelf doen door aan e-Justice gerelateerde voorstellen in te dienen bij de Europese Commissie. Het Ministerie van Justitie zal deze van harte ondersteunen.

Verwijzingen

NVVIR 1996
10 jaar IT & Recht: verleden, heden en toekomst (Nederlandse Vereniging van Informatietechnologie en Recht), Samsom: Den Haag 1996.

Schmidt 1996
A.H.J. Schmidt, 'Expertsystemen & juridische informatisering', in: *10 jaar IT & Recht: verleden, heden en toekomst* (Nederlandse Vereniging van Informatietechnologie en Recht), Den Haag Samsom: 1996, p. 87-95.

26 *Kamerstukken* II, 2007-08, 23 490, nr. 467, p. 3.

Computers kunnen er niks van!

Wim Voermans■

Persoonlijke frustratie – deel 1: of hoe het begon

Ergens in 1989, het jaar waarin na de val van de Berlijnse muur en de snel ontwikkelende computertechnologie de mogelijkheden van de mens en de wereld een moment lang oneindig en onuitputtelijk leken. In dat jaar vroeg mijn mentor en baas, hoogleraar HB, of ik even tijd voor hem had. Maar natuurlijk. Eenmaal op zijn kamer passeerden verschillende thema's de revue. Het eerste gespreksonderwerp was er een van alle tijden. Mijn tijdelijke dienstverband liep ten einde (nog maar een jaar nadat het werkelijk in ernst was aangevangen) en we moesten zien hoe we dat zouden kunnen verlengen. De facultaire financiële nood was als vanouds hoog, het belang van de wetenschap groot en dat van mij niet minder. Het tweede onderwerp, dat we in verlengde van het eerste aansneden, vormde aangenamer gesprekstof. Waarom niet het nuttige met het nodige paren? Als ik wilde blijven zou het wellicht iets zijn om een proefschrift te schrijven, en misschien konden we iemand – bijvoorbeeld het Ministerie van Justitie – vragen dat onderzoek te financieren. Twee vliegen in één klap. Aanstelling verlengd, want geld en nog een mooi proefschrift op de koop toe. Het was een moordplan.

Dat ik als staats- en bestuursrechtelijk geschoold jurist niets wist van (rechts)informatica (handig met de computer, dat wel) en er ook geen enkele aanleiding of indicatie was om te denken dat een ministerie als dat van Justitie zo'n onderzoek wilde financieren, deerde op dat moment niet. Er was een goed plan en een combinatie van optimistische natuur, geluk en toeval zou de rest moeten doen. Zoals het al zo vaak gedaan had…

Extatische vreugde – deel 1: weidse vergezichten

Ik begin me in te lezen en tegelijkertijd ook direct een plan te schrijven voor dat onderzoek waar een financier misschien in zou willen stappen. Er was nog niet veel geschreven op het terrein van computerondersteuning in het wetgevingsproces. Een Tilburgse bundel – Trias automatica (originele titel!) – waarin een ambtenaar van Justitie had geschreven over het potentieel van computertechnologie voor wetgeving[1] en een stuk van een Amerikaan, ene

---

■ Wim Voermans is hoogleraar staats- en bestuursrecht aan de Universiteit Leiden en rector van de Europese Academie voor Recht en Wetgeving (EALL).

1 Hustinx 1985.

mijnheer Stoyles, die in een stuk met de prikkelende titel 'The Unfulfilled Promise Use of Computers by and for Legislatures'[2] ook wat mogelijke computerzegeningen voor wetgevers op een rij had gezet. Boodschappenlijstjes en mooie titels, veel meer was er niet. Nou ja, er waren wel al wat stukken over artificiële intelligente en het recht waarin – met het oog op mogelijke automatisering – werd getracht onderdelen van het recht in schema's en logische redeneringen te vatten. Als het zou lukken de normen van het recht in logische redeneerstappen en schema's op te schrijven – met behulp van predicatenlogica – zouden computers daarmee kunnen redeneren. Voor iemand met wiskundedyslexie, zoals ik, volstrekt onbegrijpelijk, maar, zoveel begreep ik er dan ook weer wel net van, voor wetgeving ook volstrekt irrelevant. Ik wilde immers geen normen automatisch gaan laten toepassen, ik wilde de wetgever, de wetgevingsjuristen die wetsvoorstellen schrijven, en ambtenaren en politici die zich een weg door het wetgevingsproces moeten zien te banen, helpen bij hun werk. En dat is niet het zelfde als het mechanisch toepassen van normen.

En toen werd die baas van me ineens minister en vertrok van de faculteit. Wel had hij er, wijzend op het fraaie plan en de financiering die we er mogelijk voor zouden kunnen krijgen, de faculteitsdirecteur een paar maanden eerder er nog van kunnen overtuigen mijn aanstelling voor een jaar te verlengen. Die had er dan maar node 'ja' gezegd omdat hij toch voortaan liever een concrete financiële onderbouwing voor een aanstelling zag, in plaats van een min of meer onrijp plan op termijn. Enfin, vort dan maar, nog een jaar. Maar wat dan? Zo zonder de grote HB in de buurt, tegen wie je eigenlijk geen neen zeggen kan, leken de kansen op vervolg van mijn tijdelijke aanstelling dat jaar daarop – 1990-1991 – wel erg minimaal. Zeker ook nu eerste verkenningen bij het departement van Justitie al hadden geleerd dat er minder dan lauwe belangstelling bestond voor het hele idee van computerondersteuning bij wetgeving. Het hielp ook al niet dat er niet met desktop-computers werd gewerkt op dat departement en dat degenen die het in dat departement voor het vertellen hadden een zekere huiver aan de dag legden voor dat nieuwe instrument. Directeuren, plaatsvervangend directeuren, directeuren-generaal en de secretaris-generaal – allemaal mannen – waren grootgetrokken in een context van typekamers, met talloze typisten, secretaresses die dictaat namen en dure mooie Mont Blanc-pennen waarmee, in een veelvoud van verschillende de auteur kenmerkende kleuren, brieven, memo's en nota's werden becommentarieerd en geparafeerd. Computers over de vloer zouden wel eens kunnen betekenen dat die knusse, arbeidsintensieve bureausituatie ingeruild zou gaan worden voor een ontsierende televisie op een schoenendoos met een tikbord voor je neus. En dat je dan zelf je brieven en stukken zou moeten tikken. Als was je een commies derde klas. Een horreur, een schande![3]

2 Stoyles 1989.

3 Zie over de angst voor het verlies van de tikkamer het stukje "*Olivetti M24*" op http://www.wimvoermans.nl/pdf%20documenten/De%20Olivetti%20M24.pdf .

De mensen in de automatiseringsafdelingen van departementen – van wie ik er ook een paar sprak in het kader van verkennende interviews – waren er ook niet blij mee. Die afdelingen werden toentertijd bevolkt door hardwerkende mainframe-stofjassendragers, mannen (ook hie) in de weer met ponskaarten en magnetische slappe schijven van 25 bij 25 centimeter. Die zagen helemaal niks in de micromatisering van hun nering. Hun baan zou daarmee onmiddellijk op de tocht komen te staan. En diegenen die wel openstonden voor het gebruik van wat het front van wetenschap en technologie konden bieden, waren na hele korte tijd al cynisch en somber over de kansen van kleine en decentrale computertechnologie voor het werk van departementen. Ook zij waren opgelopen tegen de taaie, hiërarchische-tik-papier-dictaatcultuur, die zo kenmerkend was voor de bureaus van de departementen. Een jonge vent, die ik sprak in 1993 bij Justitie en die gelijk nadat ik was gaan zitten maar vertelde dat hij twee weken later bij een grote automatiseerder zou gaan werken omdat hij het niet meer bij het departement trok. Die vermoeide jonge vent vertelde me een ervaring die ik later nog een keer terugzag op televisie.

Het was hem dan op een gegeven moment eindelijk gelukt desktop-computers op een afdeling in het departement te introduceren. Vraag niet hoe. Vooral de jongere medewerkers waren er erg verguld mee geweest. Nadat alles was geïnstalleerd klinkt ineens op maandagmiddag uit de kamer van de directeur gevloek en getier. Enkele ambtenaren van de afdeling en iemand van de automatiseringsdienst die nog in de buurt rondloopt gaan een kijkje nemen.

'Ik zei toch dat die dingen niet werkten!' briest de directeur als het gezelschap binnen is,

'Pure geld- en tijdverspilling!'

De jongen van de automatisering moet zijn gezicht in de plooi houden om niet in lachen uit te barsten. In zijn keurige pak zit de directeur met zijn rechterhand – daarin de muis – met grote cirkelbewegingen door de lucht te zwaaien in een poging om de cursor op het beeldscherm in beweging te krijgen.[4]

Tja, bepaald niet een automatiseringsvriendelijke omgeving, het Ministerie van Justitie begin jaren negentig.

Maar niet geschoten is altijd mis. Ik maakte in de aanloop naar de lange zomer van 1990 een onderzoeksvoorstel met eigenlijk niet meer inhoud dan de vraag: 'Kunnen computers bijdragen aan het proces van totstandkoming van wetgeving?' En niet meer aanleiding om over die vraag na te denken

4 Lange tijd gold dit verhaal als apocrief en werd het zelfs als een beetje ongeloofwaardig beschouwd door mijn omgeving, totdat toenmalig premier Kok ook een keer zo'n zelfde bedieningsfout maakte in februari 1998. Tijdens een tv-uitzending pakte hij een computermuis op en richtte die als een afstandsbediening naar het scherm. Dat was op dat moment al iets wat getuigde van een zekere wereldvreemdheid, zozeer was de situatie in zes jaar veranderd. Zie http://www.refdag.nl/artikel/3776/Computermuis.html over de anekdote van Kok.

dan dat de computertechnologie zo was voortgeschreden en dat experts (twee) het er op hielden dat er van alles mogelijk zou kunnen zijn.

Ik schrok er werkelijk van toen het bericht kwam dat het Ministerie van Justitie geïnteresseerd was en voor een jaar een nader onderzoek naar die mogelijkheden wilde financieren. Dat was niet het directe gevolg van een vermoede Brabantse maffia die – in louter het gevolg van de uit Tilburg afkomstige Minister – de burelen van het Ministerie van Justitie bestormde, maar louter van een verandering in het beleid. In 1990 zette Nederland een hele andere koers in met het wetgevingsbeleid. Jaren van lichtvaardig gebruik van wetgeving om allerhande doelen na te streven hadden de kwaliteit van wetgeving – met name op het terrein van de handhaafbaarheid en uitvoerbaarheid ervan – ernstig aangetast.

Nieuwe uitgangspunten, interdepartementale afspraken en manieren om de kwaliteit te controleren en te borgen werden gemaakt. Een van de problemen van dat nieuwe wetgevingsbeleid was dat het nieuw was (en omvangrijk). En, had iemand zitten denken, dan is het misschien een goed idee om dat beleid uit te zetten bij de verschillende departementen met gebruik van computertechnologie. Weer mogelijke twee vliegen in een klap. In de verpakking van een personal computer wordt dat beleid misschien ook aantrekkelijker en verteerbaarder voor de departementen en – aan de andere kant – zijn die computers een ideale manier om grote hoeveelheden nieuwe informatie op een betrekkelijk uniforme manier bij de bedoelde gebruikers te krijgen. Ik was er blij mee. Ik kon weer een jaar vooruit. De faculteitssecretaris keek me verbluft aan toen ik mijn tweede verlenging op rij bij hem op kwam halen. Of ik wel wist dat het de volgende keer niet zo eenvoudig zou gaan worden, want dan kon hij geen jaarcontract meer bieden. Tenminste als hij dat deed dan zou de volgende stap een vaste aanstelling worden, en daar waren geen mogelijkheden voor. In dat soort gevallen werd een laatste tijdelijke verlening alleen voor een vierjarencontract toegestaan. Ja, hij had het ook niet zelf verzonnen. Met een tevreden gevoel van effectief verwachtingenmanagement stuurde hij me van zijn kamer. Enfin, een jaar nog en dan zou alles weer in de normale plooi vallen… Je zag het hem denken.

Persoonlijke frustratie – deel 2: technology pull en dromers

Er was nog een hele som geld mee gemoeid met dat onderzoek voor Justitie. De universiteit verdiende er goed aan, al werd van de winst die op mijn aanstelling werd gemaakt niets gereserveerd om een eventuele vervolgaanstelling te financieren. En ik moest ook colleges geven. Niet zo'n beetje. Volle bak, zes werkcolleges staats- en bestuursrecht in twee semesters. Dat was niet hardvochtig – derdegeldstroomonderzoek was bijna onbekend binnen juridische faculteiten in die tijd – het was gewoon niet anders. Ik sliep er af en toe wel slecht van, want ik had geen idee waar ik met dat onderzoek moest beginnen en omdat er een contract was gesloten tussen universiteit en departement was mislukking geen optie.

Er kwam in die jaren wel veel meer onderzoeksmateriaal beschikbaar waarover ik kon beschikken. Veel daarvan kwam uit Leiden. Ik verdiepte me in het werk van Aernout Schmidt (Pallas ex machina – een paar jaar eerder verdedigd in Leiden), en het was het jaar van Jaap van den Herik's oratie 'Kunnen computers rechtspreken?' Mooie boeken, goed voor de discussie, maar ze hielpen me niet echt vooruit. Dat deed wel een artikel van ene mijnheer Mercatali – een onderzoeker uit een mij volslagen onbekend instituut in Florence (IDG) – waar ik toevallig tegen aan liep. Het was in het Italiaans, maar met het beetje Latijn dat nog was blijven hangen van de middelbare school kon ik het, met liniaal en woordenboek erbij, lezen. In Florence waren ze dus ook bezig een wetgevingsontwerpsysteem te bouwen. Bingo! Zoiets moest ik dus ook gaan doen. Ik besloot er eerst maar eens een artikel over te schrijven.

Ondertussen raakte ik ook in gesprek met Nederlandse rechtsinformatici. Vaak heel constructief, maar soms ook moeizaam. De rechtsinformaticagemeenschap van begin jaren negentig was een bonte stoet. Heel veel verschillende disciplines – rechtstheoretici, informaticamensen, AI-geleerden, gewone juristen, bestuurlijk informatiekundigen, noem maar op. Ze kwamen samen in het jonge Jurix, waar een gezellige en wetenschappelijk groeizame sfeer heerste. Er was echter wel altijd het probleem van de toren van Babel. We spraken elkaars taal niet. Wederom een anekdote. Ik raakte in gesprek met een groep Nederlandse onderzoekers die ook onderzoek deden naar de mogelijkheden van computerondersteuning van het wetgevingsproces. Mensen met een informatica-achtergrond. Ze beklaagden zich luid over de verschillende departementen en waren verbaasd dat ik een onderzoeksbeurs had gekregen. Dat hadden zij ook geprobeerd en het was niet gelukt. Wat ik dan voor dat departement deed. Ik legde het uit. De hoogleraar-onderzoeker fronste diep en dieper. Maar...,maar,… maar zo kon je dat toch niet aanpakken!? Het ging er om dat het wetgevingsproces en wetgeving beter gemaakt moesten worden en daarvoor waren een AI-aanpak en AI-technieken het vehikel bij uitstek. En als je dat deed dan kon je zien dat wetgeving logisch inconsistent was. Dat hadden zij bewezen. Daarom moest het roer om in het wetgevingsproces en bij het maken van wetgeving. Logische inconsistenties moesten worden opgespoord en aangepakt. Dat kon met AI en dan was zulke wetgeving ook veel eenvoudiger geautomatiseerd uit te voeren. Mijn onderzoek moest echt anders, want zo was het toch weinig wetenschappelijk. En hopeloos. Zag ik dat dan niet dat proces niet deugde?....Brrrr.

Ik bleef er langere tijd een vage buikpijn van houden. Zat ik er nu zo naast? Een paar weken later zag ik een van zijn medewerkers nog een keer en vroeg:

> 'Maar hoe erg is het nu eenmaal dat wetgeving niet logisch consistent is volgens de regelen van de predicatenlogica. Als het voor een normaal mens een beetje te volgen is, en niet gewoon inconsistent, dan is het toch goed.'

Het kwam me te staan op een paar rollende ogen die duidelijk maakten dat ik er echt hé-le-maal niets van had begrepen. Enfin, later hebben we er op de vele verschillende plekken in de wereld waarlangs de rechtsinformatica voert nog vaak over gepraat, altijd vriendschappelijk en open, en we hebben ieder van ieders kant nog best wat geleerd onderweg.

Ik kan me van 1991 niet herinneren dat ik de grond heb geraakt of wanneer ik heb geslapen. Het was aanpoten. September 1991 lag er een rapport met daarin een inventarisatie van de mogelijkheden tot computerondersteuning en een voorstel – schets – voor het bouwen een wetgevingsontwerp en –adviessysteem (LEDA). Het viel in goede aarde en vanaf 1992 mochten we het gaan ontwikkelen. Wederom wilde het ministerie er wel subsidie voor geven en wederom keek de Tilburgse faculteitsdirecteur of hij water zag branden. 'Weer?.....' Nee,toch?

Het LEDA-project voerden we uit in een interdisciplinair samengesteld team. Egon Verharen was bedreven in AI- en hypertexttechnieken (iets heel nieuws in die tijd), Luuk Matthijssen een kei in bestuurlijke informatiekunde, Martin Fridael was een voortreffelijke programmeur die ook als een van de eersten het internet (toen nog met stuurprogramma Mosaic) op ging. Een geweldige tijd was het waarin we bouwden, experimenteerden en deelonderzoekjes lieten doen. Op een gegeven moment waren we met zijn twaalven bezig. Albert Koers hield ons letterlijk op koers met zijn inzicht in methoden van systeemontwerp. Eigenlijk de enige jurist op dat moment die zag en wist hoe belangrijk activiteiten- en informatieanalyse en systeemspecificaties waren alvorens je gaat bouwen. De meeste anderen van ons leden in die tijd aan ernstige 'technopull' (de techniek is er dus *moet* die worden gebruikt in processen die wij kennen).

In 1994 konden we met gepaste trots het eindresultaat presenteren: LEDA. Een in de praktijk functionerend ontwerp- en adviessysteem voor de wetgeving dat – met als ruggengraat de Aanwijzingen voor de regelgeving – wetgevingsjuristen kon helpen bij het systematische ontwerpen van een wettekst. LEDA kon ook controleren of een eenmaal gemaakte tekst voldeed aan die Aanwijzingen. Voor de grote finale waren we besteld om het systeem in een van de pronkzalen van Justitie te presenteren. De zaal zat helemaal vol die ochtend in mei op het Ministerie van Justitie. Directeuren en directeuren-generaal waren uitgelopen om het te komen zien. Iedereen zal klaar. Het enige punt was dat Martin Fridael – onze operator – zich had verslapen. Hij belde bij het begin van de bijeenkomst op dat hij er aan kwam. En toen wij – de rest van het team – de zaak probeerden op te starten, kreeg de zaal na veel gerommel en uitloop op het grote blauwe scherm te zien 'Unable to find link 2332#' Hilarisch, maar ik dacht dat ik doodging. Sneller dan verwacht toch arriveerde Martin. Na een uitbrander van mijn kant waar hij zich toch meestal niks van aantrok, tikte hij zijn brilletje recht op zijn neus. Trok wat stekkers los en laadde wat extra bestanden. Degenen die waren achtergebleven (toch nog de meesten) kregen waar voor hun geld. Een goede show van datgene wat computertechnologie vermag bij het ondersteunen van wetgeving. Die avond versliep ik mij: ik sliep zestien uur aan een stuk.

Persoonlijke frustratie – deel 3: de onvervulde belofte

Dat was 15 jaar geleden. Ik promoveerde op het onderwerp en in de praktijk werd een groep 'innovators' en 'early adopters' bereid gevonden LEDA-praktijk te testen en gebruiksklaar te maken. Dat bleek nog lastiger dan gedacht omdat in de jaren de besturingsplatformen steeds wijzigden. LEDA was nog ontwikkeld onder een 1993-versie van Windows en departementen kenden nog nauwelijks netwerken. Verder was er een eigen databasemanager gebouwd voor het systeem dat zich niet goed verstond met andere – nieuwere – databasesystemen. De leden van de projectgroep gingen ieder hun weg. Er is nog doorgewerkt aan LEDA door het departement tot ver in de jaren negentig, maar uiteindelijk bleef er slechts een uitgeklede publieksversie over die eigenlijk alleen fungeert als een beetje een aangeklede databank voor de Aanwijzingen voor de regelgeving.

Zijn tijd te ver vooruit? Te weinig oog gehad voor de IT-omgeving van het departement (de departementen) ten tijde van de ontwikkeling? De toch steeds weerbarstige – voor ons soms ongrijpbare – bureaucultuur van Justitie? Van verschillende departementen? Wie zal het zeggen. Nou moet ik niet gaan somberen, want het wetgevingsproces en degenen die wetgeving maken hebben veel nut en rendement gehaald uit de – inmiddels geheten – informatietechnologie. Er kwamen computers, grote wetgevingsdatabanken, emailverkeer, (voorzichtige) elektronische bekendmaking van wetten en officiële stukken, noem maar op.[5] Maar dat waren en zijn steeds generieke technieken die ook heilzaam waren voor het wetgevingsbedrijf. Het zijn gedeeltelijk ook 'domme' technieken. Er zijn eigenlijk nog steeds geen IT-systemen waarmee gericht de problemen van wetgeving worden aangepakt, zoals te veel wetgeving, het onberaden en lichtvaardige gebruik van wetgeving, de administratieve lasten die ze voortbrengt, de notoire intransparantie van ons wetgevingsproces en de onzichtbaarheid van de status of fase waarin een wetsvoorstel zich bevindt, (terminologische) tegenstrijdigheden tussen verschillenden wettelijke regelingen onderling, problemen bij het accuraat voorspellen of inschatten van de uitvoerbaarheid en handhaafbaarheid van een regeling, de onleesbaarheid van wijzigingswetgeving, vergeten processtappen, fouten in de techniek, etc.

Het gekke is dat niet alleen in Nederland de pogingen tot het doelgericht ondersteunen van wetgevingsontwerphandelingen met behulp van IT-systemen grotendeels zijn gestrand. Datzelfde lot lijkt ook andere ontwerpondersteunende systemen zoals het Belgische Solon,[6] het Italiaanse Lexedit[7] en het Tasmaans, Australische Enact[8] te zijn beschoren.

---

5 Zie voor een heel volledig overzicht Groothuis 2005 en 2008.
6 Zie Kuyck, DeBaene & Van Buggenhout 1998.
7 Biagoli & Mercatali 1995.
8 Arnold-Moore 1998.

Computers kunnen er niks van, dat zou een terecht commentaar zijn als je naar de povere opbrengst van 20 jaar legimatica – de tak van informatica die zich bezighoudt met het ondersteunen van het ontwerpen van regelgeving – kijkt.[9]

Extatische vreugde deel 2 – gewoon door blijven gaan

Wetgeven is mensenwerk en het gekke is dat (rechts)informatica dat eigenlijk ook is. Dat betekent dat toeval, karakters, netwerken en culturen een grote rol spelen. Het waar en hoe de paden van informatica en werkprocessen – zoals dat van wetgeving – elkaar kruisen, valt maar tot op zekere hoogte te voorspellen. Ik heb in deze bijdrage kronkelpaden, toevalstreffers en culturen in beeld proberen te brengen, want die worden vaak vergeten als factoren in de rechtsinformatica-literatuur. Daar lijkt het er soms op dat de mogelijkheden van de techniek logisch dwingend bepaalde oplossingen dicteren of bepaalde problemen aan het licht brengen. Het is mijn stellige overtuiging dat techniek dat vermogen niet heeft, alleen de mensen die met die techniek in aanraking komen en die op de een of andere manier inzetten voor bepaalde belangen, dan wel zich er – in enigerlei mate – tegen verzetten. Leert het stuk verder nog iets? Ik weet het niet, dat moet de lezer van dit informaticanarratief maar zelf bepalen. Ik leerde ervan dat wetenschap een mooi vak is, dat weliswaar met het hoofd moet worden bedreven, maar niet zonder hart en ziel kan. Wetenschappelijke vooruitgang drijft niet op de aantrekkingskracht van methoden en technieken maar op de zucht om te weten en lol in het snuffelen. Technieken en methoden zijn heel belangrijk, maar ze zijn een middel tot een doel, niet het doel zelf.

En dat toeval – alhoewel het misschien niet eens bestaat – toch regeert. Dat leerde ik ook, al wist is dat eigenlijk al wel van schoolmeester Stephane Mallarmé: 'Un coup de dés jamais n'abolira le hasard,' dichtte hij en hij had gelijk.

Maar de belangrijkste les die ik leerde was er een met een hoog wandtegeltjeswijsheidsgehalte: 'De aanhouder wint'. Dit jaar – 2009 – startte de regering een omvangrijk programma, geheten 'Legis' dat als doel heeft het verbeteren van de kwaliteit van wetgeving en het wetgevingsproces. Daarbij is het plan om met een nieuwe, IT-gebaseerde architectuur van het wetgevingsproces de effectiviteit en de uitvoerbaarheid van wetgeving te verbeteren, de administratieve lasten te verminderen, de transparantie van wetgeving en het wetgevingsproces voor iedereen te verhogen en zo ook de mogelijkheden voor participatie in het wetgevingsproces te vergroten. Door de herinrichting het wetgevingsproces efficiënter te maken en een 'level playing field' voor democratische basisinformatie van de overheid te creeëren. Zie http://www.justitie.nl/onderwerpen/wetgeving/legis/achtergronden-legis/. Zo zie je maar.

9 Zie een eerdere inschatting in Voermans 2000.

Verwijzingen

Arnold-Moore 1998
T. Arnold-Moore, *Information Systems for Legislation*, PhD-thesis, Royal Melbourne Institute of Technology, Melbourne 1998.

Biagoli & Mercatali 1995
C. Biagoli, P. Mercatali, Strumenti automatici per redattori di testi legislativi EXEDIT2 in Ambiente di normazione, *Communicazione dal V Congresso internazionale "Informatica e attivita guridica"*, organizzato dalla Corte di Cassazione, Roma, 3-7 maggio 1993 en Carlo Biagioli, Pietro Mercatali, Giovanni Sartor, *Legimatica dal drafting al processo di produzione legislativa*, Carlo Biagioli, Pietro Mercatali, Giovanni Sartor (eds.), Legimatica, informatica per legiferare, Napoli 1995.

Groothuis 2005
M.M. Groothuis, Digitalisering en wetgeving, in: L. Loeber (red.), *Wetgeving en ICT toepassingen*, preadviezen voor de Vereniging voor wetgeving en wetgevingsbeleid 2005, p. 9-54.

Groothuis 2008
M.M. Groothuis, Wetgeving en ICT; over de rol van de wetgever, het bestuur en de burgers, *RegelMaat* 2008/6, p. 219-229.

Hustinx 1985
P.J. Hustinx, Aspecten van wetgeving m verband met automatisering, E.M.H. Hirsch Ballin en J A Kamphuis (red.), *Trias Automatica*, Deventer 1985, pp. 41 e.v.

Kuyck, DeBaene & Van Buggenhout 1998
R. van Kuyck, S. DeBaene en B. van Buggenhout, Solon – A computer aided statutory drafting system for the Flemish government, *Conference Proceedings of the Fifth International Conference on The Law in the Information Society*, Istituto per la documentazione giuridica dell CNR, Florence 1998.

Stoyles 1989
Robert L. Stoyles, 'The Unfullfilled Promise Use of Computers by and for Legislatures', *Computer Law Journal*, 1989, Vol. IX, no l, p 73-103.

Voermans 2000
W. Voermans, Ontwerpen van wetgeving met computers: een 'eeuwige belofte?' in: Debaene, S.; Buggenhout, B. van (ed.) *Informatietechnologie en de kwaliteit van wetgeving*. Antwerpen-Groningen: Intersentia, 2000, pp. 121-137.

DEEL V

PRIVACY

Assessing investments mitigating privacy risks

John Borking■

Introduction

Risk control plays an important role in privacy protection. Article 17 (1) of the Directive 95/46/EC (Data Processing Directive, further abbreviated as DPD) requires that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The Directive states that "(…) such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."[1]

According to Article 23 of the DPD a person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the DPD is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event causing the damage.

The term risk is not defined in the DPD. The term risk is frequently used as if it is a univocal term for everyone. Closer consideration proves this is not necessarily the case. Gratt, President of the American society of Risk Analysis (SRA) concluded after a two-years research project, that "a consensus was not being reached for the key definitions of risk and risk analysis".[2]

There are many definitions of risk. Miletti defines risk as "the probability or an event or condition occurring"[3] and Hewitt as "exposure to dangers, adverse or undesirable prospect, and conditions that contribute to danger".[4] Tettero defines as a risk: "a probability that, due to a particular threat, a particular vulnerability is exploited causing damage to an asset".[5]

In this article, the following definition of risk will be used: Risk = consequence * probability = (consequences_of_threat) * (likelihood_of _occurrence).[6]

■ John Borking is director of Borking Consultancy.

1 Directive 95/46/EC, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

2 Muller 2004.

3 Mileti 1999.

4 Hewitt1997.

5 Tettero 2000.

6 Van Blarkom, Borking & Olk 2003. The asterix stands for multiplication.

A privacy threat analysis or a privacy impact analysis must be carried out examining the risks and documenting the results, before designing an information system that will be capable to protect personal data adequately against loss or against any form of unlawful processing.[7]

Schneier writes that "Threat Modeling is the first step in any security solution. It's a way to start making sense of the vulnerability landscape. What are the real threats against the system? If you don't know that, how do you know what kind of countermeasures to employ?"[8]

The privacy risk analysis

There are many ways of determining privacy risks. The general approach for privacy risk analysis and subsequent requirements determination is derived from a comparable domain: the risk assessment for information security in British Standards 7799, the Code of Practice for the Risk Analysis and Management Method, Information Security Handbook of the Central Computers and Telecommunications Agency (CCTA).[9] In privacy threat analysis the focus will be primarly on threat identification and assessment of severity of consequences of such threats from five different perspectives:

- Privacy legislation, as defined in a certain country or country union: these regulations inherently list a number of privacy threats occurring if these regulations are not adhered to;
- Purpose of the system, which creates its own threats: because the user (private person) wants to achieve something, that person creates privacy threats;
- Solution adopted, which may or may not create threats on its own;
- Technology used: because of the way a certain system is implemented, certain threats may emanate from it which are not necessarily consequences of the intended purpose. Meanwhile, the technology will harbour some of the privacy enhancement measures;
- Situation in which the ultimate system will be used, which, although not necessarily creating threats of its own, may or may not aggravate (or alleviate) previously identified threats and hence may incur more demanding technological measures. This part is especially needed when a commercial off the shelf (COTS) product is going to be used in an unforeseen situation; the previous four types can be followed whether or not the system is a COTS or dedicated to a certain problem and environment.

7 Flaherty 2000.
8 Schneier 2000.
9 Borking 2003.

See figure 1.

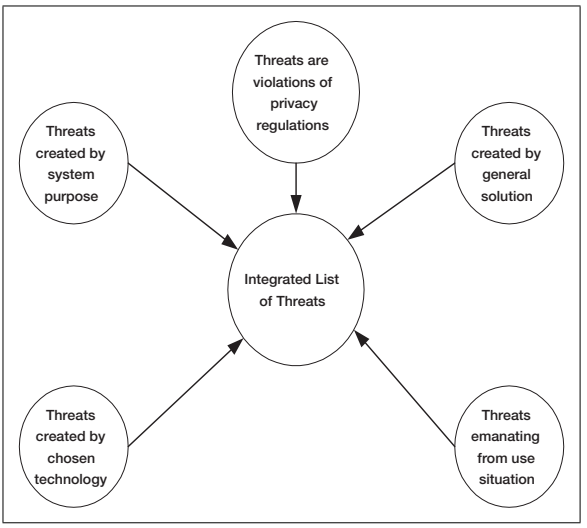


Figure 1. Five-pronged approach to Privacy Threat Analysis[10]

Derived from the privacy principles and Directive 95/46/EC (DPD) the following risks or threats can be discerned:

– Secret possession of (control over) personal data files: the data subject and the authorities are unaware of the existence of the personal data and the degree of control the controller of these data has;

– Secret processing of personal data: processing out of sight of the data subject;

– Out of bounds processing by controller: processing of personal data that is not within the bounds stipulated in the personal data constraints or can be expected to be outside the scope and intention of the collection;

– Out of law processing: processing of personal data that is illegal, forbidden by national law (or is not explicitly allowed if it can be expected to be of dubious nature);

– Personal data deterioration: personal data are in contradiction with the current situation, either caused by external changes or by incorrect or incomplete insertion, collection or insertion;

– Irresponsiveness to discontent: the controller does not respond, or incorrectly, incompletely or unduly late, to requests for correction or other implications to the personal data or the personal data constraints of a

10 Van Blarkom, Borking & Olk 2003.

data subject; the controller thwarts communication; also: there is no authority with reprehension, correction, sanction or other influence on the controller to sustain the data subject's legal rights;

– Out of bounds processing by processor: the processor does not follow the personal data constraints as provided by the controller or violates the rules;

– Out of jurisdiction processing: the personal data are transferred to a controller which has no legal obligation to obey the personal data constraints or where legal obligations about privacy are less stringent than in the data subject's privacy regime;

– Personal data and personal data constraints violation: the controller and processor disobey the obligation to follow the personal data constraints concerning disclosure, retention, termination and safeguarding of correctness, including the obligation to take precautions against loss or mutilation of the personal data or the personal data constraints.[11]

Traditional security measures do not suffice

The requirements referred to in the DPD must be implemented efficiently in the organization in order to give proper support to the citizen's right to privacy with respect to personal data. It is therefore important to devise a proper system of general processing measures and procedures that should be present in order to protect company processes and in connection with specific protective measures for the processing of personal data. The restrictions that the organization of information systems can impose on the possibility that their users can comply with privacy legislation are evident. One simple example is where a system contains an inescapable 'date of birth' field, while analysis of the company's processes shows that recording the birth date of all persons included in the system is excessive. System design can just as easily ensure that users correctly observe the law. As a rule, privacy protection will constitute a supplementary system of measures and procedures in addition to the usual processing and security measures, but it should be assigned a significant place in management processes in order to implement and maintain a balanced processing policy for personal data.

When an organization is asked what it has done to protect privacy, it is apt to emphasize the personal data security measures it has in place. Although the use of safeguards to prevent unauthorized access to personal data is an important aspect of privacy protection, it is not sufficient in its own right. This is because such safeguards rarely involve the encryption of

11 Van Blarkom, Borking & Olk 2003.

stored data; consequently, effective protection depends entirely on the security measures being correctly implemented and functioning properly.

It is therefore preferable to take technical measures that protect the individual's privacy at the point of data collection. Such measures may do away with the need to generate or record any personal data at all. Alternatively, they may minimize or even obviate the need to use or store identification data.[12]

Given the basic legal requirements for privacy protection and the risks of privacy incidents, it will be apparent that, if technical provisions are to be deemed adequate, they must go beyond the implementation of traditional security measures.

Privacy-enhancing technologies (PET)

ICT offers solutions in the shape of privacy protection for users, consumers and citizens. The application of ICT to protect privacy has become widely known under the name Privacy-Enhancing Technologies (PET or PETs).[13] PETs have been defined as a coherent system of ICT measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system.[14]

PETs can guarantee data protection without imposing excessive demands on the processing of the data. By applying PETs and streamlining personal data processing, the organizations can continue to meet high public expectations with respect to services and dealing with personal data.[15]

The basic driver to invest in PETs is their potential to avoid privacy incidents and so to reduce the risks and subsequently the damage caused by privacy breaches. In general terms a privacy incident can be defined as an event in which personal data are misused, because of the fact that personal data accompanied by a list with personal data constraints have not been respected.

Privacy breaches may impact an organization in different ways. Tsiakis and Stephanides distinguish direct, short-term, and long-term economic consequences.[16] Direct consequences are the costs for repairing or changing systems, costs of stopping or slowing down production or processes, and costs of legal action. Short term consequences comprise the loss of existing customers, contractual relations, and the loss of reputation. Companies may lose business because of privacy breaches, which harm their trust relationships with customers and other business relations. Safeguarding privacy has

12 Borking 2001.
13 Hes & Borking 1998.
14 Borking 1996.
15 Koorn et al. 2004.
16 Tsiakis & Stephanides 2005.

been identified as a major component of building trust.[17] Long term consequences include the loss of stock value and market value. An example of the latter is DoubleClick in 2000. After a serious violation of their existing privacy statement on their website and the lawsuit that was the result of this violation, their stock declined with 20%.[18] This also occurred with Choicepoint after their public announcement that they were hacked, and approximately 10 million data records were stolen. Their stock declined with 17% after the data breach.[19]

Business case for PET investments

Investments in (risk reducing) PETs require insight into costs, and quantitative and qualitative benefits. It is essential for the decision-making process concerning the investment in PETs.[20] The decision to spend money on privacy in any direction has to be financially justified. There is no point in implementing an expensive solution if a less expensive solution would offer the same risk reduction and better privacy protection. Beyond legal compliance, it makes no sense to invest in a solution if its true costs are greater than the value it offers.

From the perspective of a business, privacy implies an investment to be measured in Euros saved as a result of reduced cost, or in additional revenues and profits from new activities that would not have occurred without the investment. From the risk management literature a number of metrics have evolved to measure security risks, some of which apply to privacy risks as well.[21]

Annual loss expectancy

One of the most common measures for the assessing the risk of a harmful event is Annual Loss Expectancy, or ALE. ALE is the product of the expected yearly rate of occurrence of the event times the expected loss resulting from the occurrence. Other yardsticks here are SLE and ARO. SLE stands for the Single Loss Exposure; this is the true cost of a security incident. ARO means annual rate of occurrence; this is the frequency with which a risk occurs on a yearly basis. The annual loss expectancy foreseen from all of an organization's operations would be the sum of the expected yearly losses that could result from multiple (privacy) threats. However, determining adequate inputs to this ALE equation is very difficult, due to lack of statistical data.

17 Camp & Wolfram 2000.
18 Chapman & Dhillon 2002.
19 Privacy Rights Clearinghouse 2007.
20 Borking 2009.
21 Fairchild & Ribbers 2008.

For example, if a bank estimates the probability of a serious security incident at one of its subsidiaries during 2008 as one in a million, and the direct and indirect cost of such an incident as 150 million Euros, the ALE created by the risk of this security incident for 2008 will be € 15 million times 1/1,000,000 = € 150. Of course the actual costs of this risk will never be that of the ALE, but it will be either € 0 or €150 million. In most cases the situation will be less certain and the probability or cost may range between one in five hundred thousand and one in a million and the cost may vary between € 100 million and € 200 million. The ALE would then be between: (€100M or €200M) x (1/500,000,1/1,000,000) = €100 or €400.[22]

Return on investment (ROI)

A metric that is quickly gaining in popularity is Return On Investments and specifically Return On Security Investments (ROSI).[23] Cardholm writes that: "Return on Investment (ROI) is a straightforward financial tool that measures the economic return of a project or investment. It is also known as return on capital employed. It measures the effectiveness of the investment by calculating the number of times the net benefits (benefits minus costs) recover the original investment. ROI has become one of the most popular metrics used to understand, evaluate, and compare the value of different investment options"[24]

The equation is: ROI = [(Savings from safeguards) + (profits from new ventures)] / costs of safeguards = [ALE (baseline) – ALE (with safeguards) + (profits from new ventures)] / costs of safeguards.[25] Suppose an organization decides to implement a Privacy Management System (PMS). The business case could be substantiated as follows: if PMS were not implemented, the minimum *annual* costs for a company employing 1,000 staff to comply with privacy policies are estimated as follows:

Annual costs
Salary costs for Privacy Protection Officer (100% time allocation) Euro 100,000; Management and secretarial salary costs Euro 40,000; Costs for privacy audit Euro 30,000; Security costs with respect to privacy compliance (excluding essential information security) Euro 20,000; Report maintenance, regulations, settling registered people's rights, information, image and other damage, etc. Euro 20,000. This leads to the total annual costs of Euro 210,000.

22 Blakley, McDermott & Geer 2002.
23 Sonnenreich, Albanese & Stout 2006.
24 Cardholm 2006.
25 Ribbers, Fairchild, Tseng, Dijkman & Borking 2007.

When comparing the situation where a PMS is used, the picture is as follows:

Development and implementation of PMS
For the acquisition of PMS has to be paid: Euro 150,000; Consultancy for PMS implementation (60 days) costs Euro 80,000; Start-up costs after implementation Euro 20,000. The total one-off costs are Euro 250,000.

To these, the following costs have to be added:

a. Annual costs PMS

b. PMS operational costs are Euro 30,000;

c. Maintenance costs are ± 15% of acquisition cost per annum: Euro 22,500;

d. Costs for privacy audit: Euro 10,000;

e. Salary costs for Privacy Protection Officer (50% time allocation) Euro 50,000;

In this situation the total costs are Euro 112,500.

The saving per annum compared with the situation when there was not an investment in PMS is Euro 210,000 – Euro 112,500 = Euro 97,500. Thus, the extra investment costs for PMS would be already fully recovered after approximately two years and two months.

Return on security investment (ROSI)

ROSI is a special application of ROI. The Return On Security Investments (ROSI) formula, developed by a team at the University of Idaho led by researcher Huaqiang Wei, is the most well known ROSI calculation in the security industry. They used what they found in the research area of information security investments and combined it with some of their own theories, assigning values to everything from tangible assets (measured in dollars with depreciation taken into account) to intangible assets (measured in relative value, for example, software A is three times as valuable as software B). Different types of attacks, or incidents, were assigned as individual costs. To verify the model, the team went about attacking an intrusion detection box they had built, to see if the costs the simulation produced matched the theoretical costs. They did. Determining the cost-benefit became the simple task of subtracting the security investment from the damage prevented.[26]

26 Berinato & Scott 2002.

ROSI is an approach to take into account the investment costs of security protection and the risk the investment removes. Assuming that the annual benefit of a security investment will be received throughout the lifetime of the investment, ROSI calculates the sum of the annual benefits over its cost. Benefits are calculated by adding expected cost savings to the new profit expected from new activities and sales.

Cardholm states that "it is basically a "savings" in Value-at-Risk; it comes by reducing the risk associated with losing some financial value".[27] Three core elements are determinative for the output calculation of the investment, namely: costs, turnovers and non-financial measurable elements. ROSI can be calculated using the equation below.

ROSI = (RiskExposure * %RiskMitigated) – SolutionCosts) / SolutionCost

The earlier discussed ALE can also be written as: RiskExposure * %RiskMitigated or Risk mitigated because of the investment in security.[28]

The difficult parts in the ROI method is determining ALE and SLE – the risk-mitigating benefits of the security investment – since it is very difficult to know the true cost of a security incident. According to Sonnenreich, Albanese & Stout[29] very little is known about those costs, because very few companies track those incidents.

Cardholm has a better approach with less uncertainty. His calculation is as follows:

ROSI = R – (R – E) + T,

or

ROSI = R – ALE, where ALE = (R – E) + T

The terms in Cardholm's equation can be described as:
- ALE: What we expect to lose in a year (Annual Loss Expectancy)
- R: The cost per year to recover from any number of incidents.
- E: These are the financial annual savings gained by mitigating any number of incidents through the introduction of the security solution.
- T: The annual cost of the security investment.[30]

27 Cardholm 2006.
28 Ribbers, Fairchild, Tseng, Dijkman & Borking 2007.
29 Sonnenreich, Albanese & Stout 2006.
30 Cardholm 2006.

ROI for privacy protection

The ROI calculation methods can also be used to analyze the return on investment for PETs mitigating privacy risks. PET investments differ from 'normal' ICT investments, since the investment may not directly improve the workflow, and it does not make a process more efficient. The costs from PETs are tangible and because of that, they are relatively easy to know. The benefits however are mostly intangible, because for example reputation improvement and a decreased risk for privacy incidents are not easy to quantify. However, these intangible benefits have the biggest value in a PET investments.

Luckily, the value of risk mitigation can be calculated using the method of Darwin (2007). The Darwin Calculator can be found at www.tech-404.com/calculator.html.

The focus in this method is on tangible benefits, the value of risks mitigated and total costs, related to PET investments. This method will be named: Return on Privacy Investments (ROIPI).[31] How these figures will be calculated will be explained below in more detail in the example of the Ixquick Europrise seal business case.

The associated formula is:

ROIPI = {(TangibleBenefits + ValueOfRiskMitigated) – TotalCosts} divided (/) by the total costs

When ROIPI gives a positive result, it means that the investment is beneficial for the company since the benefits outweigh the costs. Note that if the value of risk mitigated is positive this also has a positive influence on the ROIPI. The strong point of this formula is that it is not necessary to derive at an accurate estimate. The ROIPI only has to be precise enough to support the decision-making.

ROIPI assumes that the organization will fully comply with the law. This isn't often the fact. Violation of privacy, i.e. the illegal use of personal data, generates a lot of revenue and the chance that violation will lead to a prosecution is nil, due to the lack of resources of the National Data Protection Authorities.

IXQUICK

Ixquick is a meta search engine. The website of Ixquick be found at www.ixquick.com. The Ixquick revenue model is the number of hits times the advertising benefits. The revenue is highly correlated to the search queries

31 Fritsch 2008 and Dijkman 2008 were the first persons who used the term ROPI. I prefer ROIPI, preventing misunderstanding amongst auditors.

done through the site. In 2003 and 2004, Internet traffic went down. In 2005, Internet traffic only went down with 5% and stabilized. In 2006 and 2007 the traffic increased again, due to the fact that Ixquick anonymized IP addresses and search results from June 2006. Because of the anonymization, traffic in 2006 and 2007 increased considerably. Due to the optimalization of privacy protection, triggered by the requirements for obtaining the EuroPrise privacy certificate,[32] the number of visitors of the website increased substantially in 2008 again, thanks to the investment in the PET tool anonymization. With the increased traffic, the revenues of Ixquick went up as well.

The reason of Ixquick for using PET was that it is a unique selling point; Ixquick became and still is the first fully anonymized meta search engine. Besides this reason the other driver was privacy risk minimalisation. The investment costs for the PET tool were Euro 129.800, including the extra investments needed for meeting the requirements of the EuroPrise certificate. The expenditure for the optimalized privacy protection amounted to € 37.000 for technical and legal expertise. For press releases and communication costs announcing the Europrise privacy certificate award in July 2008[33] € 8.000 was spent. The costs mentioned were non-recurring one-off expenses.

Moreover, there are also recurring costs for the maintenance and the further development of the system amounting to € 16.500 per year. The total costs for the whole PET investment was: € 183.300. The ROIPI equation can now be used for calculating whether Ixquick's privacy protection investment was the right decision of Ixquick's management.

ROIPI = {(TangibleBenefits + ValueOfRiskMitigated) – TotalCosts} / (divided) by the total costs.

The total PET costs are Euro 183.300. The tangible benefits of using PET tools are the extra revenues because of the increased data traffic. The directly tangible advantage for Ixquick due to the use of PET for the period of PET investments (2005-2008) is estimated by me[34] at Euro 345.800. To estimate the factor 'risk mitigated' the calculation tool of Darwin (2008) has been used. It will be assumed that in a privacy incident 10.000 records were stolen. Based on the daily users of the Ixquick search machine, the actual risk was much higher. The risk class of this data is of risk class II according to the guideline of the Duch Data Protection Authority (CBP)[35] since the data consist of searches, these can consist of IP address, social security numbers and credit card numbers.

32 http://www.european-privacy-seal.eu/about-europrise/fact-sheet.
33 Andriessen 2008
34 The real financial figures are confidential.
35 Van Blarkom & Borking 2001.

Based on the Darwin calculator (2008) the value of risk mitigated is Euro 1.050.300 on the 80% level (loss of 10.000 records) and the Dollar/Euro exchange rate in November 2008. Using the values, the ROIPI equation produces as result:

TotalCosts = Euro 183.300

TangibleBenefits = Euro 345,800

ValueofRiskMitigated = Euro 1.050.300

The intangible costs and benefits are appreciated as Euro 0. Thus ROIPI = {(345.800 + 1.050.300 + 0) – 183.300} / 183.300 = ROIPI = 6,6165 = approx. 662% of the PET investment. As this ROIPI value is very high, the conclusion is that the investment is very worthwhile. This number is also very high because of the value of risk mitigated. The ROIPI equation is especially preferable for SMEs because of its simplicity. This formula is a quick and reliable indicator whether the investment is worthwhile.

The intangible costs and benefits have been appreciated as zero euro, but if these intangible elements would be calculable, then the result would be even more favorable. However, the ROIPI value is sufficiently high to carry out the PET investment and to justify the investment from a business economy point of view.

Others advocate rightfully that organizations should discard the above equations and instead use discounted cash flow methods for investments that have different costs and benefits in different years. The theoretical flaw in ROI (and so in ROSI, ROIPI and related approaches) is that it processes financial figures irrespective of the dates that will be received or paid. The value of 1 euro today is not the same as of 1 euro in two years time.[36] The Discounted Cashflow methods (DCF) encompass two separate methods, the internal rate of return (IRR) and the Net Present Value (NPV). The space allotted for this article does not allow elaborating on the IRR method.

Net present value (NPV)

The Net Present Value (NPV) of a project or investment is defined as the sum of the present values of the annual cash flows minus the initial investment. The annual cash flows are the Net Benefits (revenues minus costs) generated from the investment during its lifetime. These cash flows are discounted or adjusted by incorporating the uncertainty and time value of money. NPV is one of the most robust financial evaluation tools to estimate the value of an investment.[37]

36 Ribbers, Fairchild, Tseng, Dijkman & Borking 2007.
37 Cardholm 2006.

The calculation of NPV involves three simple yet nontrivial steps. The first step is to identify the size and timing of the expected future cash flows generated by the project or investment. The second step is to determine the discount rate or the estimated rate of return for the project. The third step is to calculate the NPV using the equations shown below:

NPV = initial investment + (Cash flow year 1 divided by $(1+r)^1$) +… (Cash flow year n divided by $(1+r)^n$)

Or

$$\text{NPV} = \text{Initial investment} + \sum_{t=1}^{t=\text{end of project}} \frac{(\text{Cash Flows at Year t})}{(1+r)^t}$$

The meaning of the terms is as follows:

- Initial investment: This is the investment made at the beginning of the project. The value is usually negative, since most projects involve an initial cash outflow. The initial investment can include hardware, software licensing fees, and start-up costs.
- Cash flow: The net cash flow for each year of the project: Benefits minus Costs.
- Rate of Return (r): The rate of return is calculated by looking at comparable investment alternatives having similar risks. The rate of return is often referred to as the discount, interest, hurdle rate, or company cost of capital. Companies frequently use a standard rate for the project, as they approximate the risk of the project to be on average the risk of the company as a whole.
- Time (t): This is the number of years representing the lifetime of the project.

Experts are convinced that a company should invest in a project only if the NPV is greater than or equal to zero. If the NPV is less than zero, the project will not provide sufficient financial benefits to justify the investment, since there are alternative investments that will earn at least the rate of return of the investment.[38]

38 Cardholm 2006.

Economic justification of investments in privacy risk reducing PET

Within the context of the NPV method, the following data have to be collected:

The *initial investment in privacy protection* [I(p)], which encompasses cash outlays for Privacy Risk Analysis, process modeling, PET, implementation of PET, productivity loss, change management.

The *yearly recurring cash flow*, which contains all yearly financial effects of the proposal. This calculation bears on an analysis of expected cash flow patterns that would occur with and without the investment; it reflects a difference between two situations defined. The so-called 'without' situation will usually be the continuation of the current situation. This can for example be a situation with existing privacy protection in place, where the added value of PET is considered. The 'without' situation might also be a situation without any privacy protection. The definition of the 'without' situation depends on the starting position of the decision-maker.

Ribbers proposes to take into account the following cash flow components: Annual Loss Exposure (ALE), Reputation Recoverage Costs (RRC), Expected Revenue Accrual (ERA), Recurring Privacy Costs (RPC).[39]

ALE is the multiplied projected costs of a privacy incident and its annual rate of occurrence. Basically this encompasses revenue losses, legal claims, and productivity losses because of privacy breaches, repair costs and lost business.

RCC contain those expenses needed to restore the reputation of the company damaged by privacy breaches; examples are additional costs for PR and Marketing. Moreover, if a privacy breach affects the share price of the company (see ChoicePoint, Double Click), banks and other financial institutions may require additional financial guarantees.

ERA represents, on the positive side, possible marketing impacts on market share and revenue of publicized implementation of PET.

RPC contains the yearly (additional) privacy costs caused by the proposal; this will encompass privacy threat or impact analyses, audits, privacy officers etc.

As said, the analysis compares the project situation with the situation without the project. Basically this boils down to analyzing the cash flow differences between the two situations. This can be done either by applying a factor RM (Risk Mitigated) to the situation without the investment or by subtracting the full-expected cash flow of the two situations from one another.

The RM factor for the applied privacy risk reducing/protection solution indicates what part of ALE and RRC has been compensated by the solution. Mitigated Risk is expressed as a reduction of the expected number of privacy breaches per year.

39 Ribbers, Fairchild, Tseng, Dijkman & Borking 2007.

The resulting NPV of a privacy protection solution is consequently as follows:[40]

$$NPV = - I(p) + \sum_{J=1}^{n} \{(ALE + RRC)\, RM + ERA - RPC\} / (1+i)^{j}$$

The case of the national victim tracking and tracing system (ViTTS)

The nation-wide implementation in the Netherlands of the Victim Tracking and Tracing System (ViTTS) is an important contribution to effective disaster management. The system provides regional medical officials with support to their tasks, through access to the required relevant contextual information, it supports the allocation of injured persons to local and regional hospitals, and it provides the relevant competent authorities with necessary information. Moreover, municipalities will be in a better position to execute mandatory registration procedures under the municipal disaster plan, and hospitals will be provided with timely information about the numbers of victims and the nature of their injuries. Due to the fact that sensitive personal medical information is processed about victims, the DPD requires optimal protection of such sensitive personal data. Privacy issues with respect to the health sector are particularly sensitive.

The EU PRIME[41] research team[42] has applied the NPV calculation approach in several case studies. One of the case studies is ViTTS. The following data have been collected from ViTTS.

The initial investment in privacy protection *I(p)* comprises the following components:

–	System analysis and design, prototyping, test runs:	Euro 15,000
–	Privacy audit and Privacy risk assessment:	Euro 50,000
–	Smart Cards for on line authentication and encryption:	Euro 25,000
–	Implementation costs of PET measures:	Euro 80,000
	The total initial investment in reducing the risks of privacy incidents:	Euro 170,000

40 Ribbers 2007. He drafted the first version of this equation.

41 PRIME (Privacy and Identity Management for Europe) Contract No. 507591 Research period 2004-2008.

42 The PRIME researchers were P. Ribbers (UoT), A. Fairchild (VUB), J. Tseng (EUR), R-J. Dijkman (UoT) & J.J. Borking (BC).

Privacy breaches affecting the process of handling victims would have serious consequences and should be avoided at all cost. The privacy threat analysis showed that without privacy protection the ViTTS system would undergo privacy breaches on a regular basis. The damage that would result from that can be estimated as follows.

The direct consequence of a breach (SLE: Single Loss Exposure) would be loss of reputation of the national government, possible wrong allocation of victims to hospitals with ineffective treatment and possibly deceases as a consequence. This may lead to significant legal claims. Claims of Euro 100,000 per case are not exceptional.

Such a breach would necessitate a nation-wide roll out of system adaptations, for which two man-months per designated preventive health care safety region are needed, at Euro 100 per hour:

Total costs	Euro 347,000
Test and Trials to prove effectiveness of the system:	Euro 80,000 per region:
Total cost	Euro 800,000
Training and education roll out:	Euro 50,000
The total recovery costs (RCC) would amount to:	Euro 1,197,000

The expected revenue accrual (ERA) can be estimated as follows. The most important reason for designated preventive health care safety regions to adopt the system is the built-in optimal privacy protection. So without privacy protection or with a much less rigid privacy protection such a system would not have been developed.

The estimated salary costs to replace the system by manual procedures would amount to 3 FTEs per region, which amounts to Euro 180,000 per region.

Nationwide, this would result in a cost of:	Euro 1,800,000
The total benefits of protecting privacy and reducing the risks of privacy incidents can be estimated at:	Euro 2,277,000

(in this number legal claims are not included)

Scenario

For the NPV calculation the following is assumed:

1. a time horizon of 6 years
2. a serious privacy breach every 2 years
3. a cost of capital of 5%

Applying the equation results into the following:

I(p):	Euro 170,000
Recurring cash flows:	
– costs avoided every two years:	Euro 2,277,000
– yearly recurring privacy costs:	Euro 400,000
– privacy costs in year 3 (no costs in year 6 given the assumption)):	Euro 25,000

Under this assumption the calculation would be as follows:

NPV = – 170,000 + 2,277,000 (0.907029 + 0.822702 + 0.710681) – 25,000 (0.863838) – 400,000 (5.242137) = Euro + 3,268,368

This (positive) business case does not include possible legal claims.

The business case for the investment mitigating the risk of privacy incidents is positive. Other scenarios lead to a positive business case as well. The privacy protection will even be profitable under the unrealistic assumption of a privacy breach only occurring once (and taking legal claims into account).

Conclusions

The ROI and NPV calculation methods are useful tools for assessing the (planned) investments in PETs, reducing the risks of privacy incidents considerably. ROI, ROSI and ROIPI provide useful insights. For a 'quick and dirty' assessment of a PET investment ROIPI is useful especially for SMEs, such as in the Ixquick business case. However ROIPI and other ROI methods are based on evaluating reductions in risks and do not take a time factor into account. The best approach would be to consider investments in PET as regular investments, characterized by cash flow patterns.

The Net Present Value approach is applied on the ViTTS case. This approach is effective in the context of assessing investments in PET, reducing privacy risks and enhancing privacy protection. As many data are uncertain due to the lack of recorded privacy incidents, scenarios have to be designed and assessed to give decision makers an understanding of the behaviour of cost and benefit factors and their effect on the business case. Much more research on the economics of privacy has to be done.

References

Andriessen 2008
V. Andriessen, 'Nederlandse Internetzoekmachine Ixquick ontvangt eerste Europese privacycertificaat', *Het Financieele Dagblad*, 15 juli 2008.

Blakley, McDermott & Geer 2002
B. Blakley, E. McDermott and D. Geer, 'Information management is Information Risk Management', in: *Proceeding NSPW'01*, Cloudcroft, New Mexico, 2002.

Blarkom & Borking 2001
G.W. van Blarkom and J.J. Borking, *Beveiliging van Persoonsgegevens*, Achtergrond en Verkenningen 23, Den Haag 2001.

Blarkom, Borking & Olk 2003
G.W. van Blarkom, J.J. Borking and J.G.E. Olk, *Handbook of Privacy and Privacy-Enhancing Technologies*, The Case of Intelligent Software Agents, Den Haag, 2003.

Borking 2003
J.J. Borking, 'The Status of Privacy Enhancing Technologies', in: E. Nardelli, S. Posadziejewski & M. Talamo (eds.), *Certification and Security in E-Services*, Boston, 2003.

Borking 1996
J.J. Borking, 'Der Identity Protector', in: *Datenschutz und Datensicherheit*, 11, 1996.

Borking 2001
J.J. Borking, 'Mag het een bitje minder zijn?', in: *Compact* 2001 nr. 4.

Borking 2009
J.J. Borking, 'El "business case" de PET (Tecnologías de Mejora de la Privacidad) y el sello EuroPrise', Madrid 2009.

Camp & Wolfram 2000
L.J. Camp and C. Wolfram, 'Pricing Security', in: *Proceedings of the CERT Information Survivability Workshop*, Boston MA, 2000.

Cardholm 2006
L. Cardholm, *Adding Value to business performance through cost benefit analyses of information security management*, Gävle 2006.

Chapman & Dhillon
S. Chapman and G.S. Dhillon, 'Privacy and the internet: the case of DoubleClick, Inc.', in: *Social Responsibility in the Information Age: Issues and Responsibilities*, Fort Lauderdale-Davie, 2002.

Dijkman 2008
R-J. Dijkman, *A Method for Making a Business case for Privacy Enhancing technologies*, doctoral thesis, Tilburg 2008.

Fairchild & Ribbers 2008
A. Fairchild and P. Ribbers, 'Privacy-Enhancing Identity Management in Business', in: *Privacy and Identity Management for Europe*, J. Camenish, R. Leenes & D. Sommer (eds.) Brussels, 2008.

Flaherty 2000
D.H. Flaherty, 'Privacy Impact Assessments: An Essential Tool for Data Protection', in: *Privacy Law & Policy Reporter* Vol 7, No 5, October 2000.

Fritsch & Abie 2008
L. Fritsch and H. Abie, 'A Road Map to the Management of Privacy Risks', in: *Information Systems*, Oslo, 2008

Hes & Borking 1998
R. Hes and J.J. Borking, *Privacy-Enhancing Technologies: The Path to Anonymity*, The Hague, 1998.

Hewitt 1997
K. Hewitt, *Regions of risk: A geographical introduction to disasters*, Harlow, Essex, 1997.

Koorn et al. 2004
R. Koorn, H. van Gils, J. ter Hart, P. Overbeek, R. Tellegen and J.J. Borking, *Privacy Enhancing Technologies, Witboek voor Beslissers*, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag 2004.

Mileti 1999
D.S. Mileti, *Disasters by Design, A Reassessment of Natural Hazards in the United States*, Washington D.C. 1999.

Muller 2004
E.R. Muller (ed.), *Veiligheid, Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn 2004.

Parker, Benson & Trainor 1988
M.M. Parker, R.J. Benson and H.E. Trainor, *Information Economics-linking business performance to information technology*, PrenticeHall, 1988.

Ribbers, Fairchild, Tseng, Dijkman & Borking 2007
P. Ribbers, A. Fairchild, J. Tseng, R.J. Dijkman and J.J. Borking, *Privacy and Identity Management for Europe*, PRIME Report F3, Brussels 2007

Schneier 2000
B. Schneier, 'Threat Modeling and Risk Assessment', in: H. Baumler, *E-privacy, Datenschutz im Internet*, Wiesbaden 2000.

Sonnenrecht, Albanese & Stout 2006
W. Sonnenreich, J. Albanese and B. Stout, 'Return on Security Investment (ROSI) – A Practical Approach', in: *Journal of Research and Practice in Information Technology*, Vol. 38, No. 1, Feb. 2006.

Tettero 2000
O. Tettero, *Intrinsic Information Security: Embedding Security Issues in the Design Process of Telematics Systems*, Telematica Instituut Fundamental Research Series, No. 006, (Ph.D. thesis) Enschede, 2000.

Tsiakis & Stephanides 2005
T. Tsiakis and G. Stephanides, 'The economic approach of information security', in: *Computers & Security*, 24, 2005.

Recht en markt: met falen en opstaan

Mireille Hildebrandt■

Introductie

Mijn waardering voor Aernout Schmidts *be*scheidenheid, eruditie en historisch besef is des te groter nu hij tegelijk een scherp analyticus is, altijd bereid om wat voor de hand ligt af te zetten tegen wat onder de voet wordt gelopen. De *ver*scheidenheid van zijn belangstelling drong zich op toen hij liet vallen dat hij Heimito Doderers *Die Strudlhofstiege* ging aanschaffen, waardoor ik een nieuw stukje van mijn eigen onwetendheid en een nieuwe auteur van het formaat van Musil ontdekte.[1] Schrijvend over het Wenen van de eerste helft van de 20e eeuw voegt Doderer zich in de lange rij van Midden-Europese overgangsfiguren die worstelden met de confrontatie tussen een rationalistisch, op natuurwetenschappelijke causaliteiten gebaseerd wereldbeeld en de duistere oprispingen van het onderbewuste.[2] Voorzover Doderer de verheerlijking van het onbewuste weet te vermijden die in sommige interpretaties van Schopenhauer, Nietzsche en Freud naar voren treedt, zou ik hem zelfs aan kunnen halen bij het formuleren van een kritiek op het rationele keuzemodel dat ten grondslag ligt aan de economische analyse van het recht.

Zo'n kritiek is echter al eerder geschreven en de huidige generatie rechtseconomen lijkt zich bewust te zijn van de *caveats* bij haar uitgangspunten.[3] In dit hoofdstuk zal ik mij in eerste instantie dan ook beperken tot de vraag in hoeverre nieuwe ICT-infrastructuren tot een vorm van marktfalen kunnen leiden die de effectiviteit en de legitimiteit van rechtsregels aantast.[4] Bij het zoeken naar remedies zal ik vervolgens aandacht besteden aan de mate waarin een economische analyse recht kan doen aan juridische begrippen

---

■ Mireille Hildebrandt is universitair hoofddocent rechtsfilosofie en rechtstheorie aan de Faculteit Rechtsgeleerdheid, Erasmus Universiteit Rotterdam. Sinds 2002 is zij parttime gedetacheerd naar het centrum voor Law Science Technology and Society studies (LSTS) aan de Vrije Universiteit Brussel. Zij werkt als senioronderzoeker op het 5-jarige fundamenteel onderzoeksproject inzake 'Law and Autonomic Computing: Mutual Transformations'. Zij was 5 jaar lang coördinator van het onderdeel 'profiling' van het Europese KP6 project inzake de Future of Identity in Information Society (FIDIS) en redigeerde samen met Serge Gutwirth *Profiling the European Citizen. Cross-Disciplinary Perspectives* (2008). Zie http://works.bepress.com/mireille_hildebrandt/.

1 Von Doderer 1953.

2 Twee cultuurhistorische beschrijvingen van deze periode: Luft 2003 en Schorske 1981.

3 Ulen 1999 en Kerkmeester 1999.

4 Over de invloed van ICT op de Trias Politica, zie meesterlijk Schmidt 2008.

die constitutief zijn voor een rechtsstatelijke democratie. Ik zal de vraag verder inperken door haar toe te spitsen op de bescherming van privacy in het tijdperk van profileringstechnologie.

Commodificatie van privacy: Lessig en gegevensbescherming

In de eerste versie van zijn *Code and other Laws of Cyberspace* (1999) stelt Lawrence Lessig voor om de bescherming van privacy te regelen via het toekennen van eigendomsrechten op persoonsgegevens.[5] Deze rechten zouden toe moeten komen aan de 'data-subjecten'[6] die er vervolgens naar eigen inzicht mee zouden kunnen (onder)handelen. Hoewel Lessig in de tweede versie (2006) gas terug neemt naar aanleiding van de kritiek die zijn voorstel heeft ontvangen, wil ik hier nog eens aandacht vragen voor zijn betoog.[7] De reden daarvoor is dat naar mijn mening de commodificatie van persoonsgegevens onder het regime van de Richtlijn Gegevensbescherming allang een feit is, nu het uitwisselen van gegevens op grond van toestemming een van de belangrijkste rechtsgronden is voor het verwerken van gegevens.[8] Dat roept de vraag op of deze commodificatie effectieve bescherming biedt voor de privacy.

Lessig noemt twee voordelen van het toekennen van eigendomsrechten: ten eerste ontstaat daardoor een prikkel voor marktpartijen die brood zien in het verwerken van persoonsgegevens om zich van toestemming te verzekeren, en ten tweede schept deze oplossing de mogelijkheid om de individuele preferenties van data subjecten ruim baan te geven. Het eerste voordeel lijkt te suggereren dat het verwerken van persoonsgegevens zonder toestemming beter als een inbreuk op een eigendomsrecht kan worden gezien dan als een inbreuk op een persoonlijkheidsrecht.[9] Zou de prikkel om toestemming te regelen groter zijn als de aanspraak op persoonsgegevens wordt gekwalificeerd als eigendomsrecht dan wanneer sprake is van een persoonlijkheidsrecht? In beide gevallen staat het de rechthebbende vrij om afstand te doen van haar recht of van de uitoefening van het recht en is het ook onder de Richtlijn Gegevensbescherming niet verboden om consumenten die bereid zijn hun persoonsgegevens te verstrekken in ruil daarvoor korting of toegang tot bepaalde informatie te geven. Het gaat Lessig dan ook niet om het afzetten van de eigendomsvariant tegenover die van het persoonlijkheidsrecht, maar om de vergelijking met de bescherming op basis van de

5 Lessig 1999.

6 Een 'data-subject' of 'betrokkene' is degene op wie een persoonsgegeven betrekking heeft (art. 1 sub f Wet Bescherming Persoonsgegevens).

7 Lessig 2006, p. 228-230.

8 Richtlijn Gegevensbescherming D 95/46 EC, art. 6; in Nederland uitgewerkt in de Wet Bescherming Persoonsgegevens art. 8.

9 Voor nadere overwegingen over privacy als persoonlijkheidsrecht en de commodificatie van persoonsgegevens zie Prins 2004.

onrechtmatige daadsactie. Zijn inspiratie komt voort uit het beroemde artikel van Calabresi en Melamed, waarin zij op rechtseconomische gronden de bescherming van eigendom als efficiënter beschrijven dan die van de onrechtmatige daad.[10] Ik kom daar in de volgende paragraaf op terug, bij de bespreking van de kritiek van met name Paul Schwartz op Lessigs voorstel. Hier is het goed om vast te stellen dat ook als privacy wordt gekwalificeerd als een persoonlijkheidsrecht, persoonsgegevens niet noodzakelijk onvervreemdbaar zijn en in de typologie van Calabresi en Melamed (en Lessig) eerder onder de eigendomsregels zullen vallen.[11]

De vraag is of het eerste voordeel wel een voordeel is, nu het regelen van toestemming geen garantie is dat de privacy van de betreffende persoon daadwerkelijk wordt beschermd. De schier eindeloze discussie over hoe die toestemming tot stand zou moeten komen (opt in of opt out) geeft al aan dat het hier vaak om een formaliteit gaat die gedachteloos wordt verricht (uit onderzoek blijkt dat de default-instelling bepalend is voor het geven van toestemming: bij opt in worden gegevens niet verstrekt; bij opt out worden ze quasi-automatisch gegeven).[12] Het feit dat een eigendomsrecht een prikkel geeft om toestemming te verzekeren leidt dus niet noodzakelijk tot bescherming van de privacy. Dat Lessig dat anders ziet, hangt samen met het feit dat hij ertoe neigt privacy te reduceren tot het vrijwillig afgeven van persoonsgegevens; het gaat hem er vooral om de controle over die gegevens in handen te stellen van degene die het betreft.

Dat hangt direct samen met het tweede voordeel dat hij noemt. Lessig meent terecht dat het er bij privacy *niet* om gaat zo min mogelijk gegevens te verstrekken, maar juist mogelijkheden te scheppen om het data-subject zelf vast te laten stellen welke gegevens zij in een bepaalde context wel of niet met een bepaalde partij wil delen. Lessig benadrukt dat het van belang is om de juridische en technische infrastructuur te ontwerpen die precies deze vrijheid organiseert. Juridisch kiest hij voor eigendomsrechten omdat de betrokkene dan zelf kan bepalen of en zo ja welke gegevens zij met wie wil delen en ook zelf de prijs vast kan stellen waartegen zij bereid is ze af te staan. Eigendomsrechten zouden consumenten aldus een zelfbeschikkingsrecht geven over hun persoonlijke informatie. Wat Lessigs voorstel zo interessant maakt is dat hij zich bewust is van de noodzaak om de uitoefening van dat recht technisch mogelijk te maken. Daartoe kiest hij voor een systeem waarbij de betrokkene wordt bijgestaan door een software-programma (elektronische butler) dat communiceert met de software van de wederpartij om bijvoorbeeld na te gaan wat met de gegevens zal worden gedaan en of ze aan derden zullen worden geleverd; dankzij het instellen van privacy-preferenties kan het eigen software-programma dan automatisch persoonsgegevens

10 Calabresi & Melamed 1972.

11 Naast eigendomsregels en aansprakelijkheidsregels onderscheiden Calabresi en Melamed regels voor onvervreemdbare aanspraken, waarbij een aanspraak onvervreemdbaar is in de mate waarin zij niet mag worden overgedragen.

12 Zie bijvoorbeeld Bouckaert & Degryse 2006.

uitwisselen als het privacy-beleid van de wederpartij aansluit op de wensen van het data-subject. Op deze manier zou zich in rechtseconomische termen een pareto-optimale situatie kunnen ontwikkelen waarbij voor alle partijen de meest gunstige gegevensuitwisseling plaats vindt. Pareto-optimaal betekent in dit geval dat geen enkele uitwisseling van gegevens het welzijn van een partij nog kan vergroten zonder dat van een andere partij navenant te verkleinen. Tegen deze commodificatie zal ik twee typen bezwaren aanvoeren. Ten eerste zal ik beargumenteren dat hier sprake is van marktfalen, waardoor geen pareto-optimale situatie wordt bereikt. Ten tweede zal ik het privacybegrip dat ten grondslag ligt aan de door Lessig geponeerde voordelen van commodificatie bekritiseren.

Marktfalen bij de uitwisseling van persoonsgegevens

In zijn kritiek op Lessig schetst Schwartz nog eens het kader dat Calabresi en Melamed ontwierpen voor het onderscheiden en evalueren van eigendomsregels en aanprakelijkheidsregels. Eigendomsregels beschermen aanspraken op een goed door 'een recht te verlenen dat zonder instemming van de rechthebbende niet mag worden aangetast. Het recht kan slechts worden overgedragen door een vrijwillige transactie'.[13] Een dergelijke regel werkt vanuit rechtseconomisch perspectief goed als sprake is van weinig partijen, subjectieve waardering en lage transactiekosten. Het grote voordeel is dat partijen naar eigen inzicht transacties aan kunnen gaan, zelf de prijs bepalen en in beginsel geen verantwoording af hoeven te leggen aan derden of aan de staat. Tegelijkertijd leiden deze eigendomsregels – als aan de voorwaarden van weinig partijen en lage transactiekosten is voldaan – tot een pareto-optimale situatie.

Wanneer sprake is van een veelheid van partijen, monopolie posities, strategisch onderhandelen en hoge transactiekosten leidt dit soort regels tot marktfalen in de zin dat geen pareto-optimale situatie tot stand komt. Partijen kunnen namelijk niet overzien wat in hun belang is, gezien de complexiteit van de verhoudingen, de ongelijke onderhandelingspositie en het gebrek aan informatie. In dat geval raden Calabresi en Melamed een aansprakelijkheidsregel aan 'die inhoudt dat de aanspraken van een ander mogen worden aangetast, maar dat hier de verplichting tot een objectief vastgestelde schadevergoeding tegenover staat. Deze bescherming is niet afhankelijk van een overeenkomst tussen laedens en gelaedeerde en heeft daardoor haar waarde in situaties van hoge transactiekosten'.[14]

Wat opvalt is dat Calabresi en Malamed eigenlijk niet spreken over het juridische eigendomsrecht of de rechtsfiguur van de onrechtmatige daad, ook al vormen die de inspiratie van hun model en kunnen hun aanbevelin-

13 Kerkmeester & Holzhauer 1999, p. 30.
14 *Ibid*, p. 31.

gen wel leiden tot het creëren van eigendomsrechten (denk bijvoorbeeld aan emissierechten in het milieurecht). Persoonlijkheidsrechten zoals de bescherming van persoonsgegevens vallen moeiteloos onder de door hen geschetste eigendomsregels, zolang er maar een regime bestaat dat voorafgaande toestemming vereist voor het delen van persoonsgegevens (waarbij we dan overigens wel moeten abstraheren van de veelheid van andere rechtsgronden die het verzamelen van persoonsgegevens zonder toestemming juridisch mogelijk maakt).

De klassieke onrechtmatige daad vereist onrechtmatigheid, hetgeen impliceert dat aantasting van de aanspraak (op bijvoorbeeld zorgvuldig gedrag in het verkeer of van de werkgever) niet is toegestaan en juist daarom tot schadevergoeding leidt. Ott en Schaefer merken op dat Calabresi en Melamed met hun definitie van aansprakelijkheidsregels afwijken van het klassieke juridisch discours, doordat zij hun definitie beperken tot een type onvrijwillige transacties dat weliswaar schade toebrengt maar dat kennelijk sociaal wenselijk is. Over onrechtmatigheid reppen zij niet.[15] Ott en Schaefer geven het voorbeeld van de rechtmatige overheidsdaad, maar mij dunkt dat Calabresi en Melamud juist doelen op activiteiten als autorijden en het fabrieksmatig verwerken van giftige stoffen. Hun *verklaring* van de aansprakelijkheidsregels van het onrechtmatige daadsrecht wijkt dan ook evident af van de manier waarop juristen het onrechtmatige-daadsrecht zelf *legitimeren*. Kort samengevat bieden eigendomsregels (door middel van een verbod van aantasting) een bescherming vooraf, terwijl aansprakelijkheidsregels pas achteraf 'beschermen' (door middel van compensatie).

Schwartz bekritiseert Lessigs keuze voor eigendomsregels aan de hand van drie criteria, aangedragen door Calabresi en Melamed: het aantal betrokken partijen, de transactiekosten en de subjectieve waardering van het beschermde recht. Ten aanzien van het eerste criterium merkt hij op dat de uitwisseling van gegevens zich lijkt af te spelen tussen twee partijen, bijvoorbeeld een service provider en een klant. In werkelijkheid gaat het echter om een veelheid van partijen omdat gegevens vaak worden verhandeld of door anderen worden gebruikt. In welke databestanden de gegevens uiteindelijk terecht komen is voor de klant niet te overzien. Vanuit Europees perspectief kunnen we daar aan toevoegen dat de richtlijn gegevensbescherming secundair en tertiair gebruik van persoonsgegevens in beginsel uitsluit, maar dat de toegestane uitzonderingen op dat verbod legio zijn, terwijl de toestemming die aan de klant wordt gevraagd vaak impliciet of expliciet het gebruik van gegevens voor marketing doeleinden bevat en voor *client relationship management*.

Daarmee zijn we aangekomen bij het tweede criterium, dat van de informatieachterstand. Schwartz merkt op dat zolang de elektronische butler waar Lessig voor pleit niet op grote schaal wordt gebruikt, klanten geen zicht hebben op de wijze waarop organisaties omgaan met hun gegevens. Ik

15 Ott & Schaefer 2009, p. 44.

voeg daaraan toe dat Lessig's software wel kan checken of het privacy-beleid zoals vastgelegd in de *privacy policy* van de wederpartij aansluit op de privacy preferenties van de klant, maar niet kan testen of die organisatie zich aan dat beleid houdt.[16] In feite hebben klanten voorafgaand aan hun transactie geen enkel zicht op wat er met hun gegevens kan gebeuren en hoe dat hun verdere levensloop kan beïnvloeden.

Schartz's derde criterium betreft het feit dat wanneer de waardering van de te beschermen aanspraak individueel bepaald wordt en contextafhankelijk is, de voorkeur moet worden gegeven aan eigendomsregels. Hoewel ook hier op het eerste gezicht evident sprake is van subjectieve voorkeuren (privacy als persoonlijke smaak) speelt juist bij de uitwisseling van persoonsgegevens de waardering die anderen daaraan geven een doorslaggevende rol. Het meest evidente voorbeeld dat zich inmiddels opdringt is de rol die reputatie speelt in online sociale netwerken: de uitwisseling van gegevens wordt gestuurd door de hoop op een goede reputatie (of een *cool image*).[17] De idee dat gebruikers uiteindelijk zelf kunnen kiezen welk type reputatie ze willen ontwikkelen lijkt gebaseerd op een naïeve notie van individuele ontplooiing; juist omdat jongeren zich moeilijk kunnen onttrekken aan de sociale druk van hun *peer group* gaan ze over tot het uitwisselen van intimiteiten waar zij op een later moment wel degelijk spijt van kunnen krijgen. Op het moment dat de gebruiker ontdekt dat al die persoonlijke exhibitie ook door toekomstige werkgevers of door de belastingdienst, de politie of verzekeringsmaatschappijen kan worden bekeken, wordt duidelijk dat de waardering van de beschermde aanspraak geen hoogste individuele kwestie is. Schwartz behandelt onder het derde criterium ook de ongelijke onderhandelingsmacht van partijen, die ertoe kan leiden dat iemand een vrijwillige transactie aangaat bij gebrek aan beter (monopolievorming bij de aanbieder). Ook dat pleit volgens hem voor een aansprakelijkheidsregime in plaats van eigendomsregels, dan wel voor een gemengd regime. De Richtlijn Gegevensbescherming kan in die zin een gemengd regime worden genoemd, nu art. 23 de verantwoordelijke gegevensverwerker aansprakelijk stelt voor schade geleden bij aantasting van de aanspraken die door de Richtlijn worden beschermd.

Samenvattend kom ik met Schwartz tot de conclusie dat de markt voor persoonsgegevens om allerlei redenen een falende markt is, die vraagt om andere oplossingen dan het toekennen van eigendomsrechten. Een van de problemen van het model van Calabresi en Melamed in deze context is bovendien dat voor zover zij de voorkeur geven aan bescherming door aansprakelijkheid (dus achteraf) in plaats van eigendomsregels, ook die aanspraak eerst moet worden gecommodificeerd om in het model te passen.

16 De technische bescherming waar Lessig voor pleit is om die reden van veel kanten bekritiseerd. Voor een overzicht van *transparency enhancing tools* (TETs) zie Hildebrandt 2009.

17 Over de invloed van sociale netwerken op de *digital natives* zie bijvoorbeeld Tapscott 2009.

Ook de onvervreemdbare aanspraken moeten als rekeneenheid worden gekwalificeerd om er in het model mee te kunnen werken. Dit is eigen aan rechtseconomische modellen en op zich geen probleem. Op het moment dat de aanspraak betrekking heeft op een goed dat zich per definitie aan commodificatie onttrekt, biedt zo'n model echter geen uitkomst.[18]

Privacy als privaat belang en als *public good*

Een reden om goed kennis te nemen van de tekst van Schwartz is de manier waarop hij het privacy-begrip bekritiseert dat ten grondslag ligt aan Lessigs analyse.[19] Dat opent de mogelijkheid om naast een interne kritiek (eigendomsregels werken niet vanwege marktfalen) ook een externe kritiek te ontwikkelen (privacy leent zich niet onder alle omstandigheden voor commodificatie). Hoewel Lessig privacy ziet als een belangrijk constitutioneel recht, lijkt hij bij de keuze voor het model van Calabresi en Melamed terug te vallen op een soort methodologisch en normatief individualisme dat precies bij de analyse van privacy rechten problematisch is. Schwartz stelt dan ook voor om privacy niet te begrijpen in termen van de controle die een individu heeft over de eigen persoonsgegevens maar als een waarde die constitutief is voor rechtsstaat en democratie.

Daarmee is privacy niet alleen een privaat belang, dat zich leent voor een calculatie op grond van persoonlijke preferenties, maar ook een *public good* dat tegelijk voorwaarde en product is van een rechtsstatelijke democratie.[20] Het recht op informationele zelfbeschikking dat Lessig voorstaat, betreft privacy als privaat belang, waarmee vanuit een rechtseconomische benadering 'gerekend' kan worden. Hiertegenover staat de benadering die het Duitse Federale Constitutionele Hof koos in het census-arrest van 1983. Het Hof kwalificeert de aanspraak als het grondrecht (en persoonlijkheidsrecht) van informationele zelfbeschikking,[21] en baseert zich daarbij onder meer op het onvervreemdbare grondrecht van de menselijke waardigheid (art. 1 van de Duitse Grondwet). In beide gevallen is het zelfbeschikkings-

18 Rechtseconomen zullen niet snel toegeven dat er juridisch relevante aanspraken zijn die niet via een *tertium comparationis* als geld, nut of preferenties in het model kunnen worden opgenomen, zie de manier waarop Kerkmeester (1999) en Uler (1999) met dit type kritiek omgaan (zij relativeren het uitgangspunt zonder het op te geven).

19 Zie ook Solove (2002) voor een pragmatische benadering van het privacy begrip en Nissenbaum (2004) voor het conceptualiseren van privacy als 'contextuele integriteit'.

20 Ik heb dat op verschillende plaatsen elders uitgewerkt, zie bijvoorbeeld Hildebrandt 2006 en 2008b. Vgl. het WRR rapport over mondig burgerschap, dat niet alleen de vooronderstelling maar ook de opdracht en het product is van een duurzame democratie (Van Gunsteren 1992).

21 BVerfGE 65, 1 (Uitspraak van het Duitse Federale Constitutionele Hof van 15 december 1983: het census arrest). Beschikbaar via http://www.servat.unibe.ch/law/dfr/bv065001.html.

recht een instrument om een bepaald doel te bereiken. Het rechtseconomische doel is de weg te effenen voor een pareto-optimale situatie, het mensenrechtelijke doel is de bescherming van de menselijke waardigheid.[22] Dat laatste is een *public good* dat zich in beginsel onttrekt aan een denken in termen van geaggregeerde preferenties.[23] Schwartz komt met drie argumenten om privacy niet alleen te bekijken op basis van het methodologisch individualisme dat de grenzen bepaalt van een rechtseconomische analyse.

Om te beginnen lijkt Lessig's individualistische privacy paradigma blind te zijn voor de implicaties van dataverzameling en -aggregatie, data-analyse en individuele en groeps-profilering voor de constructie van persoonlijke identiteit. Persoonlijke preferenties staan niet los van de mogelijkheden die de omgeving biedt om preferenties te ontwikkelen, het zijn geen onafhankelijke variabelen. Agre en Rotenberg definiëren het recht op privacy als: "the freedom from unreasonable constraints on the construction of one's own identity." [24]

Daarmee erkennen zij het verband tussen de negatieve vrijheid (*vrijheid van* externe inperkingen) en de positieve vrijheid (*vrijheid om* een eigen identiteit de ontwikkelen),[25] en benadrukken aldus het constitutieve karakter van privacy voor de ontwikkeling van een mondig burgerschap. De tsunami aan op zichzelf genomen triviale gegevens die in databestanden zijn opgeslagen, maakt dankzij geavanceerde data-analysetechnieken een verfijnde categorisering mogelijk van consumenten, terwijl die categorisering voor henzelf verborgen blijft. Dit maakt een subliminale – onbewuste – beïnvloeding mogelijk, die afbreuk doet aan de idee van mondig burgerschap. De gevaren die hieraan verbonden zijn ziet Schwartz vooral als bedreigingen van de gelijkheid en de autonomie van burgers. De gelijkheid komt in gevaar omdat organisaties die gebruik maken van profileringstechnieken kennis in huis hebben waarmee zij (potentiele) klanten kunnen categoriseren. Dat biedt interessante mogelijkheden voor prijsdiscriminatie en manipulatie.[26] Daarmee is tegelijkertijd de autonomie van de klant in gevaar, die niet kan achterhalen waarom zij een bepaald aanbod wel of niet krijgt.

Stel dat profileringsoftware uit mijn surfgedrag afleidt dat ik op het punt sta om vegetariër te worden en deze informatie verkoopt aan bedrijven die

22 Deze opvatting leidt dan ook tot BverfGE 120, 274 (Uitspraak van het Duitse Federale Constitutionele Hof van 27 februari 2008: grondrecht op computerbescherming) waar het Hof een grondrecht afleidt op de vertrouwelijkheid en de integriteit van informatietechnologiesystemen.

23 Binnen de economische wetenschappen en de speltheorie wordt een *public good* gedefinieerd in termen van *nonrivalrousness* en *nonexcludability*, zie Stiglitz 1999. Het gaat mij eerder om waarden en belangen (aanspraken) die niet als geaggregeerde preferenties begrepen kunnen worden, bijvoorbeeld omdat ze de *incentive* structuur bepalen die preferenties mogelijk maken en mede bepalen.

24 Agre & Rotenberg (2001), p. 7.

25 Berlin (1958) 1969.

26 Zie over privacy, data analyse en prijsdiscriminatie Odlyzko 2003.

er belang bij hebben dat ik vlees blijf consumeren.[27] Gedurende enige maanden ontvang ik regelmatig kortingen en gratis aanbiedingen van vlees, maar ik zie ook 'banners' op mijn scherm als ik de *New York Times* lees, die naar wetenschappelijk onderzoek verwijzen dat de voordelen van het eten van vlees bevestigt. Allemaal geen probleem zolang ik maar doorheb dat hier een poging wordt ondernomen mijn toekomstig gedrag te beïnvloeden. Dat is echter niet het geval. De profielen op grond waarvan mijn plan om vleesloos te gaan eten is 'voorzien' zijn niet verkregen uit mijn eigen persoonsgegevens. Deze profielen komen voort uit complexe data-analyses van een enorme populatie internetgebruikers. Het toenemende gebruik van profileringstechnologieën sluit uit dat ik hoe dan ook zou kunnen overzien met wat voor profielen mijn data *matchen*; ik heb dus geen idee op grond waarvan ik aanbiedingen krijg en welke *advertorials* specifiek op mij zijn gericht.[28]

De tweede en derde reden om privacy niet vanuit een individualistisch paradigma te begrijpen, hangen samen met het feit dat de samenleving om velerlei redenen toegang nodig heeft tot persoonsgegevens om te kunnen functioneren. De idee dat individuele burgers die toegang te allen tijden kunnen blokkeren zonder rekening te houden met publieke belangen gaat volgens Schwartz in tegen de kerntaak van *information privacy law* ofwel het recht inzake gegevensbescherming. Die kerntaak bestaat niet zozeer uit de bescherming van individuele voorkeuren om informatie achter te houden, maar uit het reguleren en inperken van de toegang tot persoonsgegevens. Schwartz wijst op de informatieplichten die de welvaartsstaat oplegt aan degenen die van haar inkomensherverdeling profiteren en op de toegang tot informatie die noodzakelijk is in een open democratische rechtsorde. Als derde argument om privacy niet alleen vanuit de individuele burger te begrijpen, wijst hij ten slotte op de noodzaak van de registratie van persoonsgegevens in publieke registers die de economische efficiëntie (lage transactiekosten) bevordert binnen een markteconomie (denk aan de burgerlijke stand, het kadaster, het handelsregister).

In plaats van een eenzijdige nadruk op individuele controle over persoonsgegevens stelt Schwartz voor privacy te begrijpen als een constitutieve waarde die participatie aan de publieke zaak en vrijheid van vereniging veilig stelt in een vrije samenleving. Door te spreken van een constitutieve waarde geeft hij al aan dat privacy en democratie niet in een puur instrumentele

27 Het voorbeeld is mijn variant en verdere uitwerking van een voorbeeld van Zarsky (2002-2003). Ook Zarsky meent dat de gevaren van profiling kunnen worden samengevat als inbreuk op de autonomie en afbreuk aan non-discriminatie. Lessig zelf signaleerde dit soort gevaren al in Lessig 1999, hoofdstuk 11 (zonder ze echter op deze manier samen te vatten).

28 Over de invloed van profileringtechnieken op rechtsstaat en democratie Hildebrandt 2008b. Over *behavioural advertising* zie Gray, Zeggane & Maxwell 2008.

doel-middel-verhouding staan.[29] Dat kan verklaren waarom commodificatie een hachelijke zaak is. Het methodologisch en normatief individualisme van Lessig veronderstelt dat doelen en middelen neutraal zijn en als onafhankelijke variabelen in het model passen. Voorzover privacy echter constitutief is voor een duurzame en vitale democratie, belichaamt privacy een waarde die niet restloos opgaat in haar instrumentaliteit; privacy is niet alleen middel maar ook doel in zichzelf.

Anderzijds kan rechtsstatelijke democratie niet goed begrepen worden zonder daar de privacy bij te betrekken; privacy maakt deel uit van de idee en de praktijk van de rechtsstaat. Privacy is geen 'natuurlijk' attribuut waar mensen mee geboren worden, maar een historisch artefact dat mede ten grondslag ligt aan de veerkracht en het weerstandsvermogen van de democratische rechtsstaat. Hoewel ik meen dat privacy wel degelijk een privaat belang is van individuele burgers, dat ook vóór het ontstaan van democratie en rechtsstaat en in andere typen samenlevingen een belangrijke rol speelt,[30] is het daarnaast een belangrijk *public good* dat een ander type bescherming vereist dan wanneer het als privaat belang geldt. De mate waarin privacy onderhandelbaar is, verschilt bijvoorbeeld naar gelang het als een persoonlijke preferentie wordt gezien dan wel als voorwaarde voor een duurzame democratie. In dat laatste geval zal er een ondergrens zijn aan de bevoegdheid om handel te drijven met de eigen privacy. Die ondergrens valt niet samen met de mate waarin privacy onvervreemdbaar zou moeten zijn. Onvervreemdbaarheid veronderstelt dat privacy een attribuut of bezitting is van een persoon. Privacy is echter een relationeel goed, of het nu om een privaat belang of een *public good* gaat. In beide gevallen gaat het niet zozeer om *concealment of information*, zoals bijvoorbeeld Posner meent,[31] maar om het vermogen te onderhandelen over de grenzen tussen zelf en omgeving, zoals bijvoorbeeld Nagel verwoordt in zijn pleidooi voor *reticence* in het tijdperk van *exposure*.[32]

In die zin is privacy tegelijk meer en minder dan gegevensbescherming. Hoewel het uitwisselen van gegevens wel een rol kan spelen bij het trekken van grenzen tussen zelf en omgeving, kan privacy niet zonder meer worden gereduceerd tot controle over de eigen persoonsgegevens. Privacy is meer, omdat controle over de eigen gegevens pas betekenis krijgt als het gebruikers in staat stelt om hun identiteit(en) te ontwikkelen in onderscheiden contexten, door te anticiperen op de manier waarop de omgeving de verstrekte of gelekte gegevens 'leest'. Privacy ziet bovendien op veel meer dan gedigitaliseerde gegevens, het gaat bij privacy ook om de fysieke en psychische

29 Voor een klassieke bespreking van de constitutieve verhouding tussen middel en doel, zie de Amerikaanse pragmatist Dewey 1967.

30 Altman 1975.

31 Posner 1981.

32 Dat betekent dat Thomas Nagel's betoog (1998) dat privacy een zekere *concealment of the self* mogelijk maakt en bescherming biedt tegen *exposure* wel hout snijdt. Anders dan Posner ontwikkelt Nagel een relationeel begrip van privacy.

ruimte die mensen elkaar al dan niet laten. In die zin heeft privacy ook te maken met de uitoefening van macht en hoewel het verwerken van persoonsgegevens daarmee verweven kan zijn, is er veel meer in het spel.

Privacy is ook minder, omdat gegevensbescherming niet alleen de privacy beoogt te beschermen maar ook het vrije verkeer van gegevens mogelijk wil maken.[33] Bij gegevensbescherming gaat het dan ook niet om wat Calabresi en Melamed een onvervreemdbaar recht noemen, want het staat individuen in beginsel vrij om hun persoonsgegevens in ruil voor toegang of korting uit te wisselen. Ott en Schaefer delen zelfs het algemene privacyrecht van art. 8 EVRM als persoonlijkheidsrecht in bij de aanspraken die vallen onder de eigendomsregels.[34] Daar is vanuit een interne kritiek wellicht nog wel wat tegen in te brengen, maar belangrijker is om de tegenstelling tussen individuele controle en statelijke interventie die eigen is aan het model van Calabresi en Melamed te toetsen aan de notie van privacy als *public good*. Het zou kunnen zijn dat privacy als *public good* buiten het model valt omdat er een andere visie op de verhouding tussen individu en staat aan ten grondslag ligt. Het gaat dan niet meer om marktfalen maar om de vraag naar de verhouding tussen markt en recht.

Conclusie: wederopstanding van privacy na een falende markt?

In dit hoofdstuk heb ik een interne kritiek beschreven op de commodificatie van privacy als rechtseconomische oplossing voor een falende markt voor persoonsgegevens. Daarnaast heb ik bouwstenen aangedragen voor een externe kritiek op de commodificatie, door de geschiktheid in twijfel te trekken van het rechtseconomisch model van Calabresi en Melamed voor de analyse van privacy in het tijdperk van profileringstechnologie. Doel van deze kritiek is niet om de rechtseconomische analyse als niet ter zake doende terzijde te schuiven. De interne kritiek laat juist zien hoe nuttig het is om vanuit het perspectief van het strategisch rationeel handelende individu te bezien of commodificatie van persoonsgegevens een effectieve bescherming van privacy biedt. De externe kritiek is erop gericht de beperkingen van het model van Calabresi en Melamed zichtbaar te maken, zonder het daarmee bij voorbaat ieder nut te ontzeggen.

Voor zover dat binnen het bestek van deze bijdrage mogelijk is, heb ik geprobeerd de vraag te beantwoorden 'in hoeverre nieuwe ICT infrastructuren tot een vorm van marktfalen kunnen leiden die de effectiviteit en de legitimiteit van rechtsregels aantast'. De manier waarop de bescherming van persoonsgegevens juridisch is georganiseerd, leidt tot marktfalen voor zover

33 Over het onderscheid tussen privacy en data protection zie Gutwirth & De Hert 2008. Mijn eigen visie wijkt daar licht van af, maar belangrijk is om de twee goed te onderscheiden, zie Hildebrandt 2008b.

34 Ott & Schaefer 2009.

de uitwisseling van gegevens plaatsvindt in een omgeving waar volstrekt onzichtbaar is wat door wie met die gegevens wordt gedaan. Daarbij is het vooral van belang dat het data-subject niet weet met welke profielen haar data 'matchen' en tot welke in- en uitsluiting dat kan leiden. Omdat marktfalen in geval van eigendomsregels de rechtsregels hun effectiviteit ontneemt, zouden we volgens het schema van Calabresi en Melamed terug moeten vallen op aansprakelijkheidregels. Echter, de obstakels die tot marktfalen leiden bij eigendomsregels hebben een vergelijkbaar marktfalen tot gevolg in geval van aansprakelijkheidsregels. Burgers hebben immers geen zicht op de manier waarop hun gegevens binnen een bepaald profiel passen en wat de gevolgen daarvan zijn voor hun kredietwaardigheid, verzekeringspremie, kansen op de arbeidsmarkt, status als potentiële verdachte enzovoort en zo verder. Dit raakt niet alleen hun vermogen om ex ante vast te stellen wat hun gegevens hen waard zijn, maar maakt het bovendien moeilijk zo niet onmogelijk om ex post in te schatten, laat staan vast te stellen, welke schade zij mogelijk lijden door aantasting van hun aanspraak op privacy. Voor zover sprake is van marktfalen verliezen de regels van het gegevensbeschermingsrecht hun effectiviteit en daarmee ook hun legitimiteit. Voor zover het beschermende aspect van de Richtlijn Gegevensbescherming het instrumentele aspect legitimeert,[35] vervalt die legitimatie als de bescherming een bepaalde effectiviteitsdrempel niet haalt.

Een niet te onderschatten bijkomend probleem is dat privacy zich niet zonder betekenisverlies laat vertalen in termen van een *commodity* waarmee op een al dan niet falende markt kan worden gehandeld. Privacy is niet alleen een persoonlijk belang dat naar eigen inzicht kan worden verruild voor kortingen of toegang tot bepaalde diensten. Het is ook een relationeel rechtsgoed dat constitutief is voor een rechtsstatelijke democratie. Dat vraagt om een nadere analyse van de verhouding tussen markt, recht en technologie met bijzondere aandacht voor de complexe wisselwerking tussen de drie. Mijn eigen inschatting is dat falende markten baat kunnen hebben bij het inbouwen van adequate bescherming in de technische infrastructuur die de privacy bedreigt.[36] Het zou dan vooral moeten gaan om het ontwerpen van juridische transparantienormen die technisch verankerd worden en het aldus mogelijk maken om te anticiperen op de groepsprofielen waarmee individuele burgers worden beoordeeld. In rechtseconomische termen zou dit de transactiekosten aan de kant van degenen die worden geprofileerd terugdringen en het kennismonopolie van degenen die profiling-technologie gebruiken relativeren. Dat zou kunnen leiden tot een wederopstanding van de privacy, voorzover de burger beter kan inschatten welke persoonsgegevens zij wel of niet wil delen. In een wat bredere context zouden transparan-

35 Vanuit een relationele rechtsopvatting horen rechtsregels zowel een beschermende als een instrumentele dimensie te hebben. Cf. Foqué & 't Hart 1990.

36 Deze mogelijke oplossing gaat het bestek van deze bijdrage te buiten, zie verder Hildebrandt 2008d.

tierechten het machtsevenwicht tussen consument en aanbieders van diensten en tussen burger en overheid kunnen herstellen, waardoor de bescherming van privacy als *public good* weer mogelijk wordt.

Verwijzingen

Agre & Rotenberg 2001
P.E. Agre and M. Rotenberg (eds.) (2001), *Technology and Privacy: The New Landscape*, Cambridge, Massachusetts: MIT.

Altman 1975
I. Altman (1975), *The Environment and Social Behavior. Privacy Personal Space Territory Crowding*, Montery: Brooks/Cole.

Berlin 1958
I. Berlin (1969/1958), 'Two concepts of liberty', in: I. Berlin (ed.), *Four essays on liberty*, Oxford New York: Oxford University Press, p. 118-73

Bouckaert & Degryse 2006
J. Bouckaert and H. Degryse (2006), 'Opt in versus opt out: a free-entry analysis of privacy', *Tilburg University, Center for Economic Research,* Working paper nr. 1831.

Calabresi & Melamed 1972
G. Calabresi and A.D. Melamed (1972), 'Property Rules, Liability Rules and Inalienability: One View of the Cathedral', *Harvard Law Review,* 84, p. 1089-128.

Dewey 1967
J. Dewey (1967), 'The Logic of Judgements of Practice', in J.A. Boydston (ed.), *The Middle Works, 1899-1924* (8), Carbondale: Southern Illinois University Press.

Doderer 1953
H. von Doderer (1953), *Die Strudlhofstiege; oder, Melzer und die Tiefe der Jahre*, München: Biederstein Verlag, 908 p.

Foqué & 't Hart 1990
R. Foqué and A.C. 't Hart (1990), *Instrumentaliteit en rechtsbescherming*, Arnhem Antwerpen: Gouda Quint Kluwer Rechtswetenschappen.

Gray & Maxwell 2008
T. Gray, T. Zeggane and W. Maxwell (2008), 'US and EU Authorities Review Privacy Threats on Social Networking Sites', *Entertainment Law Review,* 19 (4), p. 69-74.

Gutwirth & De Hert 2008
S. Gutwirth and P. De Hert (2008), 'Regulating Profilng in a Democratic Constitutional State', in: M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Dordrecht: Springer, p. 271-302.

Hildebrandt 2006
M. Hildebrandt (2006), 'Privacy and Identity', in: Erik Claes, Antony Duff, and Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerpen – Oxford: Intersentia, p. 43-58.

Hildebrandt 2008
M. Hildebrandt and S. Gutwirth (eds.) (2008), *Profiling the European Citizen. Cross-disciplinary Perspectives*, Dordrecht: Springer.

Hildebrandt 2008a
Hildebrandt, M. (2008a), 'Profiling and the Rule of Law', *Identity in the Information Society*, (1) 1, p. 55-70, beschikbaar op http://www.springerlink.com/content/467887wtv826j6p4/fulltext.pdf.

Hildebrandt 2008b
M. Hildebrandt (2008b), 'Profiling and the identity of the European citizen', in M. Hildebrandt and S Gutwirth (eds.), Profiling the European citizen. Cross-discplinary perspectives, Dordrecht: Springer, p. 303-326.

Hildebrandt 2008c
M. Hildebrandt (2008c), 'Legal and technological normativity: more (and less) than twin sisters', (12) TECHNÉ (12) 3, p. 169-183.

Hildebrandt 2008d
M. Hildebrandt (2008d), Hildebrandt, Mireille (2008), 'A Vision of Ambient Law', in: R. Brownsword and K. Yeung (eds.), *Regulating Technologies*, Oxford: Hart, p. 175-191.

Hildebrandt 2009
M. Hildebrandt (ed.) (2009), *Behavioural Biometric Profiling and Transparency Enhancing Tools* (Brussels, the Future of Identity in the Information Society), beschikbaar op http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf.

Kerkmeester & Holzhauer 1999
H.O. Kerkmeester and R.W. Holzhauer (1999), *Rechtseconomische annotaties*, Kluwer.

Kerkmeester 1999
H.O. Kerkmeester (1999), 'Methodology: General', in Boudewijn Boeckaert and Gerrit De Geest (eds.), Encyclopedia of Law and Economics, Edward Elgar and the University of Ghent, p. 383-401.

Lessig 1999
L. Lessig (1999), *Code and other laws of cyberspace*, New York: Basic Books.

Lessig 2006
L. Lessig (2006), *Code Version 2.0*, New York: Basic Books.

Luft 2003
D.S. Luft (2003), *Eros and inwardness in Vienna: Weininger, Musil, Doderer*, Chicago: University of Chicago Press, xiv, 257 p.

Nagel 1998
T. Nagel (1998), 'Concealment and exposure', *Philosphy & Public Affairs,* 27 (1), p. 3-30.

Nissenbaum 2004
H. Nissenbaum (2004), 'Privacy as Contextual Integrity', Washington Law Review, 79, p. 119-158.

Odlyzko 2003
A. Odlyzko (2003), 'Privacy, economics, and price discrimination on the Internet', *Proceedings of the 5th international conference on Electronic commerce*, Pittsburgh, Pennsylvania: ACM.

Ott & Schaefer 2009
C. Ott and H.-B. Schaefer (2009), 'The dichotomy between property rules and liability rules: experiences from Germand law', *Erasmus Law Review,* 1 (3), p. 41-58.

Posner 1981
R.A. Posner (1981), 'The Economics of Privacy', *The American Economic Review,* 71 Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic Association (2), p. 405-409.

Prins 2004
J.E.J. Prins (2004), 'The Propertization of Personal Data and Identites', *Electronic Journal of Comparative Law* 8(3), available at http://www.ejcl.org/.

Solove 2002
D.J. Solove (2002), 'Conceptualizing Privacy', *California Law Review* 90, p. 1087-1156.

Schmidt 2007
A.H.J. Schmidt (2007), 'IT and the judiciary in the Netherlands – A state of affairs', *Computer Law & Security Reports* 23(3), p. 1-8.

Schorske 1981
C.E. Schorske (1981), *Fin-de-siècle Vienna: politics and culture*, 1st Vintage Book edn.; New York: Vintage Books, xxx, 378 p.

Tapscott 2009
D. Tapscott (2009), *Grown up digital: how the net generation is changing your world*, New York: McGraw-Hill xvi, 368 p.

Van Gunsteren 1992
H.R. van Gunsteren (1992), *Eigentijds burgerschap*, 's Gravenhage: Wetenschappelijke Raad voor het Regeringsbeleid.

Ulen 1999
T.S. Ulen (1999), 'Rational Choice Theory in Law and Economics', in: Jan Bouckaert and Gerrit De Geest (eds.), *Encyclopedia of Law and Economics*, Edward Elgar and the University of Ghent, p. 790-818.

Zarsky 2002
T.Z. Zarsky (2002-2003), '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion', *Yale Journal of Law & Technology* 5(4), p. 17-47.

Digital Diversity: Protecting Identities Instead of Individual Data

Corien Prins■

Introduction

Today, in our already information-intensive society, tailored and individualized services and platforms appear to gain unprecedented popularity. New technologies such as mobile location-based services, Radio Frequency Identification (RFID), smartcards, ambient technologies and biometrics support an ever greater capturing of customer and user information and allow for tailored services to the individual's needs and desires. Prospects to private as well as public sector organizations in applying these and other services are numerous: they range from the improvement of quality of service delivery and customer relations, to getting to know your customer and behavioural marketing, cost reduction and a more efficient achievement of organizational goals (e.g. profit, policy effectiveness), as well as effective enforcement of legal rights (e.g. copyright). In addition, a growing number of individual people benefit from new technology-based facilities. Individuals themselves e.g. create an unprecedented rich digital source of information by teaming up with like-minded people to create social network sites and other web 2.0 applications. And, with mobile location-based services, people can trace other individuals with similar preferences that are present within the same geographical space of about 30 metres.

Insight knowledge about individual customers, patients or citizens provide commercial as well as public sector organizations with highly valuable information. Some organizations even join forces with groups of individuals. Illustrative is the well-known industry-patient partnership patientslikeme.com.[1] Personalized information also allows companies to address a large number of people on an individualised basis at the same time; not only within the territorial vicinity of the company or organization, but even globally. Web-based personalisation is one of the fastest growing segments of the digital economy, having spawned a multimillion-dollar industry.[2]

■ Corien Prins is professor of law and informatisation at Tilburg University with the Institute for Law, Technology, and Society (TILT), and Council member of the Dutch Scientific Council for Government Policy (WRR) in The Hague.

1 See http://pharmexec.findpharma.com/pharmexec/News+Analysis/UCB-Teams-with-PatientsLikeMe-to-Learn-What-Patien/ArticleStandard/Article/detail/604391.

2 For an analyses of the market value of social networks, see http://www.techcrunch.com/2008/06/23/modeling-the-real-market-value-of-social-networks/.

Some argue we find ourselves on the eve of a new type of market. In describing the characteristics of the new 'collaborative economy', Yochai Benkler claims that peer production and other forms of collaboration reverse earlier market strategies by breaking down the barrier between the market self and the social self.[3]

In short, personalization facilitated by technology seems to be an important, if not inevitable tool and strategy for private and even public organisations to deploy all kinds of individual-centric activities and services. The proliferation of personalized services, however, also triggers concerns. For the development may have profound effects on information and transaction relationships between individuals, organizations and/or communities in our society. At the heart of these concerns and effects is the very issue of user identification. It raises privacy problems as well as concerns with respect to inclusion and exclusion. Personalization may be a threat to a user's privacy because it provides companies and organizations with a powerful instrument to know in detail what an individual wants, who he or she is, whether his or her conduct or behaviour shows certain symptoms, and so forth. Also, personalization may be disturbing because it facilitates the selected provision to specific users only and may thus diminish certain preferences, differences and societal values. In a worst-case scenario, personalization may have larger societal and political consequences when it would shape the overall movement of information and expression within society. A discussion on how to react to the emergence of online personalization, should therefore not be limited to a discussion on privacy implications and how to protect individual data. Instead, it should be a discussion about essential interests such as autonomy, control, transparency and (digital) diversity.

In this contribution, I will be concentrating on some key effects of the emergence and growing popularity of online personalized services. Issues that will be addressed are privacy, inclusion and exclusion as well as transparency and control. As will become clear from this discussion, personalized services and the creation of digital identities are closely related. We should therefore recognize the crucial role of digital identities in the further development of online services. Based on an analyses of the afore-mentioned issues, I will be arguing that the focus of the discussion on enhanced privacy protection mechanisms should therefore move away from entitlements of single data. What we need are instruments to enhance the visibility of and our knowledge about how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes. A discussion of privacy protection in an information society characterized by personalized services should therefore be a discussion about protecting our digital identities instead of our individual personal data.

3 Benkler 2009.

Property rights in personal data

As said, the development of personalization services will have important effects on privacy. What raises problems in relation to privacy is first the potential for further use and sometimes abuse of the detailed and rich knowledge on individuals. Connecting and (re)selling data sources has become a highly profitable business and certain companies may compromise users' privacy for profits. In the meantime, studies have shown that consumers and citizens are under certain conditions particular about the type of information they are willing to provide in return for personalized content.[4] However, most consumers hardly understand how personalization technologies actually work and have ample opportunity for control over the dissemination of their personal or behavioural information. Various personalization services deploy hidden instruments to track and trace users and thus consumers are usually not aware of their data and preferences being collected.

With the growing importance of personalization services, it is clear that ownership rights in personal data and individual user profiles become the key instrument in realizing returns on the investment. As early as October 2003, Jupiter Research study found that to develop and deploy a personalized website can cost four or more times than operating a comparable dynamic website.[5] Thus, a healthy business model for personalized services requires that the key asset, i.e. the personalized information, 'belongs' to the organization that has configured its system to allow users to perform personalization. But who then owns and thus may control personal data? Who owns our personal Google-profile or any of the profiles created in one of the many popular social networks? At first glance, day-to-day practice appears to indicate that the data controller, i.e. the organization that collected the data for personalization purposes, holds some sort of property right in these data. Several bankruptcy cases in the early years of this decennium have shown that databases containing personal data and consumer profiles are a highly valuable asset.[6] With the at that time downturn in the e-business market, various companies decided to sell their customer data as a means of generating cash flow and silencing creditors. In many other situations, customer lists and databases appeared a highly valuable asset as well. Large amounts of personal data changed hands or 'ownership', as part of merger-

4 For an overview of studies on privacy attitudes, see: http://www.rogerclarke.com/DV/Surveys.html.

5 Mentioned in: Daniel J. Greenwood, *The "Person" in Personalization*, paper presented at the International Expert Meeting on Issues in Online Personalization, Oxford Internet Institute, Oxford, 5 March 2004.

6 See e.g. the discussion and court proceedings on whether the bankrupt US Internet retailer Toysmart could sell the personal details of its former customers to the highest bidder. See: L. Enos, "Deal Afoot to Destroy Toysmart Database", *E-Commerce Times*, January 10, 2001.

acquisitions, reorganizations and other strategic company movements.[7] More recently, the takeover of various companies that have made their business in the online world testifies of what is at stake when it comes to the acquisition of subscriber, user and customer lists.[8] Companies may even actually believe that they have ownership rights in the personal data compilations because the law itself offers indications for such a position. In addition to protection under the regime of trade secrets, businesses that have invested in the collection and compilation of personal data are granted exclusive rights under the European Directive on database protection.

In line with the debate on ownership in personal data, commentators have argued that it is the individual who should own the information about himself and decide how the data are being used and by whom. In this view, ownership and control of identity must belong to the person identified. In the 1990's, creating property rights in personal data was thought to be a plausible way of securing interests in our modern technology-based era. Academics in the area of law and economics, argued that by granting individuals a property right in their personal data, they could sell or license their data and thus determine how much information they share with others and at what price.[9] In looking at privacy as a problem of social cost, commentators felt that the accepted conception of privacy was an ineffectual paradigm and that, if we want strong privacy protection, we must replace it with the more powerful instrument of a property right.[10] By vesting a property right in individuals, businesses would be forced to internalize the costs associated with the collection and processing of personal data.

At present, businesses gain the full benefit of using personal information, but do not bear the societal costs: personal data can usually be collected for free, and with the advent of new technologies, it has become much easier and cheaper to gather and use data of individuals. Once companies have to internalize the societal costs associated with using personal data, they would perhaps be less inclined to gather and compile personal data than they currently do. This, in turn, would enhance levels of privacy. Moreover, "placing some cost burden on processors and users of personal data promotes greater respect for individual dignity than requiring individuals to purchase their privacy against a default rule of no-privacy".[11] Thus, the costs are no longer only borne by those individuals who both desire privacy and can afford it, but instead by society as a whole.[12]

Others however warned for what they called the failure of licensing and thus the failure of a property-based protection model. Individuals will gladly consent to certain personalized uses of their data or user profile. Or they

7 Gauthronet 2001.
8 Gauthronet 2001.
9 Laudon 1996.
10 Sholtz 2000.
11 Cohen 2000.
12 Cohen 2000, p.1390.

may not wish to consent or are reluctant to consent, but are nevertheless forced to consent because without use-rights the company is not willing to provide certain services. In other words, bargaining seems impossible or consumers have no effective choice in the matter. To do any good, the property right might have to be inalienable and waivable only in certain limited circumstances (comparable to the moral rights under intellectual property law).[13] But even if data subjects would be willing to permit the use of their personal data, actually licensing all the necessary data will be costly, inconvenient, and time-consuming which in the end could mean that companies no longer have the adequate incentive to offer personalized services.

Technology as a solution

More recently, an alternative proposal that has been suggested: to use technology to create and sustain the conditions for personalized choices of the data used. Certain digital technologies, such as privacy enhancing technologies and 'technologies of identity' as described by Phil Agre[14], make it possible to prevent personal data from being collected at all. Also, technology can provide the means for encoding personal data with detailed information about restrictions on use, exchange and further processing. In line with this argument, Cohen contended that the same technologies that enable personalized distributed rights-management in the area of copyrighted works might enable the creation of privacy protection that travels with data – obviating the need for continual negotiation of terms, but at the same time redistributing "costs" away from individuals who are data subjects.[15]

Zittrain, describing the use of personal data in the medical arena, made the claim that 'trusted' architectures (i.e. hardware and software that take note of various entitlements to personal data they store and automatically enforce those entitlements) could help negotiate the allocation of use rights to personal data.[16] Personalization techniques could thus balance the legitimate interests of companies and organizations who wish to use data and the interests of individuals who 'produce' these data for the very reason that personalization techniques increase the ability to uphold and enforce rights and obligations. The inclusion in techniques of certain default rules that restrict the collection of personal data without individual consent could provide individuals with a tool to control information about themselves, permitting them to waive it, but setting default contract terms that help shape the licensing practice that may thus develop.

13 For an overview of the discussion: Samuelson 2000; Lemley 2000; Prins 2006.
14 Agre 1997.
15 Cohen 2000.
16 Zittrain 2002.

Thus, in line with what has been contended by Samuelson, this approach would not focus on granting individuals a law-based property right in their personal data, but rather on restricting or conditioning the use and alienability of these data once obtained by a specific compiler. By now, several open standards for so-called identity management have been developed, based on ownership models and rooted in the concepts of the individual's autonomy and sovereignty.[17]

Inclusion and Exclusion

A consideration closely related to the use of personal data and privacy protection is the inclusion and exclusion of individuals when it comes to certain personalized services. Clearly, the deployment of personalization applications will facilitate the widespread monitoring of what people read, view, or listen to. By using personalization services their proprietors will potentially have what Philip Agre referred to ten years ago as "God's-eye view of the world."[18] To the extent that personalization applications allow the user to be tracked easily and thoroughly, it is a simple matter to limit the scope of certain facilities to a tightly controlled group of consumers. For example, personalization services will facilitate the selected provision of access to certain services only to consumers who live in preferred zip codes, or have certain levels of income. Also, personalization services seem well-suited to choose who will be allowed to view or read a particular work and who will not. But personalization is not only about inclusion or exclusion of certain services. It will also facilitate price-discrimination – that is, proprietors of services can ask different consumers to pay different prices.

Is this inclusion or exclusion good or bad? It could be argued that inclusion or exclusion is economically useful, because it will do a better job of getting the right information (commercial as well as public sector information) to the right persons. In the absence of personalization techniques, organizations must make wasteful investments in distributing information to consumers of whom they do not know whether they appreciate this information. Thus, techniques that facilitate inclusion and exclusion may be especially useful to accommodate the varying preferences of consumers and citizens. As such, personalization is a good way to achieve an efficient market. Personalization, further, provides an efficient and effective tool with which companies can monitor who is granted access to certain works and who is not. By using personalization techniques, content-producers obtain control over the uses of a variety of legally protected works and the techniques will thus allow providers to choose who will be allowed to view or read particular works. The control facilitated by personalization techniques e.g. will

17 See, e.g.: www.prime-eu.org; http://www.projectliberty.org; http://ecitizen.mit.edu.
18 Agre 1999.

increase the copyright owners ability to uphold and enforce their copyrights. Also, one could argue that personalization techniques would offer consumers a better privacy perspective because it provides them with the power to restrict the collection of personal data.

Of course, one might argue that inclusion and exclusion of (access to) certain services is essentially nothing new and as such there is nothing bad to it. Today, consumers and citizens behaviour is also predetermined by their attachment to a group, their cultural or societal position or predisposition, etc. What is different however with the new dimension of personalization services is that it may force individuals into restraining, one-dimensional models, based on the criteria set by technology and of those who own and apply the technology.[19] With commercial personalization services, the myriad of individual differences is reduced to one or a few consuming categories. And on the basis of these few categories everything has been said about their preferences, character, life-style, and so forth.

But also from other perspectives it seems disturbing that personalization offers the ability to diminish certain preferences, differences and values. For example an exclusion of access to and the use of information and copyrighted works (music, books, films) puts the values of free speech and information under pressure. What is more, personalization may have larger societal and political consequences when it would shape the overall movement of information and expression within society. Free citizens are the cornerstone of democratic constitutional societies. In an ultimate scenario personalization services could put cultural and social diversity at stake: one political or religious message is to dominate the whole discourse. In other words, personalization may have serious consequences when it means that behaviour is manipulated, freedom of self-determination and personal autonomy is limited and societal freedom is eroded. Personalization as such is nothing new, since inclusion and exclusion are part of our daily life. However, the control facilitated by personalization services may potentially have (serious) consequences for freedom of speech, freedom of consuming and freedom of conscience, as well as the public interest of cultural and political diversity.

A discussion on the pros and cons of personalization from the inclusion and exclusion perspective could be held along the lines of the concepts of autonomy and paternalism. The concept of autonomy has been described in many different terms and values. Feinberg described autonomy as: "The kernel of the idea of autonomy is the right to make choices and decisions… put compendiously, the most basic autonomy right is the right to decide how to live one's life."[20] Thus, to act as an autonomous individual, freedom and respect in making choices is essential. To be able to make choices, an individual:

19 Van der Hof & Prins 2008.
20 Feinberg 1986.

- must be free from unwarranted interference by others (non-interference);
- must be able to make choices (capacity);
- must be able to make meaningful choices, i.e. understanding the relevant information (informed).[21]

Of course, unchallenged exercises of autonomy are not tolerated in all situations. For example, a person will not be entirely free to make his own choice in a situation in which the exercise of such choice will directly harm third persons. Also, for certain reasons third persons (private as well as public bodies and persons) may decide what is best for others. This concept of paternalism is based on the presumption that in certain situations people, organizations or governments may and even must decide for others what is in their best interest.[22]

The key challenge with the new opportunities of personalization will in the end be to find a balance between autonomy and paternalism. But what is crucial in realizing this balance is that individuals will are at least be given the instruments to enhance the visibility of and their knowledge about how their personal data are used and combined, on the basis of what they are typified, by whom and for what purposes. In line with Nissenbaum's theory of contextual integrity, "it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances."[23]

The key problem we face with the advent of personalized techniques is, quoting Mireille Hildebrandt: "an abundance of co-relatable data and the availability of relatively cheap technologies to construct personalized knowledge out of the data, create new possibilities to manipulate people into behaviour without providing with adequate feedback of how their data have been used (…) (T)his may lead to major shifts in power relations between individual citizens on the one hand and commercial or governmental organizations on the other. The crucial issue is not abuse, but the fact that we have no effective means to know whether and when profiles are used or abused".[24] This brings us to a third consideration of importance for an analysis of privacy and personalization: transparency and quality.

21 Laurie 2002.
22 See in detail on paternalism: Dworkin 1988.
23 Nissenbaum 2004.
24 Hildebrandt 2008.

Transparency and Quality

Both concepts reveal themselves in different aspects and on different levels of personalized services; however, these concepts are also correlated to a large extent in the sense that both contribute to each other. At a practical level several requirements can be discussed when it comes to transparency and quality. First of all, transparency with respect to the personalization process itself is of importance, including information as to way the personalization process works, the different configuration options or features which are included in the service etc. Moreover, the purpose(s) for which personal data and related information (e.g., log-in information, transaction histories, and localization information) is used within the personalized service or beyond should be transparent to users. Users should also be aware of the way in which their personalized identity is created and used by the personalized service provider (e.g. what methods are used to create identities and in what context(s) are personal data used and viewed). In addition, users should be informed of the way in which personal data can be accessed, reviewed and updated and the security of this process. Furthermore, users should know if and how (e.g., by sending an e-mail to a clearly specified address) they can restrict or object to (commercial) use of their personal and other data. Such information can, e.g., be provided in a privacy statement on the website of the service provider. Privacy statements should be complete and easy to access and understand. From a quality perspective it is also important that the security of personal and other data is adequate and that usability of security and more specifically authentication mechanisms is optimized. Usability across different personalized services can, for instance, be addressed by implementing what is called single sign-on authentication mechanisms.

Transparency also demands that users can assess the objectivity, quality and reliability of information provided to them through the personalized process. More than one business or other organization may be involved in providing users with a variety of personalized services and information and, particularly, where there is a lock-in situation in which service providers determine the information to be received by individual users, users should be able to trace the origin of information in order to be (better) able to determine the quality, objectivity and reliability of such information.[25]

Personalization and Identification

Having discussed the implications of personalization for privacy, inclusion/exclusion and transparency/quality, we finally touch upon the core challenge of this new development, i.e. the implications of personalization for

25 Vedder & Wachbroit 2003.

the way our lives are typified and our identities are constructed by means of the new technological application.

As was mentioned, a key feature of personalization is that individuals are given new ways to present and profile themselves – depending on the specifics of the context – in certain roles or 'identities'. The earlier-mentioned 'patientslikeme' initiative is only one of many examples that show that people act as a certain type of citizen, consumer, patient, voter, et cetera. The thus growing importance of the context-specific concept of online identity raises challenging new questions as regards on the role as well as status of identity and identification. To what extent does the concept of 'online identity' get a different meaning compared to identity construction in offline relationships? Where exactly in social networks lie the boundaries between online identities and a person's 'own' or 'real' identity? When exactly, i.e. given what conditions, may a certain fragmented or segmented aspect of a person's identity be considered an adequate representation of the 'real' person behind that identity?[26]

If online personalization will become in part tantamount to the online identity of a person, then this state of affairs may raise the question who may control the use of the data behind this identity as well as the identity itself. Can an online identity be owned and if yes, in whom should such ownership be vested? Finally, new means of self-presentation also raises questions related to the reliability of identities and the implications of possible fraud with identities. To what extent can users 'play' with their online identity or virtual 'reputation', use their online reputation as a certain type of 'security', mislead organizations with a claimed online identity, et cetera?

Another way to consider the relationship between the public domain and the commodification of personal data is by focusing not so much on the individual data, but on the *effects* of the present-day technologies, in particular the almost limitless surveillance capacities of new technologies, such as location-based systems, radio frequency identifiers (RFIDs) and online personalization instruments. In a sense, these surveillance techniques require that we shift our attention from individual sets of personal data toward the statistical models, profiles and the algorithms with which individuals are assigned to a certain group or 'identity'. For these models and algorithms are privately owned, and thus unavailable for public contestation. But the interests of personal data protection seem to require that they are made known to the public and thus are part of the public domain. Let me discuss this point in some more detail.

Our behaviour in the 'public domain' is increasingly monitored, captured, stored, used and analyzed to become privately-owned knowledge about people, their habits and social identity. Indeed, the term *personal data* protection may loose its significance once we acknowledge this trend toward a commodification of *identities and behaviour*. It is this trend that is lacking in

26 Leenes 2008.

the present debate on personal data protection. Personal data are not used and processed anew and in isolation each time a company acquires a set of personal data. In contemporary society, 'useful' information and knowledge goes beyond the individual exchange of a set of personal data. In 'giving' his or her personal data to a certain organization, the individual does not provide these data for use in an 'objective' context. Today, the use and thus 'value' of personal data cannot be seen apart from the specifics of the context within which these data are used. Processing of personal data occurs within, and is often structured by, social, economic and institutional settings, as is e.g. shown by Phillips in his analysis of the implications ubiquitous computing developments.[27]

Thus, the question is not so much *whether* personal data are processed. They always are and will be, whether for legitimate or unlawful purposes. It is an illusion to think that vesting a property right in personal data will limit the use of personal data. Rather, the problem is *how* personal data are processed, in what context, and towards what end. Therefore, the focus of the discussion should move away from entitlements of single data. What we need are instruments to enhance the visibility of and our knowledge about how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes.

A similar suggestion is for other reasons made by academics in the area of marketing.[28] This is a much more fundamental issue which cannot be tackled by vesting for example a property right in individual data. To illustrate this argument, I would like to point towards another new technology-based development: ubiquitous computing environments. Ubiquitous computing will create a context-aware environment in which, by means of the coordinated use of databases, sensors, micro-devices and software agents, numerous systems scans our environment for data and serve us with particular information, based on certain notions about what is appropriate for us as unique individual persons given the particulars of daily life and context. Some thus argue that ubiquitous systems will to a large extent structure and determine our daily life, mediating our identity, social relations and social power. Not only will our homes and working offices become public places, but our social identities as well.

Conclusion

Given not only the development of personalization but also other developments in the area of 'pervasive' computing, the discussion about protecting personal data must become a discussion about how individuals are typified (upon what social ontology, with what goal?) and who has the instruments

27 Phillips 2005.
28 Zwick & Dholakia 2004.

and power to do so. In this sense, personal data protection is not about something (i.e. personal data) that can be owned. It has everything to do with position, social ordering, roles, individual status and freedom. Therefore, protection of personal data in our present-day society assumes the capability to know and to control about how our identities are constructed. It requires the availability of instruments to enable awareness of the context in which personal data are used and to monitor the data-impression that individuals are exhibiting to others.[29] In other words, the discussion on the future of privacy protection must be a discussion on whether, and to what extent, the statistical models, profiles and algorithms that are used to generate knowledge about our individual behavior, social and economic position, as well as personal interests, are transparent and controllable. And in the end, it is precisely this discussion that is essential in the interest of societal values such as autonomy, control, transparency and (digital) diversity. Almost ten years ago, Vedder advocated the introduction of the new concept of 'categorical privacy'. This concept is largely based on the concept of individual privacy, but including privacy as regards information that is no longer identifiable to persons, because such information may still have possibly negative consequences for group members.[30]

But perhaps the time has come to take it one step further: to call for the recognition of a sui generis right, namely the 'right to identity'.[31] By making explicit and 'legal' the value of identity, this new basic right would provide a better-equipped instrument to balance the private and public interests at stake than only the rights to privacy or liberty. Others, however, believe that the negative aspect of freedom – the maintenance of legal, administrative, political and ethical opacity – is and should remain quintessential. Issues pertaining to 'identity' or to be protected by normative prohibitions of interferences such as foreseen by privacy and some aspects of data protection law, but also by freedom of conscience and speech, physical integrity, etc.[32] It is too early to decide what road to follow. What is however clear is that the focus of the discussion on the future of privacy protection should move away from entitlements of single data. What we need are instruments to enhance the visibility of and our knowledge about how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes. A discussion of privacy protection in a world of internet of things, ambient intelligence, social networks and convergence should therefore be a discussion about protecting our virtual identities and the interests behind this concept, instead of our individual personal data.

29 Nguyen & Mynatt 2002.
30 Vedder 2000.
31 Prins 2007; De Hert 2008.
32 Gutwirth 2009.

References

Agre 1997
Ph.E. Agre, 'Beyond the Mirror World: Privacy and the Representational Practices of Computing', in: *Technology and Privacy: The New Landscape* (Philip E. Agre, Marc Rotenberg, eds.), 1997, p. 29.

Agre 1999
Ph.E. Agre, 'The Architecture of Identity: Embedding Privacy in Market Institutions', 2 *Info. Comm. And Soc'y* 1 (Spring 1999). Available at: http://www.infosoc.co.uk/00105/feature.htm.

Benkler 2009
J. Benkler, 'The Collaborative Company', available at http://whatmatters.mckinseydigital.com/internet/the-collaborative-company.

Cohen 2000
J.E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object', 52 *Stanford Law Review* May 2000, p. 1390.

Dworkin 1988
R. Dworkin, *The Theory and Practice of Autonomy*, Cambridge: Cambridge University Press, 1988.

Feinberg 1986
J. Feinberg, *Harm to Self*, Oxford: Oxford University Press, 1986, p. 54.

Gauthronet 2001
S. Gauthronet, 'The future of personal data in the framework of Company reorganisations', *23rd International Conference of Data Protection Commissioners*, Paris September 2001.

Gutwirth 2009
S. Gutwirth, 'Beyond Identity?', *IDIS – Identity in the information society* 1.1 (2009): http://works.bepress.com/cgi/viewcontent.cgi?article=1014&context=serge_gutwirth.

De Hert 2008
P. De Hert, 'A right to identity to face the Internet of Things', 21 p. at http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf.

Hildebrandt 2008
M. Hildebrandt, 'Profiling and the Identity of the European citizen', In: M. Hildebrandt, S. Gutwirth S (eds.), *Profiling the European Citizen. Cross-disciplinary perspectives*, Springer 2008.

Van der Hof & Prins 2008
S. van der Hof and J.E.J. Prins, 'Personalisation and Its Influence on Identities, Behaviour and Social Values', In: M. Hildebrandt, S. Gutwirht (eds.), *Profiling the European Citizen, Cross-diciplinary perspectives*, Springer 2008.

Laudon 1996
K.C. Laudon, 'Markets and Privacy', *Communications of the ACM*, vol. 39, no. 9 1996, p. 104.

Laurie 2002
G. Laurie, *Genetic Privacy. A Challenge to Medico-Legal Norms*, Cambridge: Cambridge University Press, 2002, p. 186-187.

Leenes 2008
R.E. Leenes, 'Do they know me? – Deconstructing identifiability', University of Ottawa Law & Technology Journal, 4(1) 2008.

Lemley
M.A. Lemley, 'Private Property', 52 *Stanford Law Review* 1545 (2000).

Nguyen & Mynatt 2002
D.H. Nguyen and E.D. Mynatt, 'Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems', *Georgia Institute of Technology Technical Report* (2002) Available at: http://quixotic.cc.gt.atl.ga.us/~dnguyen/writings/PrivacyMirrors.pdf.

Nissenbaum 2004
H. Nissenbaum, 'Privacy as Contextual Integrity', 79 *Washington Law Review* , p. 119 (2004).

Phillips 2005
D.J. Phillips, 'From Privacy to Visibility: Context, Identity, and Power in Ubiquitous Computing Environments', *Social Text* 23(2), 2005.

Prins 2007
J.E.J. Prins, 'Een recht op identiteit', *Nederlands Juristenblad*, 82(14): p. 849 (2007).

Samuelson 2000
P. Samuelson, 'Privacy as Intellectual Property', 52 *Stanford Law Review* 1125 (2000).

Sholtz 2000
Paul Sholtz, 'The Economics of Personal Information Exchange', *First Monday,* volume 5, number 9 (September 2000). Available at: http://firstmonday.org/issues/issue5_9/sholtz/.

Vedder 2000
A. Vedder, 'Medical Data, New Information Technologies and the Need for Normative Principles Other Than Privacy Rules', *Law and Medicine* (eds. M. Freeman, A. Lewis), Oxford: Oxford University Press, 2000, p. 441-459

Vedder & Wachbroit 2003
A. Vedder and R.S. Wachbroit, 'Reliability of information on the Internet: Some distinctions', *Ethics and Information Technology, 5*, 2003, p. 211-215.

Volokh 2000
E. Volokh, 'Personalization and Privacy', *Communications of the ACM*, vol. 43, no. 8 2000. Available at: http://www1.law.ucla.edu/~volokh/acm.htm

Zittrain 2000
J. Zittrain, 'What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication', 52 *Stanford Law Review* 1201 (2000).

Zwick & Dholakia 2004
D. Zwick and N. Dholakia, 'Whose Identity is it Anyway? Consumer Representation in the Age of Database Marketing', *Journal of Macromarketing*, June 2004; 24, p. 41.

Privacy and Singularity: little ground for optimism?

Bart Schermer■

Introduction

During one of the many animated lunchtime discussions at eLaw@Leiden, the topic was the notion of a technological Singularity. Singularity is a theoretical point in the future of mankind where we will be able to create smarter-than-human-intelligence through the use of technologies such as artificial intelligence and nanotechnology.[1] Being a techno-optimist myself, I feel this is an exciting prospect. Professor Schmidt however, saw cause for great concern instead of ground for optimism.

Much like Asimov, who noted that science gathers knowledge faster than society gathers wisdom, Schmidt argues that society will be unable to cope with the problems of smarter-than-human intelligence. Apart from the obvious problems of a smarter-than-human mind setting itself to nefarious purposes, and the possibility of an immense (digital) divide between normal humans and 'smarter-than-humans', professor Schmidt argues that Singularity may also threaten the legitimacy of our law systems.[2]

While in general I feel Singularity (if it ever occurs) will be beneficial for mankind, I must agree with professor Schmidt that it will pose serious problems for the working and legitimacy of our legal system(s). In this article I shall look at a specific cause for concern: the protection of the right to privacy in (near) Singularity societies. But before I discuss the problem statement of this article, I shall first describe more in depth what we mean by a technological Singularity.

Countdown to Singularity

Technological Singularity is a concept introduced by science fiction author Vernor Vinge and expanded on by many authors and researchers, most notably Ray Kurzweil.[3] In examining the history of human evolution and technology, Vinge and Kurzweil observed that the pace of technological development is growing at an exponential rate. They argue that in the near future

---

■ Bart Schermer is partner of Considerati, and assistant professor at the Leiden Law Faculty.

1 Kurzweil 2005.

2 Schmidt 2009.

3 Vinge 1993, Kurzweil 1990, 1999 and 2005.

(some thirty to forty years from now) our technology will have evolved so far, that we will have the technological capabilities to create smarter-than-human intelligence. This point in time is called Singularity.

Singularity will come about as a result of the convergence of *N*anotechnology, *B*iotechnology, *I*nformation technology and insights from *C*ognitive sciences (NBIC). In particular, the advent of 'strong' artificial intelligence will enable us to surpass our current physical and mental boundaries. For instance by using nanobots we can heal our bodies and slow the aging process, by using sophisticated brainscanning techniques we can map our brain functions for replication in a computer, and through brain-machine interfaces we can enhance our brains with technology. These ideas have led 'Singulatarians' such as Vinge and Kurzweil to believe that we will be either surpassed by a smarter-than-human intelligence or gradually transform into a post-human species. This idea of post- or transhumanism is as appealing as it is disturbing. Though it is my personal opinion that the controversial theories set forth by Kurzweil on self-replicating nanobots, the emergence of strong artificial intelligence and possibly even the ability to copy our conscience into a machine, are plausible, we cannot hope to verify or falsify them at this point in time. Nonetheless, since Singulatarian ideas seem grounded in science, they deserve careful study, most importantly because they will pose significant ethical and societal challenges.

Unfortunately, it is impossible to discuss the ethical and societal implications of Singularity for the simple reason we cannot begin to comprehend what the advent of smarter-than-human intelligence will mean. Actually, this is the reason why Vinge called the advent of smarter-than-human intelligence 'the Singularity' in the first place. Much like Singularity at the heart of a black hole, where the normal rules of physics no longer apply, we cannot see beyond the technological Singularity point because we are not as smart as post-humans and are thus enable to predict or comprehend their actions. Therefore, we will be unable to draw up an ethical framework with accompanying rules and regulations. What we can do however, is take a few steps back on the road to Singularity and focus on what I would like to call 'near Singularity' issues. While it is possible that Singularity will happen abruptly and unexpectedly (what is called 'the hard take off' scenario), I feel it is more likely that there will be steady improvements in technology, which in the end will lead to Singularity (what is called the 'soft take off' scenario).[4]

This does not mean that near Singularity issues likely to arise in a soft take off scenario will be any less profound. On the contrary, the technological changes and their societal effects will have a profound impact on our notions of autonomy, justice, equality, property, privacy *et cetera*. In this article I will focus on the possible effects of near Singularity technologies on the privacy of individuals. In particular I shall focus on the use of these technologies for surveillance purposes and discuss the following problem statement:

4 A view supported by Kurzweil, see: http://www.acceleratingfuture.com/peopleblog/2007/the-Singularity-a-hard-or-soft-takeoff/.

What are the effects on near-Singularity technologies on the privacy of individuals and how can we maintain the right to privacy in the face of these technologies?

To (try and) answer this problem statement I shall start by describing the impact of technology on privacy and how the law has responded to these challenges. Apart from a historical description I shall also describe how privacy will change in the coming years as a result of the ubiquitous computing paradigm and the rise of NBIC technologies. From there I shall describe what risks the use of these technologies may entail. From there I shall suggest possible solutions to counter the negative effects of these technologies.

A brief history of privacy … and its end

Research into primitive societies suggests that mankind has always needed some measure of privacy.[5] Throughout history, there has been a need for privacy in every society. However, what 'privacy' exactly entailed within these societies, is markedly different from our current notion of privacy. This is due to the fact that privacy, as a social institution, is defined by the realities of a particular place and time in history.[6] Changing attitudes towards the body, the house, the family, work and the State have always influenced the right to privacy. In the last hundred years or so, the rapid pace of technological development has been the driving force behind changing attitudes towards privacy. It is my opinion that in the next twenty years, technology will completely blur the boundaries between the public and the private, prompting us to rethink fundamentally our current notions and ideas about privacy.

1890-1928: cameras and wiretapping

At the end of the 19th century and the beginning of the twentieth century technological developments such as the invention of the snapshot camera and the increasing use of telecommunication networks (and the ability to tap these networks), gave rise to questions about a right to privacy. Justices Warren and Brandeis made the first explicit reference to a right to privacy in their renowned article *The Right to Privacy: The Implicit Made Explicit*.[7] Dismayed as they were by the practices of the gossip press which used *"new inventions and business methods"* to invade the *"sacred precinct of private and domestic life"*, Warren and Brandeis set out to explore the possibility and origin of a right to privacy. Warren and Brandeis came to the conclusion that the right to privacy formed part of the inviolate personality and saw it as: *"the next step that must be taken for the protection of the person, and for securing to the individual… …the right 'to be let alone'"*.[8]

5 Westin 1984.
6 Solove 2008.
7 Warren & Brandeis 1890.
8 Warren & Brandeis 1890.

It was the same Brandeis who in his dissenting opinion in the case of *Olmstead versus the United States* insisted on a person's right to private communications.[9] In *Olmstead* the United States Supreme Court held that tapping a phone line outside someone's house is not a violation of the right to privacy since no physical search or seizure is conducted. The decision in Olmstead came to be known as the 'trespass doctrine'. The trespass doctrine linked privacy to a physical place (*viz.* the house), rather than to the communication itself. It was not until *Katz v. the United States* that the trespass doctrine was reversed.[10] In this decision, the Supreme Court held that the legitimacy of interference into the personal sphere is determined by an individual's 'reasonable expectation of privacy'. The Court held that a person has a right to privacy with regards to his private conversations and therefore wiretapping is prohibited without a prior warrant.

1960-2010: the rise of information technology

The next technological development that had a major impact on privacy was the invention of the computer. In the course of some fifty years, our society has been transformed from an industrial society into an 'information society'. This transformation has been spearheaded by the development of the personal computer and the internet. The 'digital revolution' has had a profound impact on privacy and the conceptualisation of privacy as a human right.

The rise of automated recordkeeping in the sixties and seventies gave rise to a growing worry that automated data processing would pose a threat to basic human liberties. In the Netherlands for instance, there was active protest against the 1971 census (volkstelling), which was seen as an infringement of privacy. In 1973 the United States Department of Health, Education, and Welfare drafted a seminal report titled *Records, Computers and Rights of Citizens* that contained a *Code of Fair Information Practices*. These Fair Information Practices consisted of five basic principles to which every data processing party should adhere. They are: 1) no secret recordkeeping, 2) a duty to inform data subjects, 3) purpose binding, 4) the right to correct or amend information, and 5) quality of recordkeeping. These principles (together with the OECD Guidelines on privacy and personal data) formed the basis for personal data protection law.[11] For the purpose of this article it is important to note that while personal data protection law also applies to public entities, the application of surveillance technologies for law enforcement purposes is for the most part governed by the laws of criminal procedure.

We may conclude that privacy as a 'physical state' (i.e. the absence of information about, or interaction with an individual) receded as our society

9 Olmstead v. the United States, 277 U.S. 438, 478 (1928).

10 Katz v. the United States, 389 U.S. 347, 351 (1967).

11 *Recommendation Concerning and Guidelines Governing the Protection of Privacy and the Transborder Flow of Personal Data,* Organisation for Economic Cooperation and Development (OECD), 1980.

became more and more digitised and that data protection rules were put in place to remedy this situation.

2010-2020 Ubiquitous computing

We are currently in the early stages of the third phase of computer development, which Weiser and Brown have named the phase of 'ubiquitous computing'.[12] In the first phase of computing (the mainframe era), when computing power was still scarce, many people shared one computer (the mainframe). In the second phase (the PC era), computing power became so cheap, that (almost) every person could own a computer. Now, after a transition phase in which computers became connected through the internet, computing power is so cheap that countless computers can be embedded in our physical world. More or less, this is a reversal of the first phase: instead of many people sharing a computer, many computers 'share' a single person.

The era of ubiquitous computing will greatly benefit mankind: our environment will be able to respond intelligently to our presence in the physical space. This 'ambient intelligence' will make our lives easier, more efficient and safer.[13] As Weiser pointed out in his seminal article on ubiquitous computing, computing will recede to the background of our lives, ushering in an age of calm technology where computers aid and support us in an unobtrusive manner.[14]

While ubiquitous computing has the potential to greatly enhance our lives, it also brings with it significant risks for the (informational) privacy of individuals. In order to function properly and aid persons in their daily lives, the ambient intelligent environment has to process huge amounts of (personal) data. These data are not only gathered and accessed in 'cyberspace', they are for the most part gathered in the physical world and have their effects there as well, leading to potential breaches of informational privacy that are currently not possible. This threat is compounded by the fact that the design philosophy of ubiquitous computing is to make computing unobtrusive and invisible. So, while the possibilities for gathering personal data will be enhanced, transparency will greatly diminish.

2020-2040 The rise of NBIC technologies

According to Kurzweil, the convergence of nanotechnology, biotechnology, information technology (in particular artificial intelligence), and insights from the cognitive sciences will ultimately bring about Singularity. But even before we reach the Singularity point, NBIC technologies, by themselves or in convergence, will significantly impact society and our notions of privacy within that society.[15]

12 Weiser & Brown 1996.
13 Aarts, Harwig & Schuurmans 2002.
14 Weiser 1991.
15 Teeuw & Vedder 2008.

Nanotechnology for instance, will allow for the creation of extremely small surveillance equipment, which will be (almost) impossible to perceive with the naked eye. Apart from the size of surveillance equipment, advances in nanotechnology and information technology will vastly reduce the price of surveillance equipment in general, allowing for their implementation in every corner of our physical world.

Artificial intelligence will also have a great impact on privacy, in particular in relation to surveillance. Currently, the sheer amount of data gathered by surveillance equipment makes it nigh impossible to process effectively. The volume of data thus becomes too great to yield information and knowledge, a problem known as 'information overload'. Artificial intelligence promises to solve the problem of information overload. Moreover, advances in the area of data-mining will enable computers to 'predict' behaviour to an increasing extent. Furthermore, artificial intelligence will enable machines to identify objects, people and situations. Already facial recognition software is used to identify people. In the (near) future not only the accuracy of this software will increase, but also its capabilities will expand. For instance, intelligent cameras could scan a person's face and recognise the emotional state of that person (happy, angry, frightened). This information can then be used to make predictions about the behaviour of the person (is this person about the commit a violent act? Is this person behaving suspiciously?). Currently, human operators perform this task, but unlike their computer counterparts, humans cannot perform their tasks indefinitely. Artificial intelligence can thus overcome the basic limitations of human surveillance operators: 1) the inability to process vast amounts of data, and 2) limited attention span.

Another way in which NBIC technologies may threaten privacy is through their destructive capabilities. NBIC technologies have the potential to place the capabilities for mass destruction in the hands of individuals. Examples of this include nano-pathogens and destructive self-replicating nanobots. In turn, the proliferation of this new breed of weapons of mass destruction (or the threat of their proliferation) will prompt the need for increased surveillance.[16]

Nearing the Singularity

Ultimately, the convergence of NBIC technologies will bring us closer and closer to Singularity. The implications of (near)-Singularity technology applications for privacy, identity and personal autonomy will be so profound that our current 'pre-Singularity' privacy issues seem petty by comparison. In my opinion, two related technological developments that will have an immense impact on privacy are 1) brain-machine interfaces and 2) the reverse engineering of the brain.

The first technological development that will severely impact privacy is direct brain-machine interfacing. In order to interact more efficiently and

16 Schmidt 2009.

effectively with the technology that will surround us, we will increasingly use direct brain-machine interfaces. While this allows us to interact directly with machines in an intuitive manner (and on an almost subconscious level), it will also open up a link between the outside world and our brain. This means that our bodies and brain will no longer be a bastion of privacy and personal identity, but may become 'visible' for others. This will not only challenge notions of 'public' and 'private' but even challenge notions of 'individual' and 'collective'. So, while direct brain-machine interfaces will make us vastly more efficient and effective as human beings, they also bring with them significant new threats. Since brain-machine interfaces will work both ways, it might become possible to examine, visualise, and record a person's thoughts.

The second technological development will severely impact privacy is the 'reverse engineering' of the brain. Our knowledge on the human brain and the way in which it works continues to grow every day. Since the cognitive sciences are becoming increasingly adept at reverse engineering the human brain, it will become possible in the future – to some extent – to predict a person's behaviour. Already experiments are under way aimed at 'sensing' people's thoughts and feelings and it is likely that this trend will continue.[17]

What is the problem?

Currently, physical boundaries (walls, doors, the mind) and the limits of the human brain (e.g. fading memories, limited attention span) still provide us with some measure of privacy. However, these 'physical' boundaries will disappear once ubiquitous computing and NBIC technologies develop further. As mentioned before, even the mind may ultimately fall as a bastion of privacy. Therefore, privacy as a 'physical state' or 'physical reality' will disappear within the next twenty years.[18]

From the above we have seen that once privacy as a physical state disappears; regulations are put in place to recreate artificially the lost measure of privacy. So what is most interesting to note about the end of privacy is that the (possible) destruction of privacy in a certain instance creates the need for a *right to* privacy in that very same instance. Thus, while privacy as a physical property is disappearing, the need for a strong right to privacy is growing.

---

17 For instance, brainwave fingerprinting is a controversial forensic technology that can determine whether a person is lying on the basis of brainwave readings. In 2001, results from a brainwave fingerprint were admitted as evidence in a criminal case in the United States (Harrington v. State, Case No. PCCV 073247. Iowa District Court for Pottawattamie County, March 5, 2001).

18 See also: Schermer 2007.

In the following section, I shall describe why the right to privacy is so important, in particular in the age of ubiquitous computing and the following age of converging NBIC technologies. I argue that (the right to) privacy protects individuals and groups against the dangers of information asymmetry, paternalism, mistakes, and risk justice.

Information asymmetries
An important role of privacy (or a right to privacy) is preventing information asymmetries. When one party has intimate knowledge about another party as a result of surveillance, and the other party lacks a similar form of knowledge, the resulting information asymmetry creates a disturbance in the balance of power between these parties. The essence of surveillance is strengthening one's information position and as such surveillance creates information asymmetries almost by definition. Privacy has always acted as a natural barrier against information asymmetries, and in the absence of privacy, the right to privacy.

Paternalism
As technology becomes more effective at identifying and classifying human behaviour, the ability to influence our behaviour will grow. This in turn might lead to paternalism on the part of those in power. This is compounded by the fact that ubiquitous computing and NBIC technologies will enable us to influence the physical world in real time. An example of this can already be seen in England where CCTV operators not only observe the physical space, but also actively influence it. When someone displays behaviour that is considered inappropriate (littering, loitering, vandalism), CCTV operators call out to the person in question over a loudspeaker in an effort to alter their behaviour.

Mistakes
An issue with surveillance in general is that of false positives and false negatives. Since surveillance technology is not infallible (nor is it likely ever to become infallible), surveillance systems will also point out people who are in fact not criminals or terrorists at all (so-called false positives). The other problem is false negatives. Since most of the information on crime and terrorism that will guide surveillance is based on previous experiences and behaviour, new forms of deviant behaviour may escape attention. Since criminals and terrorists also innovate, they will employ new methods and use new attack vectors that are not detected by surveillance systems. False positives and false negatives may undermine the trust in surveillance systems, reducing the legitimacy of their use.

Risk Justice
The desire for risk-management and security in society has had a significant influence on the development of criminal law in recent years. It could be

said that we are moving towards a system of 'risk justice'.[19] In such a system the focus is not on solving crime and the legal punishment of criminal offences, but rather on the prevention of criminal offences and the reduction of risk. In both substantive criminal law and the law of criminal procedure we can clearly discern the development of risk justice. The scope of criminal liability for instance, has been greatly expanded over the past years, most notably in the area of terrorism. The increased criminal liability creates a 'gray area' in the law between merely thinking about a criminal act and actually committing one, where sweeping investigative powers and surveillance may be used nonetheless. One could argue that the change this has brought in our criminal justice system is that it is no longer just the actual criminal *act* that is punishable, but also the *thought* of a criminal has become punishable. It is clear that this situation can lead to mistakes and arbitrary decisions by law enforcement agencies that could threaten the privacy and liberty of individuals.

There is an interaction between the expansion of criminal liability (substantive criminal law), the use of investigative powers (criminal procedure) and the development of technologies that can sense and predict behaviour (surveillance technology). As these technologies become more advanced and the pressure to use them higher (for instance because individuals will have the power of mass destruction through weaponised NBIC technologies), substantive criminal law and the law of criminal procedure will open up possibilities for their use. In turn, this will lead to new efforts to develop advanced surveillance technologies.

Ultimately, it is not unthinkable that in a near Singularity society, the government could use the power of human-brain interfaces and reverse engineering of the brain to detect thoughts that are considered dangerous for the well-being of society. With brain-machine interfacing and increasing knowledge of the human brain, the idea of the persecution 'thought crimes' might thus become a reality.

The right to privacy

We may conclude that privacy as a 'physical reality' is quickly becoming a thing of the past. Privacy as a physical barrier to the observing gaze of others will no longer be a reality in a near-Singularity society. One could therefore argue that since the protection of privacy is a lost cause, we should abandon any hopes of retaining it all together. Scott Neally, CEO of Sun Microsystems, already stated in 1999 that: "you have zero privacy anyway, get over it".

But from the above we may also conclude that the erosion of privacy in near-Singularity societies brings with it such significant risks for individuals, that we will continue to need a right to privacy. So, we have to rely on

19 Moerings 2006.

the law (i.e. the right to privacy) for the protection of the interests (most notably individual liberty) hitherto protected by privacy in a physical sense. However, unlike physical barriers, rights, especially individual rights, can be revoked for the good of the community as a whole. In particular the destructive capabilities of NBIC technologies might trigger the need for greater, more infringing investigative powers. The problem of risk justice described in the previous paragraph seems to indicate that this is indeed the trend for the coming years.

The prospect of destructive NBIC technologies, the possibility of pervasive surveillance, the resulting disappearance of privacy, and the prospect of risk justice will severely challenge the legitimacy of our law systems. It is therefore important to find ways to strengthen the right to privacy and the interests it aims to protect.

The way forward

From the above we may conclude that while privacy as a physical barrier will disappear in the future, the *right to privacy* will become increasingly important. However, the fact that privacy will no longer be part of our physical reality but merely a 'legal concept' means that the right needs to be strengthened. Below I shall describe some measures aimed at strengthening and supporting the right to privacy.

Privacy by design
First of all, it is important to maintain whatever 'physical privacy' we can. To this end we must turn to 'privacy by design'. Privacy by design is a design philosophy whereby privacy rules are incorporated in the design of information system. By 'hardwiring' privacy rules into technology, unnecessary breaches of privacy are prevented. Means of reducing the availability of personal data through technology include anonimisation, authentication, and selective disclosure. Privacy by design is more effective than legal protection in itself, since rules can be broken or changed, whilst the design of an information system forces users to comply with the rules set forth in the design.

However, even when systems are designed with the principles of privacy by design in mind, it will be nigh impossible to maintain privacy as a physical barrier. In my opinion we must therefore also look towards other mechanisms for ensuring privacy.

Transparency and reciprocity (by design)
We have established that one of the main problems with surveillance is information asymmetry, a fact that will be compounded by the nature of ubiquitous computing in the next years and by NBIC technologies thereafter. Authors like Bailey and Brin have looked towards (reciprocal) transparency

as a means to negate information asymmetries.[20] The idea of reciprocal transparency and the related notion of *sousveillance*, are based around the premise that surveillance power should be equally distributed.

For the next twenty years or so, the challenge is to remedy the 'black box' nature of ubiquitous computing. A major part of the design philosophy for ubiquitous computing systems is that they should not burden the user. Ideally, their use should be unobtrusive and intuitive. But this design philosophy also makes the information systems less transparent. An approach is therefore necessary that entails that the data subject is properly informed about acts of data processing in order to keep a form of reciprocity between the data subject and the company or institution using his data. Where possible such an approach should be built into the technology.

The need for transparency will become even greater when nanotechnology will allow for truly pervasive surveillance. Without strict rules on the application of nano-surveillance, proper purpose specification and the ability for users to scan their surroundings for surreptitious nano-surveillance, the balance of power will be severely upset.

But transparency is not only important for the protection of the individual, it is also necessary to foster trust in surveillance. Evidence suggests that when individuals perceive that others are behaving cooperatively, they are moved by honour, altruism, and will be inclined to contribute to public goods even without the inducement of material incentives. When, in contrast, they perceive that others are shirking or otherwise taking advantage of them, individuals are moved by resentment. In that circumstance, they will withhold beneficial forms of cooperation.[21] We may infer from this that when surveillance infrastructures are no longer perceived to be beneficial to those under surveillance, or their operation is no longer transparent, they will elicit negative responses from groups and individuals. This could lead to the evasion of surveillance or possibly even the sabotage of surveillance infrastructures.

User empowerment

Currently individuals are for the most part unaware of the fact that personal data about them is being gathered through the various technological infrastructures that surround them (e.g. mobile phones, internet and CCTV). Furthermore, they have little to no influence on these technological infrastructures and the data they process. This situation will likely worsen in the future, since ubiquitous computing and NBIC technologies will be even less visible and tangible than current technology.

If users are to retain their right to privacy in the future, they must be given the means to exercise this right. This means that users must have a right to know whether surveillance infrastructures are present, get an idea

20 Bailey 2004, Brin 1999.

21 Kahan 2009.

who is using them, and what the purpose of the surveillance system is. While current data protection law and associated laws aimed at protecting privacy already grant these rights to individuals, the problem is that individuals do not have the power to actually effectuate these rights. Therefore, user empowerment is of the utmost importance.

First of all users need to have the means to detect surveillance systems. To this end they will need (automatic) detection tools (e.g. RFID detectors, software privacy agents, privacy coaches and nano-surveillance sniffers).[22] By providing these tools we can enhance the transparency of surveillance and avoid unwanted and invisible surveillance. Second, users must also get some manner of *agency*. In other words, they must have the ability to influence the use of their personal data and shield themselves from unwanted observation.

What must be noted about this approach though, is that while workable in the context of business-to-consumer or consumer-to-consumer privacy issues, it is not well suited for use in a surveillance context. The reason for this is that when it comes to surveillance of suspects, oftentimes you do not actually want the subject to be aware of the surveillance. Furthermore, you do not want to give tools to avoid or counteract surveillance to potential criminals and terrorists. As such, user empowerment has its limitations.

Accountability

Whereas individual user empowerment is difficult in the context of state surveillance, it is possible to restore the balance between the surveillors and the surveilled through proper accountability. Therefore, we should place more emphasis on the accountability of surveillance. We must ensure that proper checks and balances, judicial oversight, and regular reviews of surveillance practices are in place. Furthermore, sunset clauses should be introduced for particularly invasive surveillance technologies and investigative powers in order to ensure that their application cannot go on indefinitely without proper consideration. Not only are these measures necessary to ensure the legitimacy of surveillance practices, they also foster trust in their application.

Privacy as a collective interest

Currently privacy is conceptualised as an individual right. However, the interests that privacy aims to protect are actually also collective interests (e.g. trust, autonomy, social cohesion and equal treatment). Thus, positioning privacy as an individual right may actually be counterproductive, because the secrecy normally associated with privacy will reinforce notions of the collective versus the individual. By positioning privacy as a prerequisite for the development of a stable, democratic and free society, discussions that position an individual's right to privacy versus the security of society as a whole can be avoided.

22 See for instance: http://www.rfidguardian.org and http://www.difr.nl/?page_id=10.

Emphasis on identity and autonomy

Personally, I feel that if the predictions of Vinge, Kurzweil, and other Singulatarians are accurate, we need a far stronger emphasis on identity and autonomy in the discourse on privacy and data protection. The possible near-Singularity privacy issues set forth in this article are so fundamental for the autonomy of the individual, that an accompanying vocabulary must be used.

The concept of privacy and it conceptualisation as a right has been subject to inflation over time.[23] While human rights such as the freedom of speech or the freedom of religion are (almost) unchallenged in the political debate, the right to privacy, which in my opinion is equally important and a prerequisite for many other fundamental rights, is regularly challenged.[24] This can in large parts be attributed to the association of privacy with secrecy and hiding. So, instead of merely repositioning privacy as a collective interest, we need a new vocabulary for future privacy issues with a strong emphasis on the importance of personal identity and autonomy. For instance, instead of arguing about the privacy aspects of brain-machine interfaces we should push for a ban on state intervention in the thoughts of individuals. This would block the use of brain-machine interfaces for surveillance purposes and frame the discussion on the more fundamental level of personal autonomy.

Conclusion

The technological Singularity as described by Vinge and Kurzweil, if it ever occurs, will have such a profound impact on mankind that we cannot begin to describe the ethical and societal consequences it will entail. The aim of this article has therefore not been to describe the legal issues that arise after the Singularity, but rather describe those likely to emerge prior to Singularity. When we take the 'soft take off' scenario and look at the technological developments that will culminate in Singularity, we see that these technologies alone and in convergence, will have a significant impact on individuals and society as a whole.

In this article, I focussed on the possible consequences of near-Singularity technology for privacy. In my opinion privacy as a physical barrier against the observing gaze of others will steadily disappear over time as new, more advanced surveillance tools become available. So, to answer the first part of the problem statement would be that the effect of near-Singularity technologies on privacy will be no less than the disappearance of privacy as a meaningful physical barrier against the observing gaze.

---

23 Blok 2002.

24 A Dutch chief of police even went so far as to say that privacy is 'the hiding place of evil'.

The second part of the problem statement is much more difficult to answer. We can strengthen the right to privacy through measures like privacy by design, transparency and user empowerment, but this will be insufficient and sometimes even impossible in the context of state surveillance.

In my opinion a significant step in safeguarding (the right to) privacy in the future, particularly in the context of surveillance, is acknowledging its importance. Privacy is a prerequisite for our personal autonomy and human dignity, but in the context of surveillance is seen mainly as an obstacle for effective law enforcement. Such an attitude, while understandable, is dangerous. In my opinion we need to stop viewing privacy as an individual right (associated with secrecy), but must also consider it a collective interest, necessary for the well-being of our society. Furthermore, since future technologies may impact privacy at such a fundamental level (i.e. at the level of our personal thoughts) we need to frame the discussion at this fundamental level. This means more emphasis on the risks of surveillance for personal identity and autonomy.

We may conclude that the power of near-Singularity technologies is significant and that there will be considerable pressure to use them. Furthermore we may conclude that there seems to be little attention for the possible negative effects of these technologies for our privacy. If we fail to address these negative effects, Professor Schmidt was right in saying that there is little ground for optimism.

References

Aarts, Harwig & Schuurmans 2002
E. Aarts, R. Harwig and M. Schuurmans (2002), *Ambient Intelligence*, in: Denning, P.J. (ed.), *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, pp. 235-250. New York: McGraw Hill.

Bailey 2004
D. Bailey (2004), *The Open Society Paradox: Why the 21st Century Calls for More Openness, Not Less*, Washington: Potomac Books

Blok 2002
P. Blok (2002), *Het Recht op Privacy*, Den Haag: Boom Juridische uitgevers.

Brin 1999
D. Brin (1999), *The Transparent Society*, Redding: Perseus Books.

Kahan 2009
D. M. Kahan, *The Logic of Reciprocity: Trust, Collective Action, and Law*, Public Law and Legal Theory Research Paper No. 31, Yale Law School 2009.

Kurzweil 1990
R. Kurzweil (1990), *The Age of Intelligent Machines*, Cambridge MA: MIT Press.

Kurzweil 1999
R. Kurzweil (1999), *The Age of Spiritual Machines*, New York: Penguin

Kurzweil 2005
R. Kurzweil (2005), *The Singularity is Near, When Humans Transcend Biology*, New York: Viking.

Moerings 2006
L.M. Moerings (2006), *Risicojustitie als inzet voor een veiliger samenleving*, in: *Veiligheid en Recht, Nieuwe Doelwitten en Strategieën* (eds. Huisman, W., Moerings, L.M., Suurmond, G.), Den Haag: Boom Juridische uitgevers, p. 168

Schermer 2007
B.W. Schermer (2007), *Software Agents Surveillance, and Privacy, a Legislative Framework for Agent-enabled Surveillance*, Leiden: Leiden University Press.

Schmidt 2009
Schmidt (2009), *E-justice: No Ground for Optimism*, Leiden University.

Solove 2008
D.J. Solove (2008), Understanding Privacy, Cambridge: Harvard University Press.

Teeuw & Vedder 2008
W. Teeuw & A. Vedder (eds.), *Security Applications for Converging Technologies – Impact on the Constitutional State and the Legal Order*, The Hague: Boom Juridisch, 2008.

Vinge 1993
V. Vinge (1993), The Coming Technological Singularity: How to Survive in the Post-human Era, in: *Whole Earth Review*, Winter 1993.

Warren & Brandeis 1890
S.D. Warren and L.D. Brandeis L.D. (1890), 'The Right to Privacy: the Implicit Made Explicit', in: *Harvard Law Review*, p. 193-220.

Weiser 1991
M. Weiser (1991), *The Computer for the 21st Century, Scientific American Special Issue on Communications, Computers, and Networks*, September, 1991.

Weiser & Brown 1996
M. Weiser and S.J. Brown (1996), *The Coming Age of Calm Technology*, Xerox PARC, October 5, 1996.

Westin 1984
A.F. Westin (1984), The Origins of Modern Claims to Privacy, in: *Philosophical Dimensions of Privacy: an Anthology* (ed. F.D. Schoeman), Cambridge: Cambridge University Press, p. 56-74.

Over persoonsgegevens en IP-adressen, en de toekomst van privacywetgeving

Gerrit-Jan Zwenne■[1]

Aanleiding

Ik tik de tekst van deze bijdrage in op een netbook-computer die via een draadloze verbinding van KLM Air France is verbonden met internet. Het IP-adres waarvan ik gebruik maak is 194.209.131.192. Is dit nummer een persoonsgegeven? Is het mogelijk dat ik, of misschien iemand anders, aan de hand van dit 12-cijferig nummer, al dan niet in combinatie met andere beschikbare gegevens, kan worden geïdentificeerd? Ik denk van niet. Op dit moment zijn er schat ik ongeveer 75 reizigers in deze lounge en ongeveer de helft daarvan lijkt gebruik te maken van de internetverbinding. De dienst is gratis. Of eigenlijk: inbegrepen in de prijs van het vliegticket. Voor het gebruik van de dienst heb ik geen identificerende gegevens opgegeven. Weliswaar hebben alle bezoekers van deze lounge zich bij binnenkomst bekendgemaakt door middel van instapkaart en paspoort, maar daarmee valt voorzover ik kan overzien niet te achterhalen wie van hen precies gebruik maakt van de internetverbinding.

In deze context is het, denk ik, niet vanzelfsprekend dat het IP-adres een persoonsgegeven betreft. Voorbijgaand aan de onwaarschijnlijke situatie dat KLM Air France iedere zitplaats in de lounge zou hebben voorzien van verborgen videocamera's met gezichtsherkenningsfaciliteiten of andere meer geavanceerde surveillance-technologie, lijkt het uitgesloten dat iemand aan de hand van dit specifieke gegeven direct of indirect kan worden geïdentificeerd. Ik ga er dus vanuit dat het van KLM Air France of wie dan ook een onevenredige inspanning zou vragen om aan de hand van dit IP-adres te achterhalen wat de identiteit is van de internetgebruikers in de lounge.

Niet iedereen is het met mij eens. In de discussie over de werkingssfeer van privacywetgeving zijn privacytoezichthouders de afgelopen jaren steeds verdergaande (om niet te zeggen: radicalere) standpunten gaan innemen. Van het nog redelijk genuanceerde standpunt dat het er maar vanaf hangt of IP-adressen kunnen worden aangemerkt als persoonsgegeven is men uitgekomen op het standpunt dat deze specifieke gegevens eigenlijk altijd

---

■ Gerrit-Jan Zwenne is universitair hoofddocent bij eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij, en partner bij Bird & Bird Advocaten in Den Haag.

moeten worden aangemerkt als persoonsgegevens, of in elk geval zo moeten worden behandeld. Dit omdat deze gegevens, in combinatie met andere, door derden te verstrekken gegevens op enig moment het mogelijk zouden kunnen maken dat een natuurlijke persoon kan worden geïdentificeerd. De achterliggende redenering lijkt te zijn dat er, gelet op het belang van privacybescherming, beter te veel dan te weinig onder de werkingssfeer van de privacywet kan worden gebracht.

Er is, zeker naarmate 'instruments of mass surveillance' een alomtegenwoordig karakter beginnen krijgen,[2] begrip op te brengen voor deze redenering. En toch schiet deze om meerdere redenen haar doel voorbij. Als IP-adressen, en waarom niet nog andere identifiers, per definitie worden aangemerkt als 'persoonsgegevens' verliest dit begrip zijn onderscheidend vermogen. En dat kan uiteindelijk alleen maar leiden tot verdergaande afkalving van de privacywet.

In deze bijdrage bespreek ik de ontwikkeling van de opvattingen van privacytoezichthouders over IP-adressen en persoonsgegevens[3] en speculeer ik over hun, tot dusver nog niet erg duidelijk gemaakte beweegredenen. Zoals gezegd meen ik dat het bepaald onverstandig is het persoonsgegevensbegrip zo extensief te interpreteren. Omdat ik niettemin wel aanleiding zie om ten minste serieus na te denken over het stellen van beperkingen aan wat kan en mag met IP-adressen, doe ik een voorstel dat voortbouwt op bestaande regels in de telecomwetgeving.

Persoonsgegevens in de privacyrichtlijn en -wet

Er is sprake van een persoonsgegeven als het gaat om een gegeven waarmee direct of indirect een natuurlijke persoon kan worden geïdentificeerd. Aldus blijkt uit artikel 2, onder a, van privacyrichtlijn 95/46/EG, dat het begrip 'persoonsgegevens' definieert als:

> "iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon"

In dezelfde bepaling wordt aangegeven wat wordt verstaan onder identificeerbaarheid:

> "als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit"

2 Vgl. Klitou 2008.

3 In de bespreking van de ontwikkeling van de opvattingen van de Artikel 29 Werkgroep en CBP wordt voortgebouwd op de uiteenzetting in Bloemen-Patberg, Zwenne & De Weerd 2009.

In de preambule bij de richtlijn wordt aangegeven op welke wijze moet worden vastgesteld of iemand kan worden geïdentificeerd. Er moet, zo blijkt uit overweging 26, worden gekeken naar het volgende:

> "om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren;"

Uit dezelfde overweging blijkt dat er echter geen sprake is van persoonsgegevens als het gaat om:

> "[…] gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is."

De Wet bescherming persoonsgegevens (Wbp) heeft minder woorden nodig om hetzelfde te zeggen. Artikel 1, onder a, van de wet stelt dat onder een persoonsgegeven wordt verstaan:

> "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon."

In de parlementaire geschiedenis[4] wordt ingegaan op het identificeerbaarheidscriterium. In vrijwel dezelfde bewoordingen als van de zo even genoemde overweging 26 van de richtlijn wordt aangegeven dat moet worden uitgegaan van alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren. Het uitgangspunt is dat van 'een redelijk toegeruste verantwoordelijke'. Onder verwijzing naar eerdere uitingen van de privacytoezichthouder[5] wordt opgemerkt dat er:

> "[i]n concrete gevallen rekening [moet] worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste verantwoordelijke en anderzijds om subjectivering naar bijzondere expertise […]. Een onderzoeksinstituut als het CBS zal bijvoorbeeld gelet op zijn expertise, contacten en technische outillage, eerder in staat zijn gegevens te identificeren dan een individuele onderzoeker. Deze omstandigheid dient in de beoordeling of sprake is van een persoonsgegeven te worden meegewogen."

Voor de vraag of een IP-adres heeft te gelden als persoonsgegeven, en als zodanig onder de werking van de wet valt, is bepalend in hoeverre het mogelijk is om aan de hand van dit adres een natuurlijke persoon te identificeren. Het gaat erom in hoeverre degene die over dit gegeven beschikt in staat is daarmee de identiteit van een bepaalde natuurlijke persoon te weten

4 *Kamerstukken II* 1997-98, 25 892, nr. 3, bldz. 48-49.
5 Vgl. Registratiekamer 27 maart 1995, (kenm. 95.V.029).

te komen. En daarbij gaat het niet om de zuiver theoretische of hypothetische maar reële mogelijkheid dat de verantwoordelijke of iemand anders aan de hand van het IP-adres en met de hem redelijkerwijs beschikbare middelen ('expertise', 'contacten', 'technische outillage', enz.) in staat is deze identiteit te achterhalen.

In de parlementaire geschiedenis wordt, in de alinea na op de zo even aangehaalde alinea, ook ingegaan op de mogelijkheid dat bepaalde gegevens in verschillende contexten verschillende betekenissen kunnen hebben.

> "Wat blijkens het voorgaande voor de verantwoordelijke geldt, geldt bij het verstrekken van gegevens aan een derde uiteraard ook voor de ontvanger. Dat betekent dat de verantwoordelijke zich in een dergelijk geval zal moeten afvragen of de bewuste gegevens in handen van de ontvanger al dan niet als identificeerbaar zullen moeten worden aangemerkt. Bepalend is wat in de gegeven situatie redelijkerwijs mag worden verwacht. Naarmate een verstrekker over meer mogelijkheden beschikt om de risico's van identificatie door de ontvanger te voorzien of te beperken, mag van hem in dit opzicht meer zorgvuldigheid worden verwacht."

Het is goed mogelijk dat een bepaald gegeven ten opzichte van de éne persoon wel als persoonsgegeven kan worden aangemerkt en tegelijkertijd tegenover de ander niet. Een verantwoordelijke die beschikt over gegevens waarmee alleen hij in staat is natuurlijke personen te identificeren, kan deze gegevens verstrekken aan iemand anders. En als die andere dan niet in staat is daarmee de desbetreffende natuurlijke personen te identificeren, hebben deze gegevens tegenover die andere niet te gelden als persoonsgegevens. Het criterium is wat 'in de gegeven situatie redelijkerwijs mag worden verwacht.'

De Artikel-29-werkgroep over IP-adressen

Het overlegorgaan van nationale privacytoezichthouders, de Artikel 29 Werkgroep, stelt het onder meer tot zijn taak om de begrippen van de privacyrichtlijn 95/46/EG te verduidelijken.[6] De afgelopen jaren heeft de werkgroep zich verschillende keren uitgelaten over IP-adressen. Uit de desbetreffende werkdocumenten en opinies blijkt dat de opvattingen van de werkgroep zich hebben ontwikkeld. Eerst waren de standpunten nog redelijke genuanceerd en lieten ruimte voor de mogelijkheid dat deze gegevens niet altijd onder het bereik van de richtlijn vallen. Inmiddels is dat veranderd. In zijn latere opinies gaat de werkgroep ervan uit dat IP-adressen eigenlijk altijd en per

6 Oftewel "[d]oor uitwisseling van ervaringen tussen de nationale autoriteiten zal de Groep een coherente strategie voor de toepassing van de in de richtlijn neergelegde algemene beginselen aanmoedigen", aldus Art. 29 WG, Eerste jaarverslag, WP3, 25 juni 1997, bldz. 4. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp3_nl.pdf.

definitie moeten worden aangemerkt als persoonsgegevens, of in elk geval altijd als zodanig moeten worden behandeld.

Een van de eerste opmerkingen van de werkgroep over de kwalificatie van IP-adressen in termen van persoonsgegevens is te vinden in een eind vorige eeuw opgesteld verkennend werkdocument over verwerkingen van persoonsgegevens op internet.[7] De werkgroep merkt erin op dat 'bepaalde internetprotocol-adressen' persoonsgegevens kunnen zijn:

> "Het gebruik van infrastructuur is vaak rechtstreeks gebaseerd op de verwerking van persoonsgegevens, zoals bepaalde Internetprotocoladressen."

Volgens dit werkdocument moeten dus niet altijd alle IP-adressen per se worden aangemerkt als persoonsgegevens zijn, maar als het gaat om 'bepaalde' IP-adressen vaak wel.

Ongeveer een jaar later werkt de werkgroep dit verder uit. In zijn werkdocument over internet, privacy en online-gegevensbescherming[8] komt de werkgroep tot de conclusie dat in elk geval de door een ISP uitgegeven IP-adressen voor deze ISP als persoonsgegevens hebben te gelden. Dit omdat (of misschien: voorzover) kan worden aangenomen dat deze internetaanbieder systematisch de datum, het tijdstip, de duur en het aan hun gebruikers verstrekte (dynamische) IP-adres vastlegt. Volgens de werkgroep brengt dit met zich mee dat:

> "internetaanbieders en beheerders van lokale netwerken zonder veel moeite internetgebruikers [unnen] identificeren aan wie ze IP-adressen hebben verstrekt, doordat ze als regel systematisch de datum, het tijdstip, de duur en het verstrekte dynamische IP-adres van gebruikers in een logbestand vastleggen. Hetzelfde geldt voor internetdienstverleners die een logboek op de HTTP-server bijhouden. In deze gevallen is het buiten kijf dat men kan spreken van persoonsgegevens in de zin van artikel 2, onder a, van de richtlijn."

De werkgroep tekent daarbij wel aan dat dit voor andere internetpartijen wellicht anders is, omdat zij niet vanzelfsprekend in staat zijn om met het IP-adres internetgebruikers te identificeren. Daarbij maakt de werkgroep onderscheid tussen vaste IP-adressen waarmee identificatie geacht wordt eenvoudiger te zijn, en dynamische IP-adressen waarbij dat moeilijker is:

> "Anders is het als derden wel het dynamische IP-adres van een gebruiker kunnen achterhalen, maar dat niet kunnen koppelen aan andere gegevens die identificatie van de betrokken gebruiker mogelijk maken. Identificatie van internetgebruikers die een statisch IP-adres toepassen, is uiteraard eenvoudiger."

---

7 Art. 29 WG, Processing of Personal Data on the Internet, 23 februari 1999 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp16nl.pdf.

8 Art. 29 WG, Privacy on the Internet. An integrated EU Approach to On-line Data Protection, 21 november 2000 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37nl.pdf.

Daar voegt de werkgroep echter aan toe dat het toch vaak mogelijk zal zijn om degene die van het IP-adres gebruik maakt te identificeren, en wel door het vaste of dynamische IP-adres te koppelen aan andere gegevens die over de gebruiker zijn verkregen, bijvoorbeeld via cookies of datamining. Om deze redenen gaat de werkgroep ervan uit dat veel, maar toch niet per sé alle IP-adressen moeten worden aangemerkt als persoonsgegevens:

> "In veel gevallen is het echter wel degelijk mogelijk het IP-adres van gebruikers zodanig te koppelen aan andere (al dan niet openbaar beschikbare) persoonsgegevens dat deze gebruikers kunnen worden geïdentificeerd, vooral als gebruik wordt gemaakt van onzichtbare verwerkingsmethoden om aanvullende informatie over de gebruiker te verwerven (bijvoorbeeld met behulp van cookies die een unieke identificatiecode bevatten) of van moderne datamining gekoppeld aan grote databases met individueel identificeerbare gegevens over internetgebruikers."

Maar de werkgroep blijft redelijk genuanceerd en geeft nadrukkelijk aan dat niet is uitgesloten dat IP-adressen in voorkomende gevallen niet, althans niet voor iedereen, zijn aan te merken als persoonsgegevens, die vallen onder de werkingssfeer van de richtlijn:

> "Om deze reden wordt er, ook al is het wellicht niet in alle gevallen en niet voor alle internetpartijen mogelijk een gebruiker aan de hand van de op internet verwerkte gegevens te identificeren, in dit document van uitgegaan dat de mogelijkheid daartoe in veel gevallen wel degelijk bestaat en dat grote hoeveelheden persoonsgegevens waarvoor de richtlijnen op het gebied van persoonsgegevens gelden, op internet worden verwerkt."

Ook hier wordt derhalve aangegeven dat IP-adressen in veel gevallen moeten als persoonsgegevens moeten worden aangemerkt als persoonsgegeven. Maar niet altijd en evenmin ten opzichte van iedereen.

Deze nog steeds genuanceerde benadering werkt de werkgroep uit in een opinie over het begrip persoonsgegevens.[9] Waar het gaat om de identificeerbaarheid gaat de werkgroep uiteraard uit van de maatstaf uit overweging 26 van de preambule bij de richtlijn: er moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs zijn in te zetten door de verantwoordelijke of iemand anders. De werkgroep leidt daaruit af dat de theoretische of hypothetische mogelijkheid om een natuurlijke persoon te identificeren onvoldoende is om die persoon als identificeerbaar te beschouwen. Om te bepalen of sprake is van 'redelijkerwijs in te zetten middelen' moet rekening worden gehouden met alle relevante omstandigheden van het geval.

Als voorbeeld noemt de werkgroep de situatie dat een auteursrechthebbende de IP-adressenvan abonnees verzamelt waarvan wordt vermoed dat die inbreuk maken op zijn auteursrechten. Er is dan sprake van persoonsge-

9 Art. 29 WG, Opinion nr. 4/2007 on the concept of personal data, 20 november 2007 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_nl.pdf.

gevens als wordt aangenomen dat de rechthebbende via gerechtelijke procedures de beschikking kan verkrijgen over desbetreffende abonneegegevens:

> "Vooral in die gevallen dat het IP-adres wordt verwerkt met het doel de gebruikers van de computer te identificeren (bijvoorbeeld door de houder van een auteursrecht die computergebruikers wil aanklagen wegens schending van intellectuele-eigendomsrechten), gaat de voor de verwerking verantwoordelijke ervan uit dat de "redelijkerwijs in te zetten middelen" voor de identificatie van de betrokkenen beschikbaar zullen zijn, bijvoorbeeld via de rechtbanken waarop een beroep wordt gedaan, anders zou het verzamelen van de informatie geen zin hebben. Deze informatie moet dan ook als persoonsgegeven worden beschouwd."

Maar ook dan zijn er volgens de werkgroep nog veel voorbeelden waarbij identificatie met een IP-adres onmogelijk is, zoals het geval van een internetcafé waarbij gebruiker zich niet behoeft te identificeren:

> "In sommige gevallen is het voor bepaalde IP-adressen om diverse technische en organisatorische redenen niet mogelijk de gebruiker te identificeren. Een voorbeeld zijn de IP-adressen die zijn toegewezen aan computers in een internetcafé waar van de klanten geen legitimatie wordt verlangd. Hier zou kunnen worden aangevoerd dat de gegevens over het gebruik van computer X gedurende een bepaalde periode geen identificatie van de gebruiker met redelijkerwijs in te zetten middelen mogelijk maken en dat die gegevens daarom geen persoonsgegevens zijn."

Omdat niet in alle gevallen bekend is of er sprake is van identificeerbaarheid doet de werkgroep wel de aanbeveling dat internetdienstverleners voor de zekerheid alle IP-adressen als persoonsgegevens behandelen. Dit echter niet zozeer omdat het per definitie persoonsgegevens betreft, maar om praktische redenen:

> "De internetdienstverlener zal echter naar alle waarschijnlijkheid niet weten of het IP-adres in kwestie identificatie mogelijk maakt, en zal de aan dat IP-adres gekoppelde gegevens op dezelfde wijze behandelen als informatie die gekoppeld is aan IP-adressen van geregistreerde en identificeerbare gebruikers."

De ommekeer doet zich iets minder dan een half jaar later voor. In een opinie over internetzoekdiensten[10] neemt de werkgroep afstand van zijn tot dan toe consequent gevolgde standpunt betreffende IP-adressen moeten worden aangemerkt als persoonsgegevens. Zonder echt aan te geven waarom gaat de werkgroep in deze opinie ineens voorbij aan de nuancering dat moet worden gekeken naar de middelen waarover een bepaalde verantwoordelijke de beschikking heeft. Ook ziet de werkgroep geen ruimte meer voor de situatie waarin de éne gegevensverwerker wél identificatiemogelijkheden

10 Art. 29 WG, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.

heeft en de andere niet, zodat IP-adressen voor de eerste wel persoonsgegevens betreffen maar voor de laatste niet:

> "Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address."

De werkgroep meent dat een IP-adres hoe dan ook een persoonsgegeven betreft omdat identificatie door derden mogelijk kan zijn ('identification […] by a third party'). Weliswaar kan in de regel alléén de ISP achterhalen welke natuurlijke persoon van een IP-adres gebruik heeft gemaakt. Maar omdat 'bepaalde autoriteiten' en in voorkomende gevallen zelfs private partijen in staat zijn om van de ISP de nodige identificerende abonneegegevens te verkrijgen, meent de werkgroep dat er hoe dan ook sprake is van persoonsgegevens.

In lijn met deze opvatting, waarin de beschikbaarheid van de redelijkerwijs in te zetten identificatiemiddelen als het ware wordt verondersteld, zijn de voorwaarden die de werkgroep introduceert waar het gaat om het anonimiseren van gegevens:

> "Anonymisation of data should exclude any possibility of individuals to be identified, even by combining anonymised information held by the search engine company with information held by another stakeholder (for instance, an internet service provider). Currently, some search engine providers truncate IPv4 addresses by removing the final octet, thus in effect retaining information about the user's ISP or subnet, but not directly identifying the individual. The activity could then originate from any of 254 IP addresses. This may not always be enough to guarantee anonymisation."

Er kan volgens de werkgroep alleen dan worden gesproken van anonimisering of on-identificeerbaarheid als iedere mogelijkheid van identificering is uitgesloten ('exclude any possibility of individuals to be identified'). In de eerder gehanteerde, genuanceerdere benadering had nog kunnen worden gesteld dat gegevens zijn geanonimiseerd voorzover deze gegevens niet door iemand met de redelijkerwijs hem ter beschikking staande middelen kunnen worden gebruikt om een natuurlijke persoon te identificeren. Maar voor dergelijke nuanceringen ziet de werkgroep geen ruimte meer.

Daarmee is de werkgroep dus uitgekomen op het standpunt dat IP-adressen inmiddels, ook voor de internetpartijen die deze níet aan individuele gebruikers kunnen koppelen, altijd moeten worden aangemerkt als persoonsgegeven en als zodanig onder het bereik van de richtlijn vallen. En waar de werkgroep eerst niet uitsloot dat er in de context van bijvoorbeeld een internetcafé of een openbare bibliotheek geen sprake is identificeerbaarheid, gaat hij er in deze opinie vanuit dat er altijd zonder meer sprake is van persoonsgegevens.

Het CBP over IP-adressen

De opvattingen van het CBP over IP-adressen hebben eenzelfde ontwikkeling doorgemaakt als die van de werkgroep – niet helemaal onverwacht omdat het CBP een actief deelnemer is aan de werkgroep.

In het verleden lieten ook het CBP en zijn voorganger de Registratiekamer zich genuanceerd uit over IP-adressen en persoonsgegevens. Op de website van de toezichthouder zijn voorbeelden daarvan te vinden. Zo is er een brief uit 2001[11] waarin de Registratiekamer uiteenzet onder welke omstandigheden kan worden aangenomen wanneer met een IP-adres zonder onevenredige inspanningen de identiteit van een natuurlijke persoon kan worden vastgesteld. De toezichthouder parafraseert de parlementaire geschiedenis die weer voortbouwt op zijn eerdere correspondentie over hetzelfde onderwerp:[12]

> "Bij 'identified or identifiable' speelt vooral de vraag of de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Dit hangt mede af van de mogelijkheden waarover de houder beschikt en de bekendheid of beschikbaarheid van aanvullende informatie. Hierbij moet uitgegaan worden van een redelijk toegeruste houder. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de houder. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste houder en anderzijds om subjectivering naar bijzondere expertise."

Een en ander toepassend op IP-adressen komt de toezichthouder vervolgens tot het oordeel dat de door een ISP uitgegeven vaste of statische IP-adressen 'zonder meer' door deze ISP zijn te herleiden tot natuurlijke personen en dus als persoonsgegevens moeten worden aangemerkt. Voor dynamische IP-adressen is dit niet anders, tenminste als de ISP heeft vastgelegd op welk moment het adres door welke gebruiker werd gebruikt. Als de ISP dit evenwel niet heeft vastgelegd, kan er niet worden gesproken van persoonsgegevens. En hoewel de brief daarover niet erg duidelijk is, lijkt het uitgangspunt te zijn dat er niet kan worden gesproken van persoonsgegevens ten opzichte van anderen dan de ISP's, als deze anderen niet beschikken over de middelen om de internetgebruikers te identificeren.

---

11 CBP, 'Een IP adres is niet altijd een persoonsgegeven', 19 maart 2001, z2000-0340 www.cbpweb.nl/downloads_uit/z2000-0340.pdf.

12 Vgl. de parl. gesch, genoemd in voetnoot 5 en de brief van de Registratiekamer genoemd in voetnoot 4.

In verschillende publicaties over zgn. 'privacy enhancing technologies' gaat het CBP verder in op dit laatste aspect van het identificeerbaarheidscriterium, dat wil zeggen: de vraag in hoeverre er kan worden aangenomen dat er ten opzichte van de éne gegevensverwerker (zeg: de ISP) wél sprake kan zijn van persoonsgegevens en tegelijkertijd ten opzichte van anderen niet. Zonder daarbij in te gaan op IP-adressen zet de toezichthouder in dit kader uiteen dat er géén sprake is van identificeerbaarheid, en dus niet van persoonsgegevens, als voor het identificeren de medewerking van derden is vereist en deze medewerking niet kan worden afgedwongen.[13] Een gegeven is alleen een persoonsgegeven voor degenen die in staat zijn met dit gegeven een natuurlijke persoon te identificeren, en niet voor degenen die dat niet kunnen:

> "niet-identificeerbaarheid [wordt] aangenomen als hiervoor de medewerking van derden buiten de macht en zeggenschap van de verantwoordelijke noodzakelijk is"

In de regel worden IP-adressen daarom ten opzichte van ISP's aangemerkt als persoonsgegevens. Er kan maar hoeft niet per sé ten opzichte van anderen sprake zijn van persoonsgegevens, maar alleen voorzover deze anderen door de ISP's (of eventueel anderen) in staat worden gesteld daarmee een natuurlijke persoon te identificeren.[14]

De publicatie van de zo-even besproken opinie van de werkgroep over zoekdiensten brengt ook voor het CBP de ommekeer. In zijn persbericht over de opinie meldt de toezichthouder zonder enig voorbehoud dat nu eindelijk:

> "ondubbelzinnig [wordt] vastgesteld dat IP-adressen persoonsgegevens vormen."[15]

---

13 CBP 2002.

14 Idem Van Esch 2008, p. 75-76; Van Esch & Blok 2007, p. 206.

15 CBP-persbericht Internetzoekmachines moeten privacy respecteren, 7 april 2008 (www.cbpweb.nl/docum–enten/pb_20080407_internetzoekmachines.shtml); naar aanleiding van twee uitspraken van Cour d'appel de Paris 13ème chambre, section B Arrêt du 27 avril 2007 en section A Arrêt du 15 mai 2007 kwam de Franse privacytoezichthouder met het volgende verontwaardigde persbericht: "In two successive rulings issued in April and May 2007, the Court of Appeal of Paris judged that IP addresses collected during searches and findings of internet counterfeiting acts do not enable, even indirectly, any identification of physical persons, and that consequently they do not constitute personal data. Concerned about the consequences of such an analysis of Internet privacy protection, CNIL contacted the Minister of Justice and the Public Prosecutor to the Cour de Cassation (Supreme Court) in an attempt to lodge an appeal against both rulings in the interest of the law. In a letter dated 8 October 2007, the Minister of Justice agreed to lodge the appeal to the Cour de Cassation who should issue its ruling sometime in 2008. It should be noted that, in an opinion published on 20 June 2007, the data protection authorities of EU Member States issued a reminder that IP addresses were indeed to be regarded as personal data." (http://www.cnil.fr/english/main-issues/tracking-web-surfers/); zie daarover Peter Fleischer in zijn blogbericht van 15 februari 2008 (http://peterfleischer.blogspot.com).

Natuurlijk, deze wellicht wat overenthousiaste uiting betreft een persbericht en niets meer dan dat. En er kon indertijd wellicht nog worden volgehouden dat de persvoorlichter de opinie van de werkgroep wat kort-door-de-bocht had samengevat, en dat de toezichthouder het niet zo had bedoeld. Iets meer dan een half jaar later blijkt echter dat het CBP wel degelijk afstand heeft willen nemen van zijn eerdere, meer genuanceerde opvatting over IP-adressen. In zijn richtsnoeren[16] voor de publicatie van persoonsgegevens op het internet stelt de toezichthouder zich op het standpunt dat het niet meer uitmaakt dat ISP's de gegevens in feite niet gebruiken om natuurlijke personen te identificeren. Voldoende is dat er daartoe een mogelijkheid bestaat, bij de ISP zelf of bij anderen.

Ook lijkt de toezichthouder afstand te willen nemen van de genuanceerdere opvatting dat sommige gegevens voor de éne gegevensverwerker wel als persoonsgegevens moeten worden aangemerkt (omdat deze gegevens hem in staat stellen natuurlijke personen te identificeren), terwijl diezelfde gegevens tegelijkertijd voor anderen niet als zodanig hebben te gelden (als die anderen niet in staat zijn daarmee iemand te identificeren). Als eenmaal is vastgesteld dat een IP-adres in de context van een ISP een persoonsgegeven betreft – en daarvan wordt per definitie uitgegaan – dan werkt dat volgens de richtsnoeren dus door in al het verdere gebruik van het gegeven: ergens eens een persoonsgegeven betekent derhalve altijd en overal een persoonsgegeven. De richtsnoeren stellen:

> "Een IP-adres is een persoonsgegeven omdat het door een derde – de internetaanbieder – eenvoudig te herleiden valt tot een natuurlijk persoon, de afnemer van het internetabonnement. Dit geldt ook voor dynamische IP-adressen die worden verwerkt in combinatie met datum en tijd. Het maakt geen verschil dat een verantwoordelijke het IP-adres niet zal gebruiken om een persoon mee te identificeren. Het feit dat de mogelijkheid bestaat bij de verantwoordelijke of bij een derde om dit te doen, is voldoende."

Wel onderkennen de richtsnoeren dat 'in sommige gevallen' met behulp van IP-adressen alleen rechtspersonen worden geïdentificeerd. Maar dat doet er niet aan af dat er 'in de meeste gevallen' toch wel sprake zal zijn van persoonsgegevens en er 'dus' alle gegevens hoe dan ook als zodanig moeten worden behandeld.

> "Dat het IP-adres in sommige gevallen naar een rechtspersoon leidt, in plaats van naar een natuurlijk persoon, doet niet af aan het feit dat het in de meeste gevallen wel degelijk om persoonsgegevens gaat en dat dus de hele verzameling moet worden behandeld conform de uitgangspunten van de Wbp."

16 CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007 *Stcrt.* 2007, 240 www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf.

Het is onduidelijk is wat er precies wordt bedoeld met deze opmerking. Voorzover er bedoeld is te zeggen dat gegevens over rechtspersonen in de meeste gevallen toch persoonsgegevens zijn, lijkt dat overduidelijk op gespannen voet te staan met de werkelijkheid. Er kan ook zijn bedoeld dat het in deze gevallen praktisch onmogelijk is om onderscheid te maken tussen de IP-adresssen die wél en niet kunnen worden gebruikt om natuurlijke personen te identificeren. Er is dan dus niet zozeer een verplichting om ook IP-adressen van rechtspersonen te behandelen alsof het persoonsgegevens zijn, maar veeleer een (gemakshalve veronderstelde) praktische onvermijdelijkheid.[17]

Een voor de hand liggende vraag is dan waarom er in deze gevallen geen technische of organisatorische maatregelen zouden kunnen worden genomen om de persoonsgegevens te scheiden van andere gegevens. In dezelfde lijn ligt de vraag waarom er geen privacy enhancing technologies zou kunnen worden toegepast om identificeerbaarheid te voorkomen. Het lijkt erop dat de toezichthouder geen vertrouwen meer heeft in dergelijke oplossingen. Dat zou opmerkelijk zijn, omdat nou juist de toezichthouder in het verleden (terecht) veel heeft geïnvesteerd in het ontwikkelen en doordenken van dergelijke PET's.[18]

Commentaar

De geschetste ontwikkeling van de opvattingen van de werkgroep en het CBP lenen zich voor een nadere beschouwing, zij het dat deze noodgedwongen een speculatief karakter heeft omdat er door hen maar weinig is losgelaten over hun beweegredenen.

Het lijkt aannemelijk dat deze beweegredenen allereerst liggen in het intelligenter worden van de technieken waarmee gegevens met elkaar in verband worden gebracht en internetgebruikers worden geïndividualiseerd. Indertijd, zo rond de eeuwwisseling, waren de mogelijkheden daartoe nog betrekkelijk beperkt. Inmiddels zijn zoek- en selectietechnologieën – denk aan: behavourial targeting, profiling, data mining, deep packet sniffing etc. – veel intelligenter geworden en daarbij breed beschikbaar, wat aanleiding kan zijn om veel eerder uit te gaan van identificeerbaarheid.

---

17 In een recent onderzoek volstaat het CBP grotendeels met verwijzingen naar de eigen richtsnoeren. Op het verweer dat niet alle IP-adres naar individuen verwijzen, reageert het CBP met de opmerking dat het dit argument 'niet steekhoudend' acht, omdat "het niet afdoet aan de herleidbaarheid tot een individu van een groot deel van de IP-adressen". Ofte wel: omdat een groot deel van de IP-adressen herleidbaar is tot individuen zijn alle IP-adressen persoonsgegevens. Aldus de definitieve bevindingen van het onderzoek naar de zgn. 'Geen Stijl IP-checker op GeenCommentaar.nl (z2008-01174), 27 oktober 2008.

18 De website van het CBP noemt o.a.: Koorn et al, 2004; Van Blarkom, Borking & Olk (eds.) 2003; Kenny & Borking, 2002; CBP 2002; Borking & Raab, 2001.

In het verlengde daarvan is denkbaar dat deze beweegredenen wellicht ook liggen in wat tegenwoordig allemaal kan met IP-adressen en andere identifiers. In de richtsnoeren wordt daarover iets interessants gezegd:

"Ten slotte is van belang dat op basis van het IP-adres beslissingen kunnen worden genomen over de toegang tot bepaalde informatie, zonder dat een dienstverlener op internet überhaupt enige moeite hoeft te doen om zelf persoonsgegevens te verbinden aan een IP-adres. Denk bijvoorbeeld aan onderscheid naar geografische herkomst bij de toegang tot en de presentatie van (delen van) websites. Ook het registreren en eventueel op internet publiceren van IP-adressen van bezoekers van een website of deelnemers aan een discussieforum valt dus onder het bereik van de Wbp."

Er wordt, zo begrijp ik, enerzijds opgemerkt dat persoonsgegevens kunnen worden verbonden aan IP-adressen, waarmee wordt gesuggereerd dat IP-adressen a priori geen persoonsgegevens hoeven zijn, maar dat kúnnen worden als er een verband wordt gelegd met persoonsgegevens. Anderzijds lijkt te worden gezegd dat IP-adressen, ook als ze eigenlijk geen persoonsgegevens zijn, niettemin onder de werkingssfeer van de Wbp zouden moeten worden gebracht. Dit omdat ze zouden kunnen worden gebruikt om 'beslissingen' te nemen over nog niet geïdentificeerde of identificeerbare internetgebruikers.

Er staat niet wat er staat, dichtte Nijhoff. En ik lees er misschien meer in dan wordt bedoeld. Dat doet er evenwel niet aan af dat aan de hand van IP-adressen inderdaad beslissingen kunnen worden genomen met betrekking tot geïndividualiseerde, maar niettemin nog ongeïdentificeerde of onidentificeerbare internetgebruikers. Zeg: de internetgebruiker van wie is vastgesteld dat hij eind oktober jl. in de executive lounge te Geneve Cointrin International gebruik maakte van IP-adres 194.209.131.192.

Allereerst kan dergelijke informatie worden gebruikt om onderscheid te maken tussen internetgebruikers naar geografische locatie, bijvoorbeeld om te voorkomen dat voornoemde internetgebruiker bij iTunes zijn muziek niet in euro's afrekent, maar met de voor hem voordelige dollars.[19] Verder is voorstelbaar dat Apple en wellicht ook Nike om andere redenen belangstelling hebben voor deze, vooralsnog ongeïdentificeerde maar wel geïndividualiseerde internetgebruiker. Zeker als uit de analyse van zijn (of haar) internetactiviteiten zou blijken dat hij (of zij) bovengemiddeld is geïnteresseerd in grote hardloopevenementen, trendgevoelige draagbare muziekspelers, en daarbij met enige regelmaat vliegreizen binnen Europa maakt. Waarom maakt het voor het sportmerk of elektronicabedrijf niet uit dat deze gebruiker (vooralsnog?) niet is geïdentificeerd? Omdat het voor hen voldoende is als zij op de eigen websites, en die van anderen, aan deze specifieke gebruiker de juiste web-advertenties of banners kunnen laten zien. Bijvoorbeeld over de nieuwste generatie (Air Force) loopschoenen en een iPod Sport Kit.

19 Denk ook aan: differentiëren naar geografische locatie van internetgebruikers en het voorkomen van parallel-import; vgl Bloemen-Patberg, Zwenne & De Weerd 2009, p. 79.

Daarvoor hoeft de gebruiker niet te zijn geïdentificeerd, maar alleen geïndividualiseerd. En daarvoor is een IP-adres toereikend.

Er is meer mogelijk. Wat in de online reclamewereld wordt aangeduid als behavourial targeting of profiling – het met onder meer IP-adressen in kaart brengen van de voorkeuren van geïndividualiseerde internetgebruikers[20] – kan in andere contexten worden toegepast, soms met ernstigere consequenties dan het vertonen van banners. Aangenomen mag worden dat bijvoorbeeld auteursrechtorganisaties belangstelling hebben voor geïndividualiseerde downloaders. En dat niet alleen om deze op enig moment te identificeren, maar ook om alvast het dossier op te bouwen en vast te leggen wat deze geïndividualiseerde internetgebruikers allemaal doen. Ook denkbaar is dat deze rechthebbenden van ISP's gedaan krijgen dat wordt overgegaan tot het afsluiten van de niet door hen geïdentificeerde, maar wel geïndividualiseerde abonnees die gebruik maken van de door hen als verdachte aangemerkte IP-adressen.[21] Ook in deze situatie volstaan IP-adressen en is niet per se nodig dat de identiteit van de abonnees (al?) bekend is.

Er is weinig fantasie voor nodig om in het verlengde daarvan andere situaties te bedenken waarin er aanleiding is om internetgebruikers te individualiseren met IP-adressen. Wat te denken van de opsporingsautoriteiten die een zaak 'opbouwen' over bijvoorbeeld dierenliefhebbers woonachtig in kraakpanden en met een bijzondere belangstelling voor adressen van politici en de receptuur van (verf)bommen? Wat te zeggen van de wens van sommige regimes om informatieposities op te bouwen tegen de bezoekers van hen onwelgevallige websites, of tegen subversieve bloggers en de lezers van hun blogberichten, enz.

Ik wil maar zeggen. Ook als er nog geen sprake is van identificeerbaarheid zijn er talloze goede en minder goede redenen om aan de hand van IP-adressen gedetailleerde profielen aan te leggen van geïndividualiseerde maar niettemin ongeïdentificeerde internetgebruikers. In termen van privacy heeft dit implicaties, ook als er volgens de gangbare definitie nog geen sprake is van identificeerbaarheid. Voor een toezichthouder van wie de bevoegdheid is beperkt tot persoonsgegevens, is de begrijpelijke eerste reflex dan om het persoonsgegevensbegrip zo te interpreteren dat IP-adressen hoe dan ook daaronder vallen. En om zodoende individualiseren gelijk te stellen met identificeren.[22] En dat alles waarschijnlijk met als achterliggende gedachte dat een teveel aan privacywaarborgen is te verkiezen boven te weinig.

---

20 Koeter 2009.

21 Zo is het naar verluid wel gebeurd dat een heel studentenhuis werd afgesloten omdat er één gebruiker iets had gedaan wat volgens de ISP (of anderen?) niet door de beugel kon.

22 In die zin laat Hustinx, de voorzitter van de Europese privacytoezichthouder, zich uit in een kort webinterview op ZDnet: "identifiable in the sense of personal data is singling someone out; we don't need to name name and address". http://news.zdnet.co.uk/security/0,1000000189,39540137,00.htm.

De toekomst van privacywetgeving (Privacywet 2.0)

De gedachte waarmee de vorige paragraaf eindigde is niet onsympathiek. Als het gaat om de bescherming van de persoonlijke levenssfeer is een teveel aan waarborgen te verkiezen boven te weinig. En, gelet op wat er met IP-adressen kan, is er wellicht veel voor te zeggen om op de een of andere manier beperkingen te stellen aan het gebruik van IP-adressen en andere gegevens, waarmee internetgebruikers worden geïndividualiseerd – ook als die gegevens nog niet, of nog niet voor iedereen, als persoonsgegevens zijn aan te merken.

In dergelijke beperkingen voorziet de Wbp niet, tenzij wordt uitgegaan van een zo extensieve interpretatie van het persoonsgegevensbegrip dat IP-adressen per definitie daaronder vallen. De vraag is of daarom de privacywetgeving van de toekomst (zeg: Privacywet 2.0) inderdaad moet uitgaan van een persoonsgegevensbegrip dat vanzelfsprekend ook IP-adressen omvat, en daarmee ook andere identifiers (bijvoorbeeld IMSI of IMEI-nummers, of RFID-nummers enz.).

Er zijn verschillende redenen waarom wij dit niet moeten willen. Wat mij betreft ligt de belangrijkste daarvan in het voorkomen dat de Wbp als privacywet betekenis verliest. Een extensieve interpretatie leidt ertoe dat de werkingssfeer van de wet wordt opgerekt tot ver voorbij wat nog werkbaar is. Een dergelijke interpretatie impliceert dat bij de toepassing van het identificeerbaarheidscriterium wordt voorbijgegaan aan zowel de objectivering naar de redelijk toegeruste gegevensverwerker ('wat in de gegeven situatie redelijkerwijs mag worden verwacht') als de subjectivering naar diens bijzondere expertise ('expertise', 'contacten', 'technische outillage' enz.).

En dat brengt onvermijdelijk met zich mee dat veel (heel erg veel) meer gegevens onder de werkingssfeer van de wet komen te vallen. En, wat belangrijker is, dat er dan géén hanteerbaar criterium meer is waarmee kan worden bepaald wat géén persoonsgegeven (meer) is. Als er al kan worden gesproken van identificeerbaarheid als op enig moment er de mogelijkheid zou kunnen zijn dat een individu wordt geïdentificeerd, verliest identificeerbaarheid als criterium onderscheidend vermogen. Alles wat dan op enig moment kan leiden tot identificatie is daarmee een persoonsgegeven, althans moet als zodanig worden behandeld, wat op hetzelfde neerkomt. Het risico dat ik zie is dat toepassing van de wet dan toevallig wordt, en de naleving en de handhaving willekeurig.

In het verlengde daarvan zijn er nog meer redenen waarom de door toezichthouders verdedigde extensieve uitleg van het persoonsgegevensbegrip onverstandig is. Op dit moment, uitgaande van een redelijk genuanceerde interpretatie wordt de werkingssfeer van de wet vaak al ervaren als onbegrensd.[23] Als ervan uit wordt gegaan dat IP-adressen altijd als persoons-

23 Vgl. bijv. Van der Horst 2002; De Hert & Gutwirth, 2004; Zwenne et al, 2007, p. 12, 61, 64-68, 96, 137, 157 en 168.

gegevens moeten worden aangemerkt, valt daarop weinig meer af te dingen. Als dat nu al niet het geval is, dan toch in elk geval na de introductie van de nieuwe generatie van IP-adressen (IPv6), waarmee de voorraad van IP-adressen naar verluid voldoende is om ieder individueel atoom op aarde een eigen nummer te geven.[24]

Voor het toezicht is relevant dat de extensieve interpretatie zoveel rechtsonzekerheid met zich brengt dat handhavingsmaatregelen het risico lopen te stuiten op het lex certa-beginsel, het beginsel dat alleen sancties mogen worden opgelegd met betrekking tot overtredingen van normen die voldoende voorzienbaar en duidelijk zijn.[25] Ook relevant is wellicht dat de extensieve interpretatie een streep lijkt te halen door de ontwikkeling van privacy by design en privacy enhancing technologies, en alle inspanningen die daarvoor, niet in de laatste plaats door de toezichthouder, zijn gedaan.[26] Als IP-adressen per definitie als persoonsgegevens worden aangemerkt, of als zodanig moeten worden behandeld, heeft het weinig zin meer om de technische en organisatorische maatregelen te nemen om gegevensverwerkingen zo in te richten dat er geen sprake meer is van identificeerbaarheid. Althans, dergelijke maatregelen leiden dan niet tot een vermindering van de compliance-kosten, wat een belangrijke reden is om daarin te investeren.

Verder geldt dat een te extensieve interpretatie ingaat tegen andere uitingen van toezichthouders[27] en ook tegen de nog schaarse rechtspraak over IP-adressen,[28] en als zodanig de geloofwaardigheid van het toezicht geen goed doet. Ook niet onbelangrijk zijn uitvoeringsproblemen waartoe deze interpretatie aanleiding geeft, bijvoorbeeld waar het gaat om het inzagerecht, de informatieplicht, de meldingsplicht of de internationale doorgifte van de gegevens.[29] En daarbij is het maar de vraag of de privacybescherming, mede gelet op het voorgaande, uiteindelijk wel is gebaat bij deze extensieve interpretatie.

---

24 IPv4 kent 32 bits en ondersteunt iets meer dan 4 miljard (om percies te zijn 4.294.967296) IP-adressen; IPv6 kent 128 bits en ondersteunt dus het astronomische aantal van precies 3 40.282.366.920.938.463.463.374.607.431.768.211.456 IP-adressen.

25 Zie o.a. EHRM 25 mei 1993, ECRM Series A, Vol. 260; EHRM 27 september 1995, *NJ* 1996, 49; Rb.'s-Gravenhage 23 december 1998, *JB* 1999, 57; ABRvS 8 december 2004, AB, 2005, 44; ABRvS 20 november 2002, *AB* 2003, 173; CBb 24 augustus 2006, *AB* 2007, 321; CBb 20 december 2007, *AB* 2008, 56; zie ook *Kamerstukken II* 2003–04, 29 702, nr. 3, p. 86

26 Zie voetnoot 16.

27 In aanvulling op de reeds genoemde uitingen van CBP en de werkgroep kan worden gewezen op de zgn. Good practice note – Collecting personal information using websites, van 5 juni 2007, waarin de privacytoezichthouder in het Verenigd Koninkrijk overweegt dat dynamische IP-adressen niet vanzelfsprekend onder de UK Data Protection Act 1998 vallen http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf; zie daarover: Bloemen-Patberg, Zwenne & De Weerd 2009, p. 89.

28 Zie bijv. Ambtsgericht München, Geschäftsn: 133 C 5677/08, 30 september 2008; in voetnoot 15 noemde ik al Cour d'appel de Paris 13ème chambre, section B Arrêt du 27 avril 2007 en section A Arrêt du 15 mai 2007.

29 Vgl. Bloemen-Patberg, Zwenne & De Weerd 2009, p. 90-91.

Het punt is denk ik wel gemaakt. Blijft de vraag of er, gelet op wat er allemaal kan met IP-adressen, toch niet op de een of andere manier beperkingen zouden moeten worden gesteld aan het gebruik ervan, ook als er nog geen natuurlijke personen mee kunnen worden geïdentificeerd. Ik ben geneigd deze vraag bevestigend te beantwoorden. De privacy-implicaties van de technologieën als behavourial targeting, profiling, deep-packet sniffing en data mining lijken ingrijpend genoeg te zijn om daarover ten minste serieus na te gaan denken. Ik zoek dergelijke beperkingen echter niet in de Wbp maar in de telecomwetgeving. Daarin zijn al regels gesteld voor IP-adressen en andere identifiers. Meer daarover in de volgende, voorlaatste paragraaf van deze bijdrage.

Mijn voorstel voor regulering van IP-adressen

In termen van de telecomwetgeving worden IP-adressen aangemerkt als verkeersgegevens, omdat ze worden gebruikt om verkeer via elektronische communicatie (telecom, internet) over te brengen naar computers, routers, PDA's, iPhones en andere devices.[30] Voor verkeersgegevens, en dus ook voor IP-adressen, geldt een aantal specifieke regels, voorzover met deze gegevens natuurlijke of rechtspersonen kunnen worden geïdentificeerd. De hoofdregel is dat telecom- en internetaanbieders verkeersgegevens moeten verwijderen of anonimiseren, zodra ze niet meer nodig zijn voor het overbrengen van de communicatie en de facturering daarvan.[31] Uitzonderingen betreffen het met toestemming van de desbetreffende abonnee gebruiken van de gegevens voor marktonderzoek en de verlening van value added services, alsmede de bewaarplicht ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven.[32]

Er staan in telecomwetgeving geen regels voor IP-adressen waarmee geen natuurlijke of rechtspersonen kunnen worden geïdentificeerd. Er is dus geen regel op grond waarvan bijvoorbeeld ISP's en andere internetdienstverleners (zoekdiensten, ad services enz.) beperkt worden in het gebruik van IP-adressen waarmee geen natuurlijke personen kunnen worden geïdentificeerd. Wel kent de telecomwetgeving regels voor andere, tot op zekere hoogte met IP-adressen vergelijkbare gegevens of identifiers. Voor telefoonnummers van natuurlijke personen is bepaald dat deze alleen in telefoongidsen en informatiediensten mogen worden opgenomen met toestemming van de desbetreffende natuurlijke personen.[33] Ook is bepaald dat de telefoonnummers alleen met toestemming van de desbetreffende natuurlijke personen

30 In een bijlage bij de Telecommunicatiewet is de lijst opgenomen met de verplicht door ISP´s te bewaren verkeersgegevens, waaronder IP-adressen.

31 Art. 11.5, eerste lid, Tw.

32 Art. 13.2a, tweede lid, Tw jo. onderdeel A(c) van de bijlage bij deze bepaling; zie daarover Schmidt & Zwenne 2005; Zwenne & Schmidt 2008.

33 Art. 11.6, tweede lid, Tw.

mogen worden gebruikt voor andersoortige diensten, waarbij vooral moet worden gedacht aan de diensten waarmee aan de hand van het vaste of mobiele telefoonnummer de bijbehorende abonnee kan worden gezocht en gevonden. Op grond dit verbod van 'reversed search' of 'omgekeerd zoeken' is het de telefoonaanbieder niet toegestaan anderen in staat stellen om aan de hand van het telefoonnummer de identiteit te achterhalen van de abonnee die van dat nummer gebruik maakt. De telecomwetgeving voorziet daarmee in waarborgen ter voorkoming van het ongewenst, althans zonder toestemming, identificeren van natuurlijke personen met behulp van telefoonnummers.[34]

Eenzelfde regeling is voorstelbaar als het gaat om IP-adressen. Een eenvoudige regel zou kunnen zijn dat het ISP's niet is toegestaan om anderen in staat te stellen aan de hand van IP-adressen zomaar, althans zonder toestemming, de identiteit te achterhalen van de natuurlijke personen die daarvan gebruik maken. Zo een regel zou het logisch complement kunnen zijn van de bepalingen voor verkeersgegevens. Enerzijds zijn ISP's volgens de reeds geldende regels[35] gehouden IP-adressen in beginsel zo snel mogelijk te anonimiseren of te verwijderen. Zolang de IP-adressen niet zijn geanonimiseerd is het hen anderzijds, volgens mijn voorgestelde regel, niet toegestaan om zomaar zonder toestemming of andere toereikende grondslag anderen in staat te stellen daarmee de abonnees te identificeren.

In aanvulling kan ook worden gedacht aan een regeling vergelijkbaar met die voor nummerherkenning. In de telecomwetgeving is bepaald dat abonnees verschillende rechten hebben met betrekking tot het bekend worden van het nummer waarmee zij bellen. Abonnees hebben het recht om nummerherkenning uit te zetten en anoniem te bellen — dit behoudens uitzonderingen in de sfeer van alarmnummers, anti-stalking en opsporing en vervolging.[36] Een vergelijkbare regel is met enige aanpassingen denkbaar voor IP-adressen. Er zou kunnen worden bepaald dat ISP's aan hun abonnees een faciliteit moeten aanbieden waarmee het mogelijk wordt om het IP-adressen af te schermen voor derden. Als abonnees daarvan gebruik maken, kan dat natuurlijk betekenen dat allerlei internetdiensten niet of niet prettig werken. Maar in elk geval hebben de abonnee dan de keuze, zoals zij dat ook al hadden als zij gebruik maken van telefoondiensten.[37]

---

34 Opgemerkt moet worden dat zowel CBP als OPTA tot dusver het omgekeerdzoek-verbod niet echt willen handhaven. Dit omdat, in de woorden van de telecomtoezichthouder, overtreding van het verbod 'op zichzelf genomen niet als inbreuk op de persoonlijke levenssfeer wordt ervaren', zie OPTA-besluit 17 oktober 2007 (OPTA/IPB/2007/202118). Het CBP-besluit, waarin ook werd afgezien van handhaving, is niet gepubliceerd maar wordt wel genoemd in het CBP Jaarverslag 2008, p. 18 en 41.

35 Art. 11.5 Tw

36 Art. 11.9, eerste lid, onder a, jo. Art. 11.10 en 11.11 Tw.

37 Er zijn op internet verschillende typen van anonymous en pseudomynous remailers beschikbaar, maar de gebruiksvriendelijkheid daarvan laat veel te wensen over. De betrouwbaarheid ervan is niet altijd evident.

Afsluiting

Het mag duidelijk zijn. Wat mij betreft is het onverstandig is om het persoonsgegevensbegrip extensiever te interpreteren en al uit te gaan van identificeerbaarheid als er de theoretische mogelijkheid is dat er met een bepaald gegeven door iets of iemand een natuurlijke persoon zou kunnen worden geïdentificeerd. Wat mij betreft niet alleen onverstandig, maar ook onlogisch, omdat de telecomwetgeving veel meer voor de hand liggende aanknopingspunten biedt.

Onduidelijk is of er meer nodig is. Er worden vanuit heel verschillende achtergronden vraagtekens geplaatst bij de uitgangspunten van privacywetgeving, meer in het bijzonder waar het gaat om het persoonsgegevensbegrip en het identificeerbarheidscriteriumm. Van den Hoven[38] bijvoorbeeld pleit voor een bredere benadering dan die waarbij wordt uitgegaan van beschrijvingen die verwijzen naar individuen ('referential use'). Er zou ook op de een of andere manier moeten worden uitgegaan van beschrijvingen die niet verwijzen naar individuen, maar niettemin 'identity-relevant' zijn:

> "the referential reading of personal data, identity and identifiability of the EU data-protection laws leads to an unduly narrow construal of moral constraints on the use of personal data."

Vanuit een andere achtergrond stelt Prins aan de orde dat privacywetgeving te weinig aandacht heeft voor de veranderende betekenis van 'identificeren' en 'identiteiten' in de informatiesamenleving,[39] alsook dat de bestaande privacywetgeving onvoldoende waarborgen biedt om individuen te beschermen tegen de in bepaalde contexten opgelegde identiteiten.[40]

Ook andere auteurs vragen aandacht voor de uitgangspunten van de privacywetgeving en de privacy-implicaties van de verwerking van gegevens die eigenlijk geen persoonsgegevens zijn, en die dus niet door de Wet bescherming persoonsgegevens worden geadresseerd.[41] Voor deze bijdrage, die al veel meer woorden telt dan de redactie van dit boek heeft bepaald, volsta ik met een verwijzing naar Schmidt.[42] In zijn oratie wijst hij erop dat IP-adressen niet de gebruikers identificeren maar de computer waarvan deze gebruik maken. Maar dat doet er niet aan af, zo zet hij uiteen, dat het verzamelen van IP-adressen en talloze andere gegevens zal leiden tot 'mega-informatieposities' die op de een of andere wijze regulering behoeven, als wij de kwaliteit van rechtsstaat en privacybescherming serieus willen nemen:

---

38 Van den Hoven 2008.
39 Prins 2004a, Prins 2004b.
40 Prins 2009, p. 42.
41 Zie bijv. De Hert et al. 2007, Kindt & Van der Hof 2009, Marbus et al. 2009, Hoving 2008.
42 Schmidt 2004, p. 31.

> "De vraag hoe we informatieposities reguleren is van belang voor de kwaliteit van onze rechtsstaat. In die zin vormen de grote, ik zou bijna zeggen mega informatieposities van de kennisbovenbazen zowel kansen voor bescherming als voor bedreiging. Het op de individu gerichte grondrecht op privacy komt in dit spanningsveld niet erg goed uit de verf."

Een en ander krijgt praktische betekenis in de discussie over IP-adressen. Het komt mij voor dat deze discussie erbij is gebaat als zo af en toe concrete voorstellen worden gedaan. Deze bijdrage moet in dat licht worden gezien.

Verwijzingen

Van Blarkom, Borking & Olk 2003
G.W. van Blarkom, J.J. Borking en J.G.E. Olk (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*, Den Haag 2003.

Bloemen-Patberg, Zwenne & De Weerd 2009
A. Bloemen-Patberg, G-J. Zwenne en T. de Weerd, 'Wie bepaalt wat gebeurt met IP-adressen en verkeers- en locatiegegevens?' in E. Visser & M. Weij (red.), *Who controls the internet* NVvIR Den Haag 2009, pp. 79-97.

Borking & Raab 2001
J. Borking en C. Raab, 'Laws, PETs and Other Technologies for Privacy Protection', *Journal of Information, Law and Technology* 2001/1.

CBP 2002
CBP, *Mag het een bitje minder zijn*? Den Haag 2002.

Van Esch 2008
R.E. van Esch, *Juridische aspecten van elektronische handel*, Deventer 2008.

Van Esch & Blok 2007
R.E. van Esch en P. Blok, 'Privacy en elektronische handel op het internet', in: Berkvens & Prins (red.) *Privacyregulering in theorie en praktijk* Kluwer, Deventer 2007.

De Hert et al. 2009
P.J.A. de Hert et al., 'De WBP na de Dexia-uitspraken', in: *P&I* 2007/4, bldz. 147-157

De Hert & Gutwirth 2004
P. de Hert en S. Gutwirth, 'Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek', in: E.R. Muller (red.), *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn 2004, p. 587-631.

Van der Horst 2004
R.J.M. van der Horst, 'De Wet bescherming persoonsgegevens, gevolgen voor de organisatie en de automatisering', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002, p. 113.

Van den Hoven 2008
J. van den Hoven, 'Information Technology, Privacy, and the Protection of Personal Data', in: Van den Hoven & Weckert (eds.), *Information Technology and Moral Philosophy*, New York 2008, p. 301-319.

Hoving 2008
E. Hoving, 'Modellering van persoonsgegevens en groepsprofielen', in: *P&I* 2008/6, p. 273-280.

Kenny & Borking 2002
S. Kenny en J.J. Borking, 'The Value of Privacy Engineering', *Journal of Information, Law and Technology*, 2002/1.

Kindt & Van der Hof
E. Kindt en S. van der Hof, 'Identiteitsgegevens en -beheer in een digitale omgeving: een juridische benadering', in: *Computerrecht* 2009/2, p. 52/60.

Klitou 2008.
D.G. Klitou 'Backscatter body scanners – A strip search by other means', *Computer Law & Security Report* 2008/24, pp. 316–325.

Koeter 2009
J. Koeter, 'Behavioral targeting en privacy: een juridische verkenning van internet gedragsmarketing', *Tijdschrift voor internetrecht* 2009(4), p. 104-111.

Koorn 2004
R. Koorn et al, *Privacy Enhancing Technologies: Witboek voor beslissers*, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties 2004.

Marbus et al. 2009
R.C.P. Marbus et al., 'Identiteit en openbaarheid in sociale online omgevingen', in: *Computerrecht* 2009/2, p. 64-68.

Prins 2004a
J.E.J. Prins, 'Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy', *Justitiële Verkenningen*, 2004-8, p. 34-47

Prins 2004b
J.E.J. Prins, 'The Propertization of Personal Data And Identities', *EJCL*, Vol. 8.3 October 2004.

Prins 2009
J.E.J. Prins, 'Gezocht: uw identiteit', *Computerrecht* 2009/2, p. 42.

Schmidt 2008
A.H.J. Schmidt, *Bedreigen computers ons rechtssysteem?* 2008.

Schmidt & Zwenne 2005
A.H.J. Schmidt en G-J. Zwenne, 'Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens' *Mediaforum* 2005/9, p. 292-302.

Zwenne et al. 2007
G-J. Zwenne et al, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, Den Haag 2007.

Zwenne & Schmidt 2008
G-J. Zwenne en A.H.J. schmidt, 'Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens', *Mediaforum* 2008/7-8, p. 278-385.

DEEL VI

TRANSPARANTIE

Change We Can Believe In or Politics As Usual?

Government openness and technology under the Obama administration.

Dariusz Adamski■

On 21 January 2009, in his first day in office, President Obama issued a Memorandum entitled "Transparency and Open Government"[1] (the Openness Memorandum), which committed the new administration to transparency, participation and collaboration. Certainly none of those purposes, nor their overarching aim of producing "unprecedented level of openness in Government," as the Memorandum also professed, can be imagined without extensive involvement of information technologies. Aptly recognizing that information produced by his government is a national asset, the new president declared that he would make it readily available online.

This contribution will closely scrutinize the main activities and experiences of the new American administration in respect of transparency, i.e. the policy of making government information readily available to the public. The importance of transparency of government is almost undisputed: underlying data and processes must be visible and broadly available if they are to breed the other important value of participation. Transparency is therefore conditional for collaboration. But its immediate participatory effect is certainly not the only advantage that transparency breeds for democracy.

It is often argued that openness legitimizes democratic processes, that it is a means of civic and social education, and of improving policy outputs. However, does transparency really matter, considering the chasm of expertise between the small group of specialists and legions of generalists? If the latter are (rationally) ignorant about policymaking, then they should not seek the information disclosed through a transparent policymaking anyway. Uninformed majority should therefore ignore it and keep going on largely biased worldviews, disregarding the (potential) educational benefits of transparency. Media should prefer focusing on vivid information as well (like scoops leaked by insider officials-dissidents) rather than invest time in sifting through huge piles of raw data to find out irregularities or otherwise important policy patterns.

Furthermore, politicians in power have very weak incentives to pursue transparency, as it makes them primarily vulnerable to attacks by implicitly

---

■ Dariusz Adamski is assistant professor at the Faculty of Law, Administration and Economics, University of Wrocław.

1 Available at http://www.whitehouse.gov:80/the_press_office/Transparency_and_Open_Government/.

inviting opponents to "air the dirty laundry" of the government. To realize the alacrity with which this invitation should be accepted, just think of two essential features of democracy. First, it is a system of competing leadership. The opposition is thus strongly motivated to exploit transparency for its political purposes. And, second, constituents, because they are rationally ignorant, inevitably rely on heuristics when making their electoral decisions. They are therefore particularly strongly driven by exaggerations and vivid news framed as scandalous, because those attract attention most effectively.

Furthermore, in a transparent political environment, decision makers do not know which information exactly would attract attention of a broader audience. They may be certain, however, that the best they can expect for fulfilling their everyday duties honestly is to be forgotten and ignored by the public opinion, because information about everyday compliance is not particularly attractive for the broader audience. But lapses and mistakes certainly are. And each policymaking process, no matter how carefully construed, ensues huge uncertainties and inevitable slips. So why to expose them voluntarily to media, whose job is to oversimplify stories, and to political opponents, who would exploit the mistakes for their political purposes?

What the politicians also know very well is that being in office requires bargains, tradeoffs, and often choosing lesser evil; in other words – balancing of interests and values. A rational politician, one seeking power and determined to sustain it, may thus share the general conclusion that transparency improves legitimacy of the political system. But he would also know that transparency may interfere with the bargains he is supposed to strike. More government information available to the public, as the argument goes, would rather stir conflict and confuse fellow citizens about pay-offs stemming from political compromises, than would it lead to the much hoped participation. Certainly a government must be checked in order to avoid abuses of power and instances of public resources being wasted, a democratic detractor of transparency may argue further. But if the citizens have no time nor skills to do the oversight directly, then why not to entrust the control task solely to specialists hired either by the government or its opposition? Is not the enhanced transparency of the policymaking process just a waste of taxpayers' money? After all, experts should be much less prone to biases and manipulation. They are better informed and knowledgeable than generalists. It is not by accident that expert performance control in its manifold manifestations, from congressional (parliamentary) oversight to judicial review to independent comptrollers to ombudsmen are heart and soul of liberal constitutionalism.

So why to tinker with the politically treacherous tool of transparency? The experience with the Bush administration provides ample answers. Its obsessive secretiveness and reliance on a small group of chosen experts clearly led to a phenomenon called "groupthink," and (with the hindsight) to blatantly wrong political decisions. Certainly, for some time at least, some of the decisions, as the one to invade Iraq, were broadly supported by the society. But a democratic support built on ignorance and manipulation is a very

undemocratic genre of democracy. As James Madison, one of the America's Founding Fathers, put it famously: "A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both." Even after discounting the most extreme policy mistakes, the American experience under the Bush administration demonstrates that (partisan) experts may be at least as biased as uninformed citizenry (after all, pleasing to wishes of superiors is a very human feature).

At the same time, outside of the political scene there are independent experts – scientists and practitioners affiliated to universities, NGOs, think tanks, or special interests. With sufficient underlying data they can raise the flag when partisan policymakers stray. Those experts may either convince the government, if the "insiders" are receptive enough, or force it with the media, if incumbents do not want to listen, to alter the policy, saving their society's resources and/or liberty. This mechanism is emphasized by many theoretical accounts, from the notion of the public spheres (Habermas 1996) to the idea of a pluralist democracy (Dahl 1972). It gains importance as policymaking grows in complexity and as government bureaucrats loose their ability to cope with uncertainties thus engendered. Enhanced demand side for transparency is coupled with greater, and more diversified, supply side of the external expert knowledge. Better general education produces more experts who compete for attention and recognition more vigorously.

But what impact may those external experts have on generalists, who should arguably be unwilling (and rationally so!) to comprehend expert arguments? If the theory of rational ignorance is true, then more information produced by specialists increase the costs of comprehension for generalists, and this effect may further discourage average citizens from becoming interested in policy issues in the first place. At the same time relying on media as information cost economizers may prove inefficient, for they have multiple reasons to oversimplify or put a certain spin on information they purport.

To a certain extent those arguments explain some democratic inefficiencies. But, as a principal matter, media outlets which are not credible (those that misrepresent facts) do not economize on information. They in fact enhance comprehension costs for the receiving audience. Rational individuals will therefore switch off those outlets (this is how they handled official media propaganda in communist countries), or tune to other media outlets in a competitive media environment. The media certainly please to biases of receivers. But, first, this process is inevitable in a commercially driven media landscape. Second, it is necessary in a society built on a liberal (and extremely apt) assumption that no authority should be authorized to administer interpretations of true facts because no authority can be certain what interpretation is accurate before it is released to the society.

Simplifying, aggregating and filtering are manifestations of economizing on comprehending information. Therefore charging media for oversimplifying complex policy issues is not right. A voter (and one should not expect from the majority of a capitalist society more than casting a vote every few years) does not need detailed policy information to choose reasonably at

the ballot box. As electoral preferences are shaped by heuristics, a rational voter should want to learn whether the incumbent government is making the country safe and prosperous enough to "renew the electoral contract." Moreover, she should care whether past achievements of a candidate warrant his integrity, impartiality, and efficiency when elected. Paying attention to strong signals, blatant instances of politicians diverging from those principles is therefore an expression of media properly economizing on information. And it ensues perquisites for the media, because scandalous news are much more entertaining for the most of the readers than, for instance, detailed analyses of fiscal policy options. Media, therefore, adjust the profile of information, and its complexity, to rational expectations of their audiences. By the same token, they should not be too much preoccupied with nuts-and-bolts of policymaking processes, because this type of information breeds additional costs of comprehension – it is not a particularly strong attraction for the audience. But, of course, irregularities matter heuristically and they make attractive news. Media are therefore motivated to investigate the government data when this can reveal important and unexpected policy patterns and add variety to the news menu. Transparency is a prime mechanism for detecting as many of the irregularities as possible, and for calling policymakers to account as a consequence.

So accountability is the very crux of transparency. The latter adds one more layer to the more institutionalized accountability mechanisms. It therefore propels a process which is profoundly democratic (and intrinsically republican, in the classical sense of this term): of constant exacting and improving the mechanisms of government's performance. In short, the more accountable a political system, the more democratic it gets. Certainly generalists will not know which information on performance of those in power is important, especially which performance irregularities are harmful (and should be heeded by the public opinion) and which are not (and should be ignored in order to save time and efforts of the public). But, as discussed earlier, competing information economizers (intermediaries) are generally eager to help the generalists in this respect.

Transparency allows for economizing on information yet in another way. It allows for improving efficiency and compliance with the rule of law by those in power even with no member of the public in fact overseeing them. When the probability that someone, an information intermediary in the first place, would pay attention to a given policy pattern is high enough, the very expectation of this taking place is a very strong self-correcting motive for the public servant. In such a situation the benefit of accountability may be realized without anyone incurring the costs of calling to account.

There are many more grave arguments why democratic societies instinctively crave for transparency. One reason is that no authority may know who exactly would make the best of the government information and thus who should receive it. In an educated society a generalist in one policy area easily becomes an expert in another. So a software developer with no formal education in law may become a conversant reviewer of his government's patent

policy and a part-time artist working for an environmental NGO may be able to argue meaningfully how the environmental policy should be improved. There is no other way to allow those people to improve their positions (the educational aspect), and tap their expertise into the policymaking process (the output improvement aspect) than to conduct the policymaking processes transparently.

Furthermore, no authority is able to predict all the beneficial and ingenious uses of the data produced by the government. With an unencumbered access to it, entrepreneurs will reuse the data according to the particular needs of theirs, and finally – of the society. This socially enriching process cannot take place without input information produced and contributed by the government.

In four of the recent projects of the U.S. federal government information technologies have been used creatively to enhance transparency of the policymaking. Barack Obama, either as a senator or a president, was directly involved in shaping all of them.

The first of the projects stems from a piece of the federal legislation entitled: The Federal Funding Accountability and Transparency Act of 2006 (FFATA). The act aims at "full disclosure of entities receiving federal funding" (title of its Sec. 2) through "a single searchable website, accessible by the public at no cost" (Sec. 2(b)(1)). The website, http://www.usaspending.gov, was launched in late 2007.

USASpending provides very useful information on how the federal funds are spent. Interestingly, however, and congruently with what has been said earlier about ingenious applications an innovative society produces once it has access to government data, drafting the FFATA and setting up USASpending with the taxpayers' money turned unnecessary. USASpending is built on data feeds otherwise available as public information. And by the time the FFATA was signed by the president, the OMB Watch, a nonpartisan NGO promoting transparency and government accountability, launched a website (http://www.fedspending.org) compliant with both the purposes and the requirements of the act and based on exactly the same information as the USASpending would.[2]

In the following projects the federal government has not made the same mistake of attempting to redo well functioning efforts of NGOs so bluntly. Recovery.gov, the first of those projects, was established under Sec. 1526 (entitled "Board Website") of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5; known as the Stimulus Bill). Following the statutory

2 The OMB Watch sold the system's underlying technology to the federal Office of Management and Budget, responsible for putting the FFATA into practice, making more than $150.000 of profit. A three-year grant of the Sunlight Foundation the OMB Watch had received to develop FedSpending.org amounted to $334,272, while, according to the Washington Post (E. Williamson, OMB Offers an Easy Way to Follow the Money, Dec. 13, 2007, available from http://www.washingtonpost.com) the federal government paid for its technology $600,000.

language, the portal, among others, provides general information on the Stimulus Bill and makes official plans, reports, and contract solicitation information available online. Most importantly it allows (to some extent at least) to track who pays whom for what within the Stimulus Package. To use the specific language of the Stimulus Bill, the website comprises "detailed data on contracts awarded by the Federal Government that expend covered funds, including information about the competitiveness of the contracting process, information about the process that was used for the award of contracts, and for contracts over $500,000 a summary of the contract" (Sec. 1526(c)(4)). Contract summaries cover the most important contractual parameters, like purposes, deadlines, and detailed budgets of grants or loans. On the other hand, however, as in USASpending, Recovery.org does not disclose the whole, searchable stimulus contracts (nor further sub-contracts), and therefore it does not allow for a thorough discerning of the practical impact their detailed provisions exert.

The next innovative transparency initiative of the Obama administration is called "IT Dashboard,"[3] and was described by the White House blog as "a new, one-stop clearinghouse of information that allows anyone with a web browser to track federal IT initiatives and hold the government accountable for progress and results."[4] More specifically, the system (launched in June 2009), a recent upshot of USASpending, provides very sophisticated visualization tools for the evaluation of federal information technology investments. On the most general level, it visualizes the portfolio of major IT investments in each federal agency. It displays graphically the details of every such an investment by major performance indicators (cost, schedule, evaluation by the agency's chief information officer and an overall score), reveals contact data of officers responsible for the investment performance and (some) information on contracts awarded. Sophisticated analytical tools (like motion charts, treemaps, or scatterplots) allow for visual comparisons between different agencies and points in time. When launched, the IT Dashboard was probably the most innovative, sophisticated, and at the same time entertaining among official applications for analyzing government performance.

The last of the innovative tools discussed here is less entertaining but much more valuable for the society. It was launched in spring 2009 under the name Data.gov, as a warehouse of all the government data freely available to the public. According to its originator, the Federal Chief Information Officers Vivek Kundra, the application "is a platform that's going to democratize the data that the taxpayers have already paid for."[5] Data.gov provides access, in various formats, to hundreds of datasets produced by the federal agencies

3 http://it.usaspending.gov/.

4 Welcome to IT Dashboard – The Blog!, July 13, 2009, available from http://www.whitehouse.gov/blog.

5 An interview available from the Open Government Innovations Gallery, http://www.whitehouse.gov/open/innovations/Data/.

and compliant with the federal information quality standards.[6] One can search the data by category, keyword, agency, and/or format, download either raw data or document file formats, view metadata information about each dataset and, sometimes, subscribe the data (RSS or Atom Feeds) and receive access to additional functionalities provided by the agencies (Widgets). Thus, for instance, one can download the "2006 Toxics Release Inventory data for the state of New York" in the machine-readable CSV/TXT format (at the time of this writing there were almost 600 machine readable datasets available through the "Raw Data" catalogue of the website), or the "2008 Medicare and Medicaid Statistical Supplement" available through the webpage of the Department of Health and Human Services in PDF files. A separate "Geodata" catalogue links to geospatial datasets and related metadata information. As a manifestation of the Gov 2.0 approach, users can rate Data.gov datasets and send suggestions about other public information sources which should be disclosed through the system.

A comparison between all four applications (USASpending, Recovery.gov, IT Dashboard and Data.gov) points at two trends of how the federal government harnesses IT when developing the tools. First, it has attempted to make the public data available in more attractive forms, more useful at the same time – the government provides raw public data together with tools for manipulating them and drawing policy conclusions on the basis thereof. The latest application, IT Dashboard, is the best example of this trend. Second, the data has been released in more comprehensive, machine readable datasets. This feature, demonstrated primarily by Data.gov, facilitates customizing the records to the needs of particular external users and tools outside the government websites.

Those trends are blurred by one, yet important exception: the $700 billion bank and auto bailout program (Troubled Assets Relief Program: TARP). To recall: responding to the subprime mortgage crisis, the Bailout Bill ("Emergency Economic Stabilization Act of 2008," Pub.L. 110-343), signed by the president Bush in October 2008, authorized the U.S. Secretary of the Treasury to buy up distressed assets and inject capital into banks. Sec. 114 of the act provides for public disclosure obligations of the TARP recipients. As the bill explicitly states, "[t]o facilitate market transparency, the Secretary shall make available to the public, in electronic form, a description, amounts, and pricing of assets acquired under this Act, within 2 business days of purchase, trade, or other disposition" (Sec. 114(a)). What is particularly important for the further discussion, the same section says that "For each type of financial institutions that sells troubled assets to the Secretary under this Act,

6 According to Sec. 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554) general information quality standards are set by general OMB guidelines (currently Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies, Final Guidelines (corrected), 67 Fed. Reg. 8452 (Feb. 22. 2002)). More specific standards are enacted by each agency.

the Secretary shall determine whether the public disclosure required for such financial institutions (…) is adequate to provide to the public sufficient information as to the true financial position of the institutions. If such disclosure is not adequate for that purpose, the Secretary shall make recommendations for additional disclosure requirements to the relevant regulators" (Sec. 114(b)).

One thing in the statutory language is particularly important – the quality and quantity of the data revealed to the public depends entirely on the requirements indirectly imposed on the bailout recipients by the Secretary of the Treasury. The Treasury Department did put up a website of the TARP (http://financialstability.gov), but neither the previous Secretary of the Treasury, Paulson, not the new one, Geithner, have seemed to care much about the disclosure requirements. Especially Geithner, member of the team allegedly committed to unprecedented accountability and transparency, provoked stark criticism of the public opinion. In an article entitled "How Obama's transparency promise holds up," CNNMoney.com asked important questions for which not only the public, but the Treasury Department itself had no answer due to insufficient disclosure obligations: "How are banks using TARP funds? Who are bailed out banks lending to? What is the value of the assets that the Treasury has accumulated as a result of TARP? Where are stimulus funds ultimately going? (…) The Treasury Department states on financialstability.gov that the $204 billion in capital investments in banks are "for stability or lending." But it does not require banks who have received the funds to show how they are using the money."[7] Answering those questions is vital not only for the public at large and its confidence in the policymakers, nor for the press and its ability to form the public opinion about the program, but also for the proper functioning of the institutionalized accountability mechanisms. In July 2009 the Special Treasury Department Inspector General (the TARP cop, as often nicknamed) criticized the Treasury Department for playing down the federal financial commitments to the TARP. The Treasury fought back, claiming that the Inspector General exaggerated his calculations of the rescue efforts. In his reaction to this stance, the Inspector General, as reported by the media, "took offense at Treasury's accusations that his figure was inflated, saying that he got the data from Treasury and Federal Reserve's Web sites."[8] Clearly, therefore, public disclosure (or lack) of detailed and up-to-date information on how the program works is fundamental not only for "unofficial" accountability mechanisms, but also for the ability of the institutionalized watchdogs to fulfil their tasks properly.

It is still to be seen how the TARP transparency problem would be solved. A legislative intervention is one of the solutions considered, and in

7 D. Goldman, Aug. 14, 2009, available from http://money.cnn.com.

8 J. Liberto, TARP cop wants bank accountability, CNNMoney.com, July 27, 2009, available from http://money.cnn.com.

March 2009 Congress was addressed with an amendment proposal. A draft bill "To amend the Emergency Economic Stabilization Act of 2008 to provide for additional monitoring and accountability of the Troubled Assets Relief Program" (H. R. 1242) provides, among others, that the Secretary of the Treasury "shall provide (…) ongoing, continuous, and close to real-time updates of the status of funds distributed (…) through a standardized electronic database that combines all of the necessary information from existing public and private sources to track the status of the funds distributed under this title" (draft Sec. 113(e)(1)). In fact, however, the Bailout Bill as quoted earlier sufficiently authorizes the Treasury Secretary to require, obtain, and publish information necessary for tracking money spent through the TARP. One only has to read the Bailout Bill together with the Obama administration's guidelines on openness and press the Treasury Department to act accordingly.

The TARP example focuses attention on legitimate parameters of information disclosure – which information should, and which should not be made public; which records to release and which to withhold. This question becomes more vital for transparency in action than expressions of government innovation in presenting indisputably public data. It is also more informative for the assessment of the Obama administration's transparency policy and its overall democratic weigh.

At the level of general declarations the new U.S. government has fared much better than the Bush administration. The same day the Openness Memorandum was issued, the new president signed a Memorandum on the Freedom of Information Act[9] (FOIA Memorandum; the Freedom of Information Act (FOIA), 5 U.S.C. § 552, is the main statutory instrument of disclosing information produced by federal agencies). The Memorandum provided lucidly that "[t]he Freedom of Information Act should be administered with a clear presumption: In the face of doubt, openness prevails. The Government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears. Nondisclosure should never be based on an effort to protect the personal interests of Government officials at the expense of those they are supposed to serve." By establishing the presumption of openness the president implicitly, and later on the Attorney General explicitly (in a memorandum on the same issue),[10] encouraged discretionary (voluntary) disclosure of public information.[11] According to both the documents combined, federal agencies should make public infor-

9 Available from http://www.whitehouse.gov.

10 FOIA Guidelines of the Attorney General Holder – Memorandum of March 19, 2009, available from http://www.usdoj.gov/opa/pr/2009/March/09-ag-253.html.

11 Discretionary (proactive) disclosure is not preceded by a request. The information, therefore, is not disclosed to a requesting individual, but made publicly available on an agency's website.

mation generously available to the public, by narrowly construing exceptions and voluntarily putting online as much public information as possible.

Case after case, up to the moment of this writing at least, the way the new administration has handled the promise of broadening the scope of government information available to the public has been almost uniformly disheartening. It has clearly diverged from the campaign promises and subsequent general declarations of the new administration.

Insufficient disclosure discipline of the TARP recipients was one of the first disillusions, even though its logics and trajectory was drafted and implemented by the previous administration, and therefore the new one cannot be entirely blamed for it. But its negligence in bringing about the change promised during the presidential campaign was characteristic of other actions, for which the Obama administration bears a sole responsibility.

The promise of posting legislation before signing it by the president is a simple instance of this problem. On his presidential campaign website Senator Obama announced that, as a president, he "will not sign any nonemergency bill without giving the American public an opportunity to review and comment on the White House Web site for five days." It turned out, however, that after his first 100 days in office only one out of 14 signed bills had been posted for the promised five days.[12] In the policymaking terms this slip is not a grave one, because a website of the Library of Congress (http://thomas.loc.gov/) provides ample information on pending legislation. But the discomfort of seeing the practice discordant with campaign promises remains. And it was soon amplified by other decisions clearly diverging from expectations towards a man who used to be such a staunch opponent of "the politics as usual."

The whole cluster of cases involving the "war with terror" will instantiate the process. But before turning to them, two other examples should be mentioned.

The first one regards the logs of visitors to the White House. The Bush administration demonstrated its disregard for transparency and accountability by, among others, concealing information on the industry representatives whom the White House top-officials were meeting (and consulting) on policy-issues. The presidential candidate Obama promised to meet openly with the industry, in order to eliminate suspicions of unethical behavior of his administration and to let the public learn the arguments of the industry representatives for the policy choices they favor. But when the news broke out that the new president is convening meetings without even informing the public about who would participate, FOIA requests for information on who visits the White House ensued. To be more specific, the MSNBC.com requested the names of all White House visitors since Jan. 20, 2009, and the Citizens for Responsibility and Ethics in Washington (CREW), a non-parti-

12 D. McCullagh, After 100 Days, Obama's Transparency Vow Receives Mixed Reviews, April 29, 2009, available from http://www.cbsnews.com/blogs.

san organization, sought records about enumerated executives of leading coal and healthcare companies. But the Secret Service, responsible for maintaining the records, turned down all the requests. Supporting the decision in court,[13] the new DoJ simply followed the argumentation of the Bush administration, according to which the Secret Service logs are presidential information, not agency records (because the White House is not a federal agency), and therefore the requests exceed the parameters of what may be legitimately disclosed under the FOIA (this act covers records of federal agencies only). Surprisingly, however, the Obama DoJ did not heed that the very same court which hears the visitors' logs disputes, has already decided a very similar case, submitted by the very same plaintiff.[14] The court had no doubts that the Secret Service is bound by the FOIA because it falls under the Department of Homeland Security (which is indisputably an agency).

The storyline of the other example starts when a 2003 article in the Washington Post revealing the identity of a covert CIA agent spurred what has been subsequently called a "Plame affair" and which in turn led to a so called "Valerie Plame Wilson leak investigation." As part of the investigation the FBI interviewed the then Vice President Dick Cheney, accused by some to be the man behind the scene of the leak. When in 2008 the CREW requested records relating to this interview, the Bust administration balked. Soon after, when the dispute reached the court,[15] the Obama DoJ once again vindicated the stance of its predecessors and argued that the interviews should be withheld pursuant to the FOIA Exemption 7(A). This exemption covers "records or information compiled for law enforcement purposes" whose disclosure "could reasonably be expected to interfere with enforcement proceedings" (5 U.S.C. § 552(b)(7)(A)). The DoJ asserted that publicity of law enforcement interviews with senior White House officials not only would politicize the investigations, but, lacking the certainty that their interviews remain confidential, those officials would be discouraged from sharing information with law enforcement agents, to the detriment of the investigatory efforts. Such an outcome could be "reasonably expected," argued the DoJ, and therefore the documents could not be disclosed. The question before the court thus boiled down to whether the effect asserted by the defendants may be anticipated reasonably enough to justify the disclosure exemption. Certainly the answer depends on what one understands by the "reasonable expectation," which, in turn, is predicated on how well one understands the nature and how much does she appreciate the functions of openness and accountability. The plaintiff assumed that the top officials should have nothing to hide. And if so, why would they be untruthful with the law enforcement officers? Conversely, the argumentation of the new DoJ leads directly to the conclusion

13 Two cases pending before the District Court for the District of Columbia.

14 CREW v. DHS, 527 F. Supp. 2d 76, 98 (D.D.C. 2007).

15 CREW v. DoJ, Case No. No. 1:08-cv-01468 (EGS), pending before the District Court for the District of Columbia.

that it may be "reasonably expected" that every top White House official is at least aware of actions so reprehensible that he may attempt to hide related information from the public opinion. Certainly one would not expect such an argumentation from the administration so ostensibly deprecating the "politics as usual." This logics, and the signals it imparts, may be disastrous electorally for the administration, because lacking integrity of leaders is one of the few issues the electorate takes into account at the ballot box. This stance may be treacherous from the legal perspective as well, because jurisprudence has rejected the rationing presented by the defendants. In a case instructive for how the requirement of the "reasonable expectation" in the Exemption 7(A) is to be understood, a court made it clear that the expectation may only refer to enforcement proceedings "pending or contemplated".[16] Only a "concrete" prospect satisfies the requirement of law enforcement proceedings being contemplated.[17] And, what is particularly important from this perspective, the Valerie Plame Wilson leak investigation was over when the Obama DoJ refused to disclose the Cheney interview, and there were no other related proceedings, pending or contemplated. By the same token, no interference with enforcement proceedings could be reasonably expected.

Unfulfilled promises about openness in signing legislative bills, policy meetings with industry, or the role of the previous Vice President in a CIA leak affair may have been irritating for those of the Obama supporters who wanted to see him fulfilling the promise of the real "Change in Washington." Yet graver examples of practices discordant with the grandiose policy commitments refer to the war with terror, an issue particularly difficult to handle in a democratic society because of two fundamental, yet contradictory, values it involves: national security and civil liberties. Balancing them is tricky – both overprotection and underprotection may be devastating. Quite strikingly, however, the practice of the new administration, despite all its pledges to entirely different standards of openness, has supported the secretiveness of the Bush era in almost every of its manifestations.

The thesis will be illustrated with several specific examples, which in turn will be drawn against the background of the legal issues involved.

The first one, of secret electronic surveillance, may be the most muddled of all. It springs from unnecessarily secret operations of the Bush administration. The administration unnecessarily invoked "unaccountability doctrines" when the plot leaked to the press and the (rationally) infuriated public unnecessarily (and unsuccessfully) challenged the operations in courts. Finally the Obama administration stepped in and unnecessarily upheld those "unaccountability doctrines."

Still pending Jewel et al. v. National Security Agency et al.[18] illustrates the grotesque vividly. But before turning to this particular case, a few sentences

16 Coastal States Gas Corp. v. Department of Energy, 617 F.2d 854, 870 (D.C.Cir.1980).
17 Carson v. U.S. Dep't of Justice, 631 F.2d 1008, 1018 (D.C. Cir. 1980).
18 Case No. 08-cv-4373-VRW.

of introduction to the issue is necessary. Jewel is a progeny of the public uproar which burst in December 2005, when the New York Times published an article about (an) electronic surveillance program(s) instituted by the National Security Agency (NSA) in liaison with the AT&T (and other telecommunications companies) after the 9/11 attacks.[19] Only in early 2007[20] the Bush administration promised to seek court approvals, as required by the Foreign Intelligence Surveillance Act of 1978 (FISA, 50 U.S.C. 36), when undertaking domestic surveillance actions (interception of communication). Instead of amending the FISA appropriately at the very beginning of the war with terror, only in mid-2007 Congress reformed the FISA so that the judicial approval procedure be expedited as postulated by the intelligence community.[21] By the same token, it is quite clear that for about five years (2002-2007) the NSA had been involved in practices breaching the FISA.

Bringing their action against the NSA in Jewel, the plaintiffs, AT&T customers, sought damages for, as they described it, "an illegal and unconstitutional program of dragnet communications surveillance conducted by the National Security Agency (the "NSA") and other Defendants in concert with major telecommunications companies."[22] The plaintiffs believed that their communications and/or communications records (the information who communicates with whom when) had been intercepted. They felt their privacy was violated and sued in reaction. The first question was, therefore, what damage they incurred, and whether there was any damage at all for which the agency could be held liable.

The FISA determines procedures the intelligence agencies must follow in order to use information acquired from electronic surveillance, including the scope of the judicial review (50 U.S.C. § 1806). The act makes it clear that "willful disclosure or use by an investigative or law enforcement officer or governmental entity of information" obtained without a FISA court order authorizes an aggrieved party to sue the government for civil damages (50 U.S.C. § 2520). For the Jewel plaintiffs this means that whether their communications had been intercepted illegally is one thing. But another is whether communications or communications records have been used by the NSA (or other law enforcement agencies) against any of the plaintiffs. Because the latter apparently did not happen (which is very much why the plaintiffs could

---

19 J. Risen, E. Lichtblau, Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say, Dec. 15, 2005, available from http://www.nytimes.com.

20 The first authorizing orders were issued by the relevant (FISA) court in January 2007, confessed the then Attorney General Gonzales in a well known letter to the Senate Judiciary Committee. The letter is available at http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf.

21 Protect America Act of 2007 (Pub.L. 110-55) and FISA Amendments Act of 2008 (FISAAA, Publ. Law No: 110-261). Constitutionality of the FISAAA, which introduced permanent amendments to the FISA, was confirmed by a District Court in June 2009 – see Judge Rules Telecoms Have Immunity Under Unconstitutional FISA Amendments Act, June 3rd, 2009, available from http://www.eff.org.

22 Cf. http://www.eff.org/files/filenode/jewel/jewel.complaint.pdf.

not prove that the interception indeed took place), the aggravation was merely speculative.

On the one hand, therefore, the Bush government should have avoided spying on Americans for the very reason that using an evidence thus produced in any court proceeding could only lead to an action for damages against the intelligence agencies. But, on the other hand, the government could win the Jewel case solely by claiming that the plaintiffs were not able to present a prima facie case, because they could not demonstrate an injury-in-fact – a fundamental element of a claim for damages.[23] But, instead, the Obama administration picked up the arguments which clearly connote the logics of unaccountability so much appreciated by the previous administration and condemned by the then presidential candidate Obama. More importantly for the current discussion, the Bush administration's arguments endorsed by the Obama DoJ fly in the face of transparency and openness. The first of those arguments is sovereign immunity. When expressly provided for in a statutory act (and Sec. 223 of the Patriot Act did introduce it to surveillance legislation, including FISA) the sovereign immunity shields the federal government from being sued, unless the immunity has been clearly waived by a more specific statutory provision.[24] This legal trick, therefore, deprives the court before which the case is pending of its jurisdiction, and thus it eliminates the accountability mechanism of the judicial review. So even when legally available, sovereign immunity is not an argument one could expect from a government pledging to accountability and unprecedented openness. The Obama administration, however, used it so fiercely[25] that the Electronic Frontier Foundation, one of the plaintiffs, had good reasons to assert that: "In Warrantless Wiretapping Case, Obama DOJ's New Arguments Are Worse Than Bush's."[26] The new administration also embraced another favourite argument of its predecessors, of the state secrets privilege. As applied in Jewel, this evidentiary privilege bars disclosure of information by the government when "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged."[27] In practice this privilege has been invoked by the executives mainly to avoid judicial scrutiny in cases when military actions may clash with civil rights and freedoms. Pronounced to pursue the public good, it promises the executive an escape from accountability when the most ruthless state coercion instruments are in action, and therefore when the state is the most dangerous for the society. Moreover, the state secrets privilege is based on circular logics.

When the Court of Appeals implicitly vindicated the privilege in a very

23 Lujan v. Defenders of Wildlife, 504 U.S. 555, 559-60 (1992).
24 Dep't of the Army v. Blue Fox, Inc., 525 U.S. 255 (1999).
25 Notice of Motion to Dismiss, filed on Apr. 3, 2009, available at http://www.eff.org/files/filenode/jewel/jewelmtdobama.pdf.
26 http://www.eff.org:80/deeplinks/2009/04/obama-doj-worse-than-bush.
27 United States v. Reynolds, 345 U.S. 1, 10 (1953).

similar case brought by (almost) the same plaintiffs against the AT&T,[28] an attorney of the American Civil Liberties Union (ACLU), Melissa Goodman, concluded: "They are effectively saying you can't show that you've been wiretapped and you'll never be able to show that you've been wiretapped because the whole thing is so secret."[29] All in all, the state secrets privilege fits very poorly into a democratic legal system. It is used only because of its convenience for the government aware that the judiciary will not be eager to interfere with its assessment of what the national security and military matters demand.[30] But it is certainly not an argument which may strike the right balance between national security and civil liberties.

The very same dilemmas are pertinent to another example. It was mentioned earlier that the FOIA Memorandum encouraged federal agencies to shift towards the presumption of openness. By coincidence, two days after the president Obama announced his FOIA Memorandum in January 2009, the DoJ presented a document also entitled "memorandum" (in support of motion for summary judgment) in a case filed by the Electronic Frontier Foundation (EFF) against the FBI (Electronic Frontier Foundation v. Dep't of Justice, Docket No. 06-cv-1773 (D.D.C.)). The dispute originated when the EFF requested disclosure of records responding to certain questions about an FBI's massive searchable database of counterterrorism and investigative data, called "Investigative Data Warehouse" (IDW, often vividly described as "über-Google"). The FBI identified almost 900 pages of relevant documents, out of which 800 were released in a full or redacted form. Access to the remaining part was refused on the basis of disclosure exemptions of the FOIA.

Certainly the FOIA Memorandum issued at about the same time could have no impact on those very pleadings developed and submitted yet by the previous administration. Soon later, however, the judge ordered the FBI to clarify whether its position would change under the new administration and its allegedly different approach towards openness. In April, 2009, a month after the very same Department issued new FOIA Guidelines swopping the previous informal presumption of non-disclosure for a formal presumption of openness, the DoJ responded "that it does not currently seek to amend Defendant's Motion for Summary Judgment or the materials filed in support

28 ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007).

29 A. Hopkins, Court dismisses lawsuit on spying program, Reuters, Jul 6, 2007, available from http://www.reuters.com.

30 For an explication of the judicial approach: Halkin v. Helms, 598 F.2d 1, 8-9 (D.C. Cir. 1978): ("[C]ourts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in that area"); CIA v. Sims, 471 U.S. 159, 180 (1985) ("[i]t is the responsibility of the [intelligence community], not that of the judiciary to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the … intelligence-gathering process.").

of the motion."[31] Period. The EFF eagerly pointed this out as a sign that the Obama transparency commitments proved false. The organization stressed that the DoJ should have reconsidered its position regarding at least two of the eight FOIA exemptions it invoked in this case: internal personnel rules and practices of a relatively trivial nature (the so-called "low-2 Exemption") and the deliberative process privilege (sub-part of the so-called Exemption 5).[32] The EFF argued that situations potentially falling into those two categories were recognized by the new FOIA Guidelines of the DoJ as particularly well fitted for "discretionary release."[33] As the EFF summed up, "[i]t is truly remarkable that, in the face of the stated policy encouraging "discretionary releases" of requested information, the FBI has now seen fit to continue to withhold *every single word* it withheld prior to the new administration's purported change in direction."

Let us leave aside the argument regarding the low-2 Exemption.[34] Accusations of the EFF regarding the Exemption 5, however, deserve attention. This exemption essentially protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party … in litigation with the agency" (5 U.S.C. § 552(b)(5)). As such, it has been construed to "exempt those documents, and only those documents, normally privileged in the civil discovery context."[35] The FBI, invoking this exemption, withheld its internal emails containing "predecisional discussions of policies, processes, or IDW systems content or design" and other "FBI planning and assessment documents, all of which were predecisional in nature." The material comprised of, among others, a draft memorandum of understanding ("MOU") between the FBI, the Department of Homeland Security and the Department of State, portions of an agenda of a meeting on the IDW, draft IDW Privacy Impact Assessments (some of them with handwritten com-

31 Defendant's Notice in Response to the Court's February 11, 2009, Order, dated April 13, 2009, available from http://www.eff.org/files/filenode/foia_idw/doj_idw_notice_re_foia_guidelines.pdf.

32 D. Sobel, Obama's Transparency Promise: We're Still Waiting, April 19th, 2009, available from http://www.eff.org.

33 As explicated by the Office of Information Policy, US Department of Justice, President Obama's FOIA Memorandum and Attorney General Holder's FOIA Guidelines. Creating a "New Era of Open Government," available from http://www.usdoj.gov/oip/foiapost/2009foiapost8.htm.

34 The Exemption 2 is broader than its low-2 component alone, and comprises the so called high-2 category as well, which refers to more substantial internal agency matters. Contrary to what the EFF claims, the DoJ had invoked the Exemption 2 in general, without distinguishing between its high or low categories. More importantly, information withheld on the basis of the Exemption 2: "data source, data process, computer application, and systems design information" fits also (and in fact more properly so) into another category of access exemptions (Exemption 7(E)), which refers to records disclosing "techniques, guidelines and procedures for law enforcement investigations or prosecutions, if such disclosure could reasonably be expected to risk circumvention of the law" and could be exempted successfully on the sole basis thereof.

35 NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 149 (1975).

ments by legal counsel) and other records containing "attorneys' opinions on legal issues related to the IDW discussed within an internal FBI email system." Quite clearly, therefore, the scope of the documents was broad, exceeding information privileged in the civil discovery context. In other words the DoJ (both of Bush and Obama) supported an expansive reading of the Exemption 5, one generously providing the policymakers with, as the DoJ put it, "frank discussion of legal and policy issues within the government." As the administration argued, its position was, first, "to encourage frank discussion of legal and policy issues within the government, and to protect against public confusion resulting from disclosure of reasons and rationales that were not ultimately the bases for the agency's action" and, second, to enable the withdrawal of material which may raise doubts over legality of the IDW. On this reading, minimum transparency is tolerated (an outcome of the decision-making process, e.g. the final IDW Privacy Impact Assessment, has been disclosed), the public opinion is discouraged from discussing the issue ("to protect against public confusion"), and officials are provided with ample "space to think." Detractors of transparency could also add that decision-makers, once the argumentation of the DoJ is endorsed, are not forced to avoid written (and therefore traceable) communication for airing their concerns about legality or rationality of the policies developed by their agencies. In this scenario the government is held accountable for outcomes, not for processes.

Because, however, of its commitments to openness, participation and transparency, it is really unfortunate that the Obama administration decided to defend such a position. The public, represented by the EFF in the case, seems to be predominantly concerned whether the system is compliant with the law (of privacy in the first place), whether it guarantees accuracy of personal records and precludes misrepresentation and abuse. System design and investigative methods aside (those were clearly protected from disclosure by other FOIA exemptions) information about legal considerations raised or neglected, taken into account or refused in the process of developing the system, when revealed, would motivate policymakers in this and in other projects to determine all the possible legal loopholes and address concerns expressed in the development process more thoroughly. Additionally, the FOIA Memorandum clearly proclaimed that "the Government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears." It is another reason why the new DoJ should not be as conservative about its interpretation of the Exemption 5 as the previous administration.

The next (and the last) two examples of the Obama administration treading down the path set by its predecessors involve the most repulsive aspects of the war on terror. And they are particularly disturbing because, on the one hand, they refer to issues very sensitive from the perspective of civil liberties and, on the other, they are clearly dubious from the legal standpoint.

Some time after 9/11 attacks the public opinion learnt about the CIA's

Extraordinary Rendition Program (ERP) of secret transferring suspect foreign terrorists to countries where no human rights protection could shield them from interrogation techniques running afoul of international and American laws. The Jeppesen Dataplan, Inc., a subsidiary of Boeing, allegedly provided logistical support to missions to those overseas detention and torture facilities. In Binyam Mohamed v. Jeppesen Dataplan, Inc. five aliens processed through the program sued the Jeppesen Dataplan company for damages, invoking the Alien Tort Statute, 28 U.S.C. § 1350 (the act enables foreigners to claim damages for torts before U.S. courts, even if the damage is done outside the U.S. territory). The Bush administration intervened, claiming that the state secrets privilege precluded the litigation altogether, because high ranking officials confidentially declared to the court that the very subject matter of the case is a classified military secret. A district court vindicated this position and dismissed the case at the outset. The appeal therefore focuses on whether the state secrets privilege could apply to such a case, depriving the plaintiffs of the judicial protection. To the disappointment of many civil rights activists (and Obama supporters) the new administration entirely upheld the arguments of the previous administration regarding the privilege.

The indignation about the government's position became even deeper when the Court of Appeals reversed and remanded for the lower court. In his order of April 28, 2009 a judge acting for the court rejected the very idea that the government may preclude adjudication altogether by merely stating that the "very subject matter" of the litigation has something to do with classified information. He agreed that the privilege may restrict certain testimonies (after all, the privilege asserted by the government in this case is of evidentiary nature), but it cannot deprive plaintiffs of standing across the board. Doing this would be tantamount to depriving the plaintiffs of a chance to establish their prima facie case with evidences other than the classified documents. By the same token, Jeppesen would be deprived of a chance to defend itself without the privileged evidence. The most crucial is the part of the judgement condemning the theory presented by both the Bush and Obama administrations, according to which "the Judiciary should effectively cordon off all secret government actions from judicial scrutiny, immunizing the CIA and its partners from the demands and limits of the law." Indeed, accepting the logics proposed by the government(s) would exempt the intelligence agencies from the parameters of the judicial check. Consequently, and consistently with the constitutional principle of separation of powers, the court proclaimed that the judiciary "must undertake an independent evaluation of any evidence sought to be excluded to determine whether its contents are secret within the meaning of the privilege."

Binyam v. Jeppesen demonstrates not only that secretiveness goes hand in hand with unaccountability. More importantly, the judicial check — court order — retained the basic rule of law here, while the executive branch (regardless of political affiliations and worldviews professed) ultimately pressed for a decision bringing it more power and less accountability.

The same pattern emerges from the last among the cases involving the war with terror. In late 2003 civil liberties organizations (led by the ACLU) started what has been called the "Torture FOIA campaign." They have kept requesting, under the FOIA, the federal government (Departments of Defense, Homeland Security, State and Justice, some of their components, and the CIA) for records on the treatment of alien detainees in the U.S. custody. One particular offshoot of the Torture FOIA litigation is worth mentioning, because of how well it exemplifies pros and cons of transparency and accountability, and betokens their relationship with the government's legitimacy and potentially violent social action. Among the information sought by the ACLU were records of "the abuse and mistreatment of detainees in United States custody." More specifically, the ACLU wanted to see, among others, the remaining and still classified part of the famous "Darby photographs" depicting abuses of prisoners in Iraq and Afghanistan. The public knew some of them, those which had leaked from the Army (like the abuse in the Abu Ghraib prison in Iraq), but the ACLU wanted the public to be able to see all the rest.

In May 2009 the president Obama, after some hesitation, announced that he would endorse the decision to withhold the pictures. "The most direct consequence of releasing them, I believe, would be to further inflame anti-American opinion and to put our troops in greater danger" was the main argument the President proffered when he described his motives to the press. He also reminded that his subordinates have been perfectly aware, since he assumed office, that no abusive practices would be tolerated. The instances of mistreatment depicted on the photos had been investigated, argued the president, and the publication "may only have a chilling effect on future investigations of detainee abuse." He also declared that the pictures "were not particularly sensational, especially when compared to the painful images that we remember from Abu Ghraib." The press speculated that the final stance of the president was probably influenced by his top commanders on the ground, who argued that publicizing the pictures of mistreatment by previous service members would only endanger the current contingents.[36]

Certainly pictures trigger emotions much more than words, especially pictures of abuse. And in societies occupied by the U.S. troops where the path between emotions and action is short, an argument supporting of the president's decision may go, and where the people either do not know (or do not trust) the shift in the interrogation and detention policies under the new American administration, the current troops may face retaliation (after all, the uniforms have not changed). Perhaps more importantly for the top commanders, the purpose of the military missions may thus become even more difficult to accomplish. This is a soldier's logics. It does not know nor does it understand democratic values of transparency and openness. And it is

36 ABC News, President Obama Reverses Course on Releasing More Detainee Abuse Photographs, May 13, 2009, available from http://blogs.abcnews.com.

faulty. As a University of Chicago Law School's blogger pointed out sarcastically but with only small a dose of hyperbole: "[i]f we were to take seriously President Obama's view that the government should not release information to the American public if doing so might increase the risk to American soldiers, then surely the government would also be right not to disclose to the American people that (a) American military personnel tortured enemy detainees; (b) American soldiers massacred innocent civilians; (c) American soldiers were defeated in a fierce battle and suffered huge losses; and (d) the American military is using outdated equipment that does not adequately protect our soldiers."[37] Two further doubts come to mind in assessing the arguments proposed by the president in defence of his decision. First, if the pictures are "not particularly sensational," then how would they solely be responsible for endangering the American troops? More importantly, one type of accountability (transparency) never, in itself, interferes with other types (investigation of abuses), but, instead, reinforces them. This is why overlapping accountability mechanisms are construed in countries governed by the rule of law.

The assessment of general, crude geopolitical arguments aside, the issue is profoundly legal. As mentioned earlier, the president took his position in reaction to the "Torture FOIA" campaign of the ACLU. More precisely, he responded to a decision of the Court of Appeals upholding the decision of the District Court ordering release of the pictures.[38] In legal terms, what the president announced was that his DoJ would lodge a writ of certiorari (petition for review) to the Supreme Court (the cert petition was indeed submitted in August 2009), instead of releasing the 44 disputed pictures as ordered by the Court of Appeals.

The cert petition was essentially asking the Supreme Court whether releasing the pictures may fall within the FOIA Exemption 7(F). This exemption justifies withdrawal of materials which "could reasonably be expected to endanger the life or physical safety of any individual." Both of the lower courts responded in the negative. In probably the most important passage of its judgment, the Court of Appeals regarded it "plainly insufficient to claim that releasing documents could reasonably be expected to endanger some unspecified member of a group so vast as to encompass all United States troops, coalition forces, and civilians in Iraq and Afghanistan."

Despite the conservatism of the U.S. Supreme Court it is rather improbable that it would agree to review the case, for the very reason the president Obama indicated in his FOIA Memorandum: "[t]he Government should not keep information confidential merely … because of speculative or abstract fears." Yet, contrary to what the president claimed in his position about the mistreatment pictures only five months after sketching those words, inter-

37 G. Stone, What's Wrong with this Picture?, May 14, 2009, available from uchicagolaw.typepad.com/faculty/2009/05/index.html.

38 American Civil Liberties Union v. Dep't of Defense, 543 F.3d 59 (2nd Cir. 2008).

preting the exemption narrowly is not the question of doctrinal purity, but rather of recognizing how important the presumption of disclosure is for a democratic society. It is precisely why only well substantiated grounds may justify holding back public information.

Summing up

The latest American experiences show how difficult it is to achieve transparency in political practice. It is worth to pause on why any administration, even one allegedly well placed to protect civil liberties, attempts, often hazardously, to escape transparency and accountability by invoking national security arguments. For one, national security is certainly a grave and vivid social interest, and arguments based thereupon can justify limitations to accountability more convincingly than any others. Politicians and bureaucrats will therefore attempt to exploit them whenever possible to maximize their power. But the same outcome ensues even when office-holders do not espouse such self-interested motives. As the "Torture FOIA" campaign demonstrates, politicians do adulate public opinion, which naturally favours openness, with the rhetoric of openness, but quite naturally favour the opinion of experts when it differs from this of generalists. This is particularly so when a policy issue involves matters as important, extremely complex and wrought with uncertainties as war or terrorism. For most of law enforcement or military experts in the army, police or intelligence community, transparency is an alien concept.

The type of accountability an overwhelming majority of them recognizes and respects is a hierarchical one. In such an environment transparency cannot grow. Quite remarkably, therefore, when the president Obama, in one of exceptional instances of matching transparency rhetoric with real action in national security matters, released some of the famous "Torture Memos" of the Bush administration, he immediately added that "it is my strong belief that the United States has a solemn duty to vigorously maintain the classified nature of certain activities and information related to national security. This is an extraordinarily important responsibility of the presidency, and it is one that I will carry out assertively irrespective of any political concern. Consequently, the exceptional circumstances surrounding these memos should not be viewed as an erosion of the strong legal basis for maintaining the classified nature of secret activities." The purport of this statement is congruent with the overall picture stemming from the previous discussion – classification and no accountability is a rule. But when transparency and judicial review are eradicated, the rule of law itself is in a real danger.

On the other hand, as argued earlier, in less sensitive areas the Obama administration has pursued quite interesting pro-transparency initiatives. In fact, though, they have not been preoccupied with broadening the scope of information available to the public. Instead, like the IT Dashboard, those tools have made information already public more comprehensible and

attractive in form. A question warranted here is whether the federal authorities should develop such applications in the first place. As the example of USASpending shows, most often government initiatives happen to repeat the efforts of particularly vibrant American NGOs. In such instances, government actions boil down to spending federal resources on activities which otherwise would be covered by the civil society and its donors.

Whether private or public, sophisticated analytical tools require good-quality data feeds. In each case the data must come from the government. This is arguably why, when the Sunlight Foundation, a nonpartisan group seeking a more open government, asked its online audience what was the policy issue related to transparency which the new administration should accomplish during its first 120-days in office, the highest rated answer was: formal data standards, which would allow programmers to extract government databases and incorporate the source data into their own applications.

The ultimate success (or failure) of the Obama pledges to openness and transparency will depend on how much more information, comparing to the previous government, the new administration will disclose, and how "usable" and customizable for the public the information will be. In any case, President Obama was right declaring, on the day he announced his Openness and FOIA Memoranda (January 21, 2009) that "[t]ransparency and the rule of law will be the touchstones of this presidency." In fact they are touchstones of every democracy anywhere in the world.

Is het elektronisch patiëntendossier een bedreiging voor de rechtsstaat?

Hans Franken■

Inleiding

In zijn fraaie intreerede van 18 mei 2004 stelt Aernout Schmidt de vraag aan de orde of computers ons rechtssysteem bedreigen.[1] In zijn ongeclausuleerde antwoord zegt hij 'volmondig ja'. In deze bijdrage voor het aan Aernout ter gelegenheid van zijn emeritaat aan te bieden liber amicorum wil ik graag de vraag onderzoeken of het op handen zijnde wettelijk verplichte elektronisch patiëntendossier (EPD) een bedreiging vormt voor onze rechtsstaat. Computers en het gebruik daarvan zijn essentieel voor het EPD; de naam zegt het al. Bovendien is de bedoeling dat het EPD op alle burgers betrekking zal hebben.

De wettelijke maatregel, waarmee het EPD wordt vorm gegeven, is daarmee van zo vergaande strekking, dat de invoering daarvan zonder voldoende waarborgen voor de burger als een schending van de rechtsstaat kan worden gezien. Ik wil daarom het betreffende wetsvoorstel 'Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg (31 466)'[2] confronteren met de criteria die Aernout in zijn oratie als een zodanige bedreiging voor de burger heeft gekwalificeerd, dat daarmee onze rechtsstaat c.q. ons rechtssysteem onder druk komt te staan.

In het verdere betoog zal ik voor de beantwoording van de gestelde vraag eerst een résumé geven van de bedreigingen die Aernout in zijn oratie heeft opgesomd. Vervolgens zal ik een korte beschrijving geven van wat het wetsvoorstel 31 466 met het EPD bedoelt om daarna aan de hand van een viertal thema's te bezien of, en zo ja, in hoeverre, van dergelijke bedreigingen sprake is. Het opstel eindigt met een tentatieve conclusie met betrekking tot de vraag of het wetsvoorstel EPD bedreigend is voor onze rechtsstaat.

■ Hans Franken is lid van de Eerste Kamer der Staten-Generaal voor het CDA. Hij is hoogleraar informatierecht aan de Faculteit der Rechtsgeleerdheid in Leiden.

1 Schmidt 2004.

2 *Kamerstukken I en II* 31 466.

Hoe computers onze rechtsstaat bedreigen

De bedreigingen die de informatica voor ons rechtssysteem oplevert, betreffen de volgende verschijnselen. In de eerste plaats kan de legitimiteit van veel computerregelingen in Nederland niet worden bewaakt. Schmidt spreekt van formulierfrustratie, omdat alleen bepaalde informatie die op een voorgeschreven wijze is gestructureerd, kan worden gebruikt. De standaarden zijn de maat. De informatiesystemen schrijven daarmee gedrag voor aan de gebruikers. Het verschijnsel, dat door Lessig in zijn boek 'Code and other laws in cyberspace' is getypeerd als 'regulation by architecture'.[3] Hierdoor wordt niet alleen de gelding van de normering betwistbaar, want de regels zijn niet afkomstig van de democratisch gekozen wetgever, maar ook wordt de integriteit (de inhoud van de berichten) gemanipuleerd door deze te persen in de vorm van standaarden of kwalificaties. Bovendien komt de stabiliteit van ons rechtssysteem in gevaar. De burger vertrouwt de berichtgeving niet en kan als reactie massaal in verzet komen tegen de wijze van regulering.

In de tweede plaats worden de 'informatiewalhalla's' van de 'kennisbovenbazen' reële machtsdomeinen. De informatieverzamelingen van Google of Yahoo bevatten kennis, die aan de beheerders van deze systemen veel macht verschaft. De toegang tot die informatie (d.w.z. de beschikbaarheid voor de burger) kan door de 'bovenbazen' worden beperkt en de controle op het gebruik berust niet op democratisch gekozen organen. Bovendien staat de privacy van de burger onder druk. Hij weet niet wat er met de gegevens van zijn raadplegingen van of boodschappen over het net gebeurt of hoe de RFID-chips zijn koopgedrag aan bepaalde instanties openbaren.

Ten derde. De Nederlandse jurisdictie verliest aan scherpte door het ontstaan van wereldwijde wederkeringsheidsnetwerken – de open source beweging – met als gevolg dat de informatiediensten, die voor Nederland beschikbaar zijn, niet vanuit Nederland worden aangeboden en beheerd. Programmeurs, die hun krachten bundelen, leggen ons bedrijfsmodellen op die wij als een economische noodzakelijkheid moeten aanvaarden en die de eigen rechtsmacht ten aanzien van onze informatiesystemen beperken.

Aldus een scala van bedreigingen. Nu de casuïstiek.

Het landelijk elektronisch patiëntendossier

Het wetsvoorstel 31 466 beoogt in 2010 een landelijk elektronisch patiëntendossier (EPD) in te voeren. Het doel daarvan is een betere en een goed beveiligde uitwisseling van medische gegevens tussen zorgverleners.

Via het landelijk schakelpunt (LSP) kunnen zorgverleners inzage krijgen in onderdelen van het medisch dossier van patiënten. Zo kunnen ze

3 Lessig 1999.

snel beschikken over actuele medische gegevens, ook 's avonds en in het weekend. De uitwisseling van gegevens moet onnodig dubbel onderzoek voorkomen en het aantal medicatiefouten terugdringen. Al met al moet het landelijk EDP bijdragen aan een betere kwaliteit van de gezondheidszorg. Daarnaast leidt het landelijk EDP er toe dat patiënten niet bij iedere nieuwe zorgverlener hun verhaal opnieuw hoeven te vertellen. Het gaat om een faciliteit die de zorgaanbieder moet aanbieden. Patiënten zijn niet verplicht van deze faciliteit gebruik te maken. Ook de zorgverlener is niet verplicht het EPD te raadplegen; het is aan de zorgaanbieder hoe hij in het kader van verantwoorde zorg gebruik maakt van het EPD.

De zorgaanbieder kan de gegevens uit het EPD via het LSP opvragen door middel van een zgn. Unieke Zorgverlener Identificatie-pas (UZI-pas) die alleen verstrekt wordt aan beroepsbeoefenaren in het kader van de Wet BIG (beroepen individuele gezondheidszorg).

Het EPD is niet één groot bestand met de medische gegevens van alle patiënten in Nederland. (Een kennelijk nogal eens voorkomend misverstand.) Het is een elektronisch netwerk waarmee zorgverleners (onderdelen van) medische dossiers van andere zorgverleners kunnen raadplegen. Het gaat hierbij om 'relevante' gegevens, zoals een samenvatting van het dossier dat de huisarts bijhoudt. Er worden landelijke afspraken gemaakt over wat relevante gegevens zijn. Het gaat bijvoorbeeld om een overzicht van actuele lichamelijke of psychische gezondheidsproblemen, actueel medicijngebruik of allergieën.

Er is voor gekozen om het EPD in verschillende fasen in te voeren. Gestart wordt met een samenvatting van het huisartsdossier (Waarneem Dossier Huisartsen, afgekort WMD) en een medicatiedossier (ELektronisch Medicatie Dossier, afgekort EMD). Alleen bevoegde beroepsgroepen krijgen toegang. Zo hebben huisartsen op de huisartspost toegang tot een samenvatting van het huisartsdossier en kunnen huisartsen, medisch specialisten en apothekers het medicatiedossier raadplegen. De opsteller van de gegevens is verantwoordelijk voor de inhoud daarvan en beheert de gegevens. In een latere fase kunnen andere dossieronderdelen aan het EPD worden toegevoegd, zoals gegevens over de acute zorg (e-spoed), laboratoriumgegevens (e-lab) en radiologische beelden.

Is het EPD bedreigend voor de rechtsstaat? Vier thema's

De kwaliteit van de gegevens

Laten wij nu de casus toetsen aan de door Aernout Schmidt genoemde bedreigingen. Ik doe dit aan de hand van vier thema's, waarmee we de kern van het wetsvoorstel kunnen benaderen. Het eerste thema betreft de kwaliteit van de gegevens die in het EPD worden opgenomen. Precies gezegd, gaat het om de kwaliteit van de gegevens die de zorgverlener aan het dossier van zijn patient toevertrouwt. Immers de zorgverlener houdt het patiëntendossier bij, dat in het verleden op schrift stond, maar thans steeds meer

elektronisch wordt aangehouden. Deze elektronische vorm kan dan – onder bepaalde in de wet aangeduide voorwaarden – door andere hulpverleners worden geraadpleegd.

Een landelijke uitwisseling van gegevens tussen zorgverleners veronderstelt dat deze gegevens betrouwbaar zijn. Alleen dan kan de uitwisseling van gegevens bijdragen aan een hogere kwaliteit van de gezondheidszorg. Nu spelen in de gezondheidszorg niet alleen objectieve gegevens (bloeddruk, labwaarde) een rol, maar zijn ook subjectieve gegevens (anamneses, klachten van de patiënt), interpretaties door de arts (diagnose, prognose) en behandelplannen (voorschrijven van geneesmiddelen, operatieve interventies) van belang. Wanneer een arts gebruik maakt van door een andere arts verzamelde patiëntgegevens moet hij of zij niet alleen kunnen vertrouwen op de objectieve gegevens, maar ook op de subjectieve gegevens en interpretaties.

Hiermee kunnen wij stellen, dat de vraag naar de betrouwbaarheid van de gegevens, c.q. naar de inhoud van het dossier, niet eenduidig kan worden beantwoord. De integriteit van het informatiesysteem is dan in het geding. Teneinde interpretatieverschillen zoveel mogelijk te voorkomen, zullen standaarden moeten worden gehanteerd. Daarmee is de 'formulierfrustratie' aan de orde. Gelukkig hebben de beroepsgroepen zich op dit probleem geworpen en houdt de Memorie van Antwoord aan de Eerste Kamer in, dat deze professionals de betreffende standaarden in overleg zullen vaststellen. Deze ontwikkeling van berichtstandaarden en codeerafspraken is een noodzakelijke voorwaarde voor elektronische gegevensuitwisseling. Bij de standaardisatie gaat het overigens niet alleen om de techniek, maar ook om de inhoud van het berichtenverkeer. De huisartsen hebben in 2004 met hun richtlijn ADEMD (Adequate Dossiervorming met het Elektronisch Medisch Dossier) het voortouw genomen. Het is de bedoeling deze professionele standaarden in een AMvB op te nemen. We zien dat op deze wijze de gelding van de normering op een acceptabele wijze tot stand komt, terwijl de professionals zelf de verantwoordelijkheid dragen voor de inhoud van de norm/standaard.

Toegang en beveiliging

Een tweede thema betreft de toegang en beveiliging van de patiëntgegevens. Welke personen en instanties krijgen toegang tot het LSP, en aan welke voorwaarden moet worden voldaan teneinde te voorkomen dat onbevoegden toegang krijgen tot de inhoud van de medische dossiers? Het wetsvoorstel geeft aan, dat alleen geautoriseerde zorgverleners tot het EPD toegang krijgen. Deze zorgverleners mogen medische gegevens alleen inzien als er een behandelrelatie is en de gegevens noodzakelijk zijn voor de behandeling. Bovendien moet een zorgverlener voor inzage toestemming vragen aan de patiënt. Door middel van logging wordt vastgesteld wie wanneer gegevens heeft opgevraagd. Op misbruik volgen sancties van boetes tot doorhaling uit het BIG-register.

Een zorgaanbieder moet voldoen aan de eisen van een Goed Beheerd Zorgsysteem (GBZ). De veiligheid en betrouwbaarheid van het landelijk

EPD wordt periodiek getoetst door middel van audits en testen. Het is onlangs gebleken dat de beveiliging van de UZI-pas niet optimaal was, want experts uit Nijmegen waren in staat de private sleutel van de chip te achterhalen. Er is nu in de overgang naar een modernere chip voorzien. De robuustheid van de beveiliging van deze pas is uitermate belangrijk, want er zullen over enkele jaren meer dan 200.000 persoonlijke passen in omloop zijn. Het gaat nu al om 4321 huisartspraktijken, 52 huisartsendiensten-structuren, 1825 apotheken en 95 ziekenhuizen. Prof. Bart Jacobs uit Nijmegen ziet een slordige houding van de medische sector ten aanzien van beveiliging als het grootste risico. Hij wijst er op dat zorgverleners niet zijn getraind in informatiebeveiliging: een zorgvuldige omgang met logins, wachtwoorden, UZI-passen en authenticatie van patiënten.

Ook voor de toegang via internet tot de eigen medische gegevens door zorgconsumenten dienen strikte beveiligingsmaatregelen te worden getroffen. Het CBP heeft aangegeven dat voor de identificatie en authenticatie van de zorgconsument moet worden voldaan aan het hoogst beschikbare beveiligingsniveau. Daarvoor is een 2-factor authenticatie vereist, zoals bij DigiD met sms-verificatie, en een face-to-face uitgifteproces.

De zorgverzekeraar heeft volgens art. 13ha van het wetsvoorstel geen toegang tot het EPD. Tot mijn verbazing is aan dit artikel bij amendement een ontsnappingsclausule verbonden. Wanneer het noodzakelijk is voor de uitvoering van de zorgverzekeringen zou er wel inzage door de verzekeraar mogelijk worden. Bij AMvB zou dat begrip 'noodzakelijk' verder moeten worden ingevuld.

Het CBP ziet toe op de gegevensverwerking. Dat is natuurlijk een controle achteraf, maar ook ten aanzien van het system van de wet heeft het CBP een uitvoerig rapport geschreven. Daarin stonden veel punten van kritiek, maar de minister is zo wijs geweest goed naar de opmerkingen van de privacy-toezichthouder te luisteren. Het College is tevreden met het resultaat van het thans bijgewerkte wetsvoorstel.

Tengevolge van deze regeling van de potentiële gebruikersgroepen zal het gevaar van kennisbovenbazen niet snel ontstaan. Toch is de cultuurverandering van belang, waarvan wij hierboven al gewag maakten. Zorgverleners zullen in hun organisaties moeten leren om te gaan met kwetsbare dossiers. Wachtwoorden kunnen niet meer op plakkertjes op het beeldscherm worden geplakt. Onvoorzichtigheid zal snel door hackers worden bestraft. En de belangen zijn groot. Het verlies van één enkele UZI-pas met bijbehorende pincode is (ik citeer Prof. Jacobs) potentieel een nationale ramp. Verder geldt evenwel dat beveiliging nooit 'af' is en een continue monitoring, rapportage en verbetering vergt.

Positie en rechten patiënt

Als derde invalshoek kiezen wij de positie en rechten van de patient. Tijdens de parlementaire behandeling zijn over dit onderwerp veel vragen gesteld. Voor de patiënt is van groot belang, dat iedere zorgverlener toestemming moet vragen voordat zijn/haar gegevens worden opgevraagd.

Het landelijk EPD biedt patiënten de volgende functionaliteiten: inzage in de eigen medische gegevens, inzage in de logging-gegevens, inzage in de verwijsindex (d.w.z. welke gegevens bij welke zorgaanbieders aanwezig zijn), uitsluiten van zorgverleners op naam of beroepsgroep, en het maken van bezwaar. Daarnaast hebben patiënten het recht op correctie, aanvulling, afscherming of vernietiging van gegevens. Afscherming of vernietiging kan alleen in overleg met de zorgverlener plaatsvinden. Voor communicatie met burgers en klachten voorziet het stelsel in een klantenloket met als doel vragen van burgers en zorgaanbieders te beantwoorden, informatie te geven en klachten te behandelen.

De invoering van het EPD maakt het overigens niet nodig om de wettelijke regelingen voor de verdeling van aansprakelijkheden aan te passen. Als uitgangspunt geldt, dat de zorgverlener die het dossier opstelt, verantwoordelijk is voor de inhoud daarvan.

Uit deze opstelling blijkt, dat het wetsvoorstel een spilfunctie toekent aan de patient. Enerzijds is de toegang tot de gegevens van een patiëntendossier gelimiteerd tot alleen zorgverleners die BIG-bevoegd zijn. Anderzijds heeft de patiënt een aantal instrumenten om te voorkomen dat er zonder zijn instemming met 'zijn' gegevens wordt omgesprongen. De toezichthouders CBP en IGZ zullen ieder vanuit een andere invalshoek daar controle op kunnen uitoefenen.

Landelijk versus regionaal

Het vierde thema betreft de vraag of een landelijk EPD te verkiezen valt boven een regionale opzet. Hierbij geldt, dat een landelijke aanpak niet wordt gesteund door een groot deel van de zorgverleners, die onder meer als argument hanteren dat de zorg zich voor 95% regionaal afspeelt. Hetzelfde geldt dan ook voor de gegevensuitwisseling. Er bestaan bovendien al lokale en regionale systemen waarin gegevens van ruim 7 miljoen patiënten zijn opgenomen.

Ook deze kritiek is door de minister – zij het zeer kort geleden – ter harte genomen. In een uitgangspuntennotitie van 28 oktober 2009 zegt de minister van VWS met de koepelorganisaties in de volksgezondheid (waaronder de KNMG en de LHV) te zijn overeengekomen, dat het bij het EPD gaat om een landelijke infrastructuur met het Landelijk Schakelpunt (LSP), een landelijk 'telefoonboek' en voor specifieke toepassingen een landelijke verwijsindex voor veilige communicatie. Daarbij geldt, dat de regionale gegevensuitwisseling en de landelijke gegevensuitwisseling via het LSP als elkaar aanvullend zullen functioneren. Dit houdt in, dat de regionale gegevensuitwisseling zal plaatsvinden via de landelijke infrastructuur, d.w.z. met behulp van de landelijk vastgestelde standaarden. De regionale systemen zullen als 'taartpunten' in de landelijke infrastructuur worden gestoken.

Bovendien wordt er voor een bottom-up aanpak gekozen. De reeds bestaande en goed functionerende systemen van het WDH en het EMD zijn de eerste twee toepassingen die op landelijke schaal beschikbaar komen voor de EPD-infrastructuur. Er wordt prioriteit gegeven aan de invoering

van deze toepassingen alvorens wordt besloten of, en zo ja welke, andere toepassingen landelijk beschikbaar zullen komen voor uitwisseling. Van een landelijke 'bovenbaas' zal dus geen sprake (meer) zijn. Voor de overheid is in ieder geval geen 'bovenbaas'-regeling weggelegd, zoals we recentelijk wel hebben kunnen zien bij de bewaarplicht van verkeersgegevens en er bij het Elektronisch Kind Dossier (EKD) dreigt aan te komen.

Voorlopige conclusie

Hoe ziet het veld er nu uit? Dreigen de door Schmidt gevreesde gevaren bij de totstandkoming van het EPD als een groot ICT-systeem, dat invloed heeft op de individuele rechten van de burgers? Uit de bovenstaande analyses blijkt, dat de zwaarste bedreigingen na langdurige onderhandelingen en zware druk van de beide Kamers der Staten-Generaal wel – althans in theorie! – onder controle zijn. De legitimiteit van de programma's en de aansturing van de systemen zijn niet gedicteerd door vreemde machten of krachten. De 'Code as Law'-gedachte geldt niet voor de technische systemen. Toch blijft de integriteit van de inhoud van de dossiers problematisch voorzover taal als middel van communicatie wordt gebruikt. Maar hier stelt de beroepsgroep de standaarden voor communicatie en interpretatie vast. Het zijn dus niet de technology-driven managers en producenten en zeker niet de informatie-bovenbazen. Maar men dient steeds op zijn hoede te zijn. Zelfs een kleine fout kan grote gevolgen hebben. De toezichthouders komt een zware taak toe door op 7/24-basis de regionale systemen en het LSP te monitoren en daadwerkelijk in te grijpen bij overtredingen of slordigheden. Het mag niet zo zijn, dat zij zich op een gebrek aan menskracht zouden kunnen beroepen. Want alleen de mens kan de machine nog aan.

Verwijzingen

Franken 1993
H. Franken, Kanttekeningen bij het automatiseren van beschikkingen, in: *Beschikken en automatiseren*, VAR-reeks 110, Alphen aan den Rijn 1993.

Lessig 1999
L. Lessig, Code and Other Laws of Cyberspace, Basic Books 1999.

Munnichs 2009
G. Munnichs, *Startnotitie Expertmeeting elektronisch patiëntendossier (EPD)*, 9-12-2009, Commissie VWS/JG & Rathenau Instituut, 's Gravenhage 2009.

Schmidt 2004
A.H.J. Schmidt, *Bedreigen computers ons rechtssysteem?*, oratie Universiteit Leiden, 18 mei 2004.

Toegang tot juridische informatie als grondrecht

Laurens Mommers■

Inleiding

In 1998 werd de student Pavle Bojkovski voor de rechter gedaagd wegens publicatie op internet van wetteksten uit een uitgave van Vermande. De zaak vestigde destijds de aandacht op de afwezigheid van een vrij toegankelijke verzameling van geldende Nederlandse wetgeving op internet. Inmiddels is er veel veranderd. Om te beginnen is er sinds jaren een kosteloos toegankelijke website met Nederlandse wet- en regelgeving. Bovendien zijn sinds juli 2009 de elektronische Staatsbladen en Staatscouranten de authentieke versies, waarop de burger zich mag verlaten. Het accent is verschoven naar publicatie van juridische informatie op internet, maar verandert dit wezenlijk iets aan de toegankelijkheid van juridische informatie, en daarmee van 'het recht' voor de burger?

Deze bijdrage handelt over de vraag wat er nodig is om recht écht toegankelijker te maken. Daartoe begin ik met een kort overzicht van relevante Europese regelgeving op dit gebied, vervolg ik met de praktijk zoals die in Nederland is gegroeid, en analyseer ik het toegankelijkheidsbegrip, om ten slotte de vraag op te werpen of er zoiets is als een grondrecht op toegang tot juridische informatie, of zelfs een grondrecht op toegankelijke juridische informatie (let op de nuanceverschuiving). Voor het vaststellen van het antwoord op deze laatste vragen geef ik een overzicht van gerelateerde grondrechten.

Het Europese juridische kader

Hergebruik van overheidsinformatie, waaronder ook juridische overheidsinformatie, wordt gestimuleerd door de uitvaardiging van een Europese richtlijn inzake hergebruik van overheidsinformatie.[1] Deze Richtlijn verplicht de lidstaten bepaalde documenten te verstrekken, indien mogelijk digitaal, tegen een vergoeding die niet hoger is dan toerekenbare kosten ver-

---

■ Laurens Mommers is consultant bij Legal Intelligence, dienstverlener in juridische zoektechnologie. Daarnaast is hij universitair hoofddocent bij eLaw@Leiden, centrum voor recht in de informatiemaatschappij.

1 Richtlijn 2003/98/EG van het Europees Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie, *PbEG* 345/90, 31/12/2003.

meerderd met een redelijk rendement op investeringen.[2] Daarnaast dient de verstrekking plaats te vinden conform kenbare en transparante voorwaarden.[3] Bovendien stelt de Richtlijn een verbod in op discriminatie en exclusieve regelingen.[4] Diverse typen overheidsinformatie vallen niet onder deze Richtlijn maar juridische informatie valt er wél onder.[5]

In 2009 verscheen de evaluatie van de Richtlijn inzake hergebruik van overheidsinformatie.[6] In deze evaluatie wordt niet alleen duidelijk gemaakt wat de geschatte marktwaarde – en daarmee het belang – van overheidsinformatie is (27 miljard euro), maar ook wat de betekenis is geweest van de Richtlijn voor deze markt. Zo wordt hierin aangegeven dat discriminerende praktijken, monopolies en gebrek aan transparantie voor een belangrijk deel zijn weggenomen.[7] En stelt het rapport dat de volledige werking van de Richtlijn pas kan worden bereikt indien bijvoorbeeld de volgende problemen worden weggenomen: korte-termijn kostenverhaal, beperkingen op licenties, toewijzen van exclusieve rechten en beperkte kennis over welke informatie beschikbaar is.[8]

De praktijk in Europa en Nederland

De Europese Gemeenschap bood jarenlang een betaalde zoekdienst voor Europese informatie aan onder de naam Celex. In 1998 werd daarnaast een gratis dienst opgezet onder de naam EUR-Lex. In de loop van 2004 werden beide diensten met elkaar verweven tot een nieuwe dienst onder de bestaande naam EUR-Lex.[9] De recente herziening van de interface heeft niets wezenlijks veranderd aan de manier waarop de informatie in EUR-Lex ontsloten wordt, namelijk op basis van typeringen van documenten en het gebruik van trefwoorden uit de Eurovoc-thesaurus.[10] De belangrijkste sterke punten van EUR-Lex, zoals uitstekende bibliografische informatie, compleetheid en uitgebreide zoekmogelijkheden, houden nauw verband met de zwakke punten van het systeem: vertraging in de verwerking van nieuwe documenten, en lastig te gebruiken zonder kennis van het systeem en van het Europese recht.

Opvallend is dat de dienst geen eenvoudige 'interface' heeft voor het hergebruik van informatie. Diensten die alle informatie van EUR-Lex willen

2 *Idem*, art. 5 en 6.
3 *Idem*, art. 7.
4 *Idem*, art. 10 en 11.
5 *Idem*, art 1 lid 2.
6 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Re-use of Public Sector Information – Review of Directive 2003/98/EC, COM (2009) 212 final.
7 *Idem*, p. 2.
8 *Idem*, p. 3.
9 Bernet & Berteloot 2006.
10 Cf. http://europa.eu/eurovoc/.

hergebruiken, moeten daarvoor ofwel complexe scripts bouwen die de site volledig kopiëren en bijhouden welke informatie wordt toegevoegd, of ze moeten een vrij hoog bedrag betalen voor de *wekelijkse* aanlevering van al die informatie. Beide maatregelen zijn in strijd met de geest van de Richtlijn. Dus hoewel de Europese Unie haar informatie om niet beschikbaar stelt aan iedereen die die informatie wil hergebruiken, zijn de drempels daarvoor in de praktijk nog steeds vrij hoog. Inmiddels is gebleken dat dit op termijn zal veranderen. In de aanbesteding van de nieuwe versie van EUR-Lex is rekening gehouden met de introductie van relevante *web services*.[11]

Hetzelfde geldt voor de situatie in Nederland. Hoewel de Richtlijn hier geïmplementeerd is in de Wet openbaarheid bestuur (Wob), en de evaluatie stelt dat Nederland aan haar verplichtingen heeft voldaan, bijvoorbeeld op het gebied van het beëindigen van exclusieve arrangementen en het in rekening brengen van marginale kosten voor leveringen, zit de praktijk toch iets anders in elkaar dan het rapport suggereert.[12] Technische en organisatorische keuzes maken hergebruik in de praktijk een stuk lastiger. Ik noem een aantal voorbeelden:

– Veel juridische informatie is in Nederland afkomstig van toezichthouders, meestal zelfstandige bestuursorganen. Hoewel zij onder het bereik van de Wob vallen, leidt de versnippering in het toezicht ook tot fragmentatie in de beschikbaarstelling van de – zeer belangrijke – documenten van deze organisaties.

– De wijze van beschikbaarstelling beïnvloedt de herbruikbaarheid. Tot voor kort beveiligde bijvoorbeeld de OPTA haar PDF-documenten tegen indexering. Dat betekent dat alleen de samenvattingen doorzoekbaar waren voor zoekmachines, waarmee de daadwerkelijke ontsluiting van de documenten niet optimaal was.[13]

– Onaangekondigd stappen instanties over op nieuwe platforms voor publicatie van hun documenten. Dat leidt tot verlies van nieuwe én soms ook van oude documenten.[14]

– De structurering van publicatieplatforms is van belang voor de toegankelijkheid van documenten voor hergebruik. De gemakkelijke vindbaarheid van álle documenten, en de typering van die documenten met behulp van metadata zoals titel, datum, documenttype etcetera, zijn van invloed op de herbruikbaarheid.

---

11 Cf. http://publications.europa.eu/tenders/our/documents/itt_10233/template_ao_en.htm.

12 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Re-use of Public Sector Information – Review of Directive 2003/98/EC, COM (2009) 212 final.

13 Zwenne 2009, p. 31.

14 Talrijk zijn uiteraard de gevallen waarin overheidsinstanties en ZBO's onaangekondigd hun sites vernieuwen. Recent gebeurde dat onder meer bij wetten.nl.

Ook de grote juridische overheidswebsites (wetten.nl en www.officielebekendmakingen.nl) lijden onder voornoemde problemen:

– Bij de inwerkingtreding van de Wet elektronische bekendmaking ontstond een onduidelijke situatie rondom de publicatie van kamerstukken. Die waren nog niet aanwezig op de nieuwe site www.officielebekendmakingen.nl, maar de oude overheidssite voor kamerstukken leek al te zijn gesloten.

– Openbare berichtgeving over details van toekomstige wijzigingen in de sites en diensten met juridische informatie ontbreekt, zodat hergebruikende partijen daarop niet kunnen anticiperen en de continuïteit van hun dienstverlening in gevaar komt.

– De komst van een dienst voor het nagaan van de laatste wijzigingen in wet- en regelgeving heeft vertraging opgelopen; op dit moment is er alleen de mogelijkheid om te weten welke documenten zijn gewijzigd en toegevoegd, niet wat de inhoudelijke wijzigingen zijn. Deze laatste dienst heeft bovendien een tijd lang niet gefunctioneerd.

Deze problemen leiden vermoedelijk tot minder hergebruik dan mogelijk is. Hoe hoger immers de investeringen om de (overigens kosteloos te verkrijgen) informatie te hergebruiken, hoe hoger de drempel om innovatieve diensten op te zetten.[15] In de Richtlijn zijn echter wel degelijk pogingen gedaan om het type technische vereisten neer te leggen dat nodig is om de toegankelijkheid van documenten te verbeteren. Neem bijvoorbeeld overweging 13:

> "De mogelijkheden tot hergebruik kunnen worden verbeterd door de gevallen te beperken waarin papieren documenten moeten worden gedigitaliseerd of waarin digitale bestanden moeten worden gemanipuleerd om deze compatibel te maken. Openbare lichamen dienen daarom hun documenten in alle reeds bestaande formaten en alle talen, indien mogelijk en passend langs elektronische weg beschikbaar te stellen. [...] Teneinde hergebruik te vergemakkelijken, dienen openbare lichamen hun documenten beschikbaar te stellen in een formaat dat, voorzover mogelijk en passend, niet gebonden is aan specifieke software. [...]"[16]

Deze overweging kan geïnterpreteerd worden als een middel tegen het beschikbaarstellen van niet-ge-ocr'de[17] digitale bestanden (waarvan de tekst

15 De markt voor hergebruik van juridische informatie is desondanks groeiende. Niet alleen hergebruiken diverse betaalde producten van Kluwer, Sdu, Legal Intelligence en Rechtsorde Nederlandse en Europese juridische informatie, ook is er een groeiend aanbod van gratis zoekdiensten geïnitieerd door het bedrijfsleven die deze informatie toegankelijk maken naast de overheidssites die daartoe beschikbaar zijn. Het gaat om onder meer ikregeer.nl, jure.nl, liigl.nl en parlis.nl.

16 *Idem*, overweging 13.

17 OCR (optical character recognition) is een techniek waarbij in een scan van een tekstdocument de lettervormen worden herkend, zodat de lopende tekst van het oorspronkelijke document kan worden gereconstrueerd.

dus niet 'leesbaar' is voor de computer), tegen het achterhouden van geschikte bestandsformaten en tegen het beschikbaarstellen van bijvoorbeeld alleen Word-documenten. De Richtlijn laat echter ook een flink aantal noodzakelijke maatregelen achterwege. Zo is er geen bepaling voor de duurzame terbeschikkingstelling van documenten.[18] Overweging 18 stelt dat het niet langer beschikbaar stellen of bijwerken van documenten wel zo spoedig mogelijk aan het publiek kenbaar moet worden gemaakt.[19]

Niveaus van toegankelijkheid

Om orde te brengen in de hierboven genoemde praktische problemen en bezwaren onderscheid ik op het niveau van gebruik van documenten tussen vier verschillende niveaus van toegankelijkheid. Dit zijn (1) vindbaarheid; (2) doorzoekbaarheid, (3) betekenisduiding en (4) begrijpelijkheid. Deze niveaus zullen hieronder verder worden uitgewerkt. De impliciete interpretatie van toegankelijkheid door overheden (zowel blijkend uit de Richtlijn, de implementatie daarvan in de Wob en in het vigerend overheidsbeleid) is die op het eerste niveau.

Voor een goede *primaire toegankelijkheid* (vindbaarheid) van rechtsbronnen geldt het vereiste van onmiddellijkheid – de elektronische toegankelijkheid dient zoveel mogelijk samen te vallen met het moment waarop het onderliggende besluit wordt genomen. Daarnaast dient er ten minste één 'sleutel' te zijn waarmee de toegang kan worden verkregen; bijvoorbeeld. de naam van het document: om toegang te hebben tot het document dient het vindbaar te zijn. Primaire toegankelijkheid is vergelijkbaar met de toegankelijkheid van een document in een bibliotheek: er is een methode om het document in de bibliotheek te vinden maar de inhoud ervan wordt pas prijsgegeven bij het bekijken van het document zelf. De elektronische vorm van primaire toegankelijkheid komt (bijvoorbeeld) neer op het via bijvoorbeeld titelinformatie aanklikbaar maken van reeksen besluiten.

Een goede *secundaire toegankelijkheid* (doorzoekbaarheid) van rechtsbronnen hangt af van de doorzoekbaarheid van de datalaag; daarmee is het mogelijk om als het ware kennis te nemen van de strekking van de inhoud zonder het document zelf te openen. Bij tekstdocumenten gaat het dan om bijvoorbeeld de doorzoekbaarheid van de tekst die in die documenten is opgenomen. Bovendien valt binnen secundaire toegankelijkheid dat door middel van metadata relaties worden gelegd die de betekenis van losse documenten inzichtelijker maken, en in verband plaatsen met andere documenten. Secundaire toegankelijkheid is gerealiseerd in de meeste jurisprudentie- en wettendatabanken, waarvan de tekst geheel kan worden doorzocht.

---

18 Sterker, conform art. 5 lid 2 hoeven de lidstaten documenten niet te *blijven* produceren. Over het *blijvend* beschikbaarstellen van documenten doet de Richtlijn geen expliciete uitspraak.

19 *Idem*, overweging 18.

Een goede *tertiaire toegankelijkheid* (betekenisduiding) van rechtsbronnen begint met de handmatige of geautomatiseerde toevoeging van betekenisgerelateerde metadata aan documenten. Deze mogelijkheid markeert ook de relatie met het zogenaamde 'semantische web': de mogelijkheid om betekenisvol te zoeken naar informatie (in plaats van 'slechts' op trefwoord of bibliografische metadata). De meeste metadata beperken zich vandaag de dag tot bijvoorbeeld het expliciet benoemen van een auteur, rechter, publicatiedatum of instantie. Maar het is zeker niet ondenkbaar dat bepaalde tekstelementen worden gemarkeerd als een argument voor een bepaald standpunt. Een voorbeeld van tertiaire toegankelijkheid is de relatie die EUR-Lex legt tussen Europese richtlijnen en implementatiemaatregelen in de lidstaten.

Een goede *quartaire toegankelijkheid* (begrijpelijkheid) hangt af van de begrijpelijkheid van individuele documenten voor niet-gespecialiseerde juristen. Die toegankelijkheid ontstaat bijvoorbeeld door de toevoeging van een of meer complete 'vertalingen' van de bron, of van een verzameling bronnen, in een tekst; figuur of animatie die bedoeld is om de inhoud nader te verklaren, eventueel aangepast voor een bepaalde doelgroep met een bepaald kennisniveau. Hier kan eigenlijk niet meer van metadata worden gesproken. De vertaling van de bron hangt van veel meer af dan alleen de inhoud van de bron. Het is een misverstand dat het zou volstaan om de tekst bijvoorbeeld in eenvoudiger bewoordingen op te schrijven. Ook de 'contextualisering' van de vertaling is van belang waarbij de context wordt gevormd door onder meer de doelgroep; de intenties van die doelgroep en hun achtergrondkennis.[20]

Wanneer deze toegankelijkheidsniveaus worden gelegd naast twee databanken, te weten EUR-Lex en officiëlebekendmakingen.nl, vallen de volgende punten op. De eerste twee toegankelijkheidsniveaus zijn technisch gezien nauwelijks nog een uitdaging. Alle technologie bestaat om deze toegankelijkheid te optimaliseren. Organisatorische beperkingen, gebrek aan menskracht en ontwerpkeuzes kunnen wel roet in het eten gooien. Zo duurt het door de vertaling en metadatatering van documenten enkele dagen tot enkele maanden voordat zij in EUR-Lex verschijnen. De meeste (maar niet alle) documenten in EUR-Lex zijn volledig op tekst doorzoekbaar, en daarnaast te vinden op inhoudelijke en structurele metadata, zoals de trefwoorden uit de Eurovoc-thesaurus en documentnummers.

Bij officielebekendmakingen.nl lijken inmiddels alle beoogde documenten, dus ook kamerstukken, gepubliceerd te worden. De opzet van de zoekfunctie laat te wensen over qua gebruiksvriendelijkheid; die is voornamelijk 'aanbodgericht': er kan gezocht worden op beschikbare bibliografische metadata; maar bijvoorbeeld niet op thema. In het algemeen geldt voor deze site dat deze – anders dan EUR-Lex – geen geïntegreerd zicht biedt op verschillende typen juridische documenten. De site is mede gebouwd vanwege de inwerkingtreding van de Wet elektronische bekendmaking, maar toont

20 Mommers et al. 2009.

daarnaast wél kamerstukken, maar géén geconsolideerde wet- en regelgeving. Die is in een aparte website ondergebracht.

Dat brengt me meteen op de tertiaire toegankelijkheid: daar is bij EUR-Lex duidelijk wel over nagedacht (met wisselend gevolg), maar die ontbreekt grotendeels op officielebekendmakingen.nl. De enige Nederlandse overheidssite waar inmiddels kruisverwijzingen tussen verschillende bronnen worden gegeven, is wetten.nl. Daar is het mogelijk om bij een wet de wetsgeschiedenis en gedelegeerde regelgeving te bekijken. Ook interessant in dit opzicht is overigens de LJN-index, die wordt bijgehouden door de organisatie achter rechtspraak.nl. Die index geeft verschillende vindplaatsen van dezelfde uitspraak, zodat verschillende commentaren bij eenzelfde uitspraak kunnen worden gevonden, en eenduidig verwijzen via het LJ-nummer gemakkelijker wordt.[21]

EUR-Lex brengt, samen met enkele verwante sites, een flink aantal kruisverwijzingen aan bij de bronteksten. Het betreft onder meer verwijzingen naar wijzigingen aangebracht in een regeling, documenten in dezelfde rubriek, de juridische basis, gedelegeerde regelgeving, en andere documenten waarin het onderhavige document wordt genoemd. Daarnaast is het bijvoorbeeld mogelijk om het wetgevingsproces te volgen door een overzicht te tonen van de verschillende documenten van de Europese instellingen en de acties die zij uitvoeren. Daarmee ontstaat zicht op het proces dat uiteindelijk tot regelgeving leidt.[22]

Quartaire toegankelijkheid ten slotte – althans een poging daartoe – is terug te vinden in aan EUR-Lex gerelateerde diensten zoals een site met samenvattingen van het primaire en secundaire gemeenschapsrecht (vroeger bekend onder de naam Scadplus).[23] Daarnaast bestaan er de nodige thematische portals, die weliswaar vaak interpretaties van juridische bronnen bevatten, maar daarnaar niet expliciet verwijzen.[24] Op Nederlands niveau is quartaire toegankelijkheid op geen enkele wijze gerealiseerd in www.officielebekendmakingen.nl; maar er zijn uiteraard ook in Nederland initiatieven op dit vlak. Zo geeft www.overheid.nl een overzicht van overheidsproducten en -diensten aan burgers en bedrijven; alle uiteraard gebaseerd op wet- en regelgeving; en verzorgen NMa, OPTA en de Consumentenautoriteit de voorlichtingsportal www.consuwijzer.nl. Een elders zelden gevonden aspect van www.overheid.nl is dat bij elke product of dienst wordt verwezen naar de onderliggende primaire rechtsbron (de wet of de regeling).

---

21 De huidige praktijk is dat wordt verwezen naar de vindplaats i.p.v. naar de onderliggende uitspraak. Dat betekent dat eenzelfde uitspraak verschillende vindplaatsen kan hebben.

22 Zie http://ec.europa.eu/prelex/apcnet.cfm?CL=en and http://www.europarl.europa.eu/oeil/.

23 Zie http://europa.eu/legislation_summaries/index_en.htm.

24 Zie http://ec.europa.eu/health-eu/index_en.htm.

Naar een grondrecht op toegankelijkheid?

Een vingerwijzing naar de plaats van algemeen beschikbare informatie van de overheid komt uit de boven genoemde Richtlijn:

"De openbaarmaking van alle algemeen beschikbare informatie in het bezit van de overheid – dus niet alleen in de politieke maar ook in de rechterlijke en bestuurlijke sfeer – vormt een fundamenteel instrument voor verruiming van het recht op kennis, dat een essentieel beginsel is van de democratie. Deze doelstelling geldt voor instellingen op elk niveau, plaatselijk, nationaal en internationaal."[25]

Het 'recht op kennis' wordt geponeerd als noodzakelijk voor de democratie. Toegankelijke informatie op elk bestuursniveau en op elk niveau van de rechtspleging vormt daarvoor een instrument. De overweging geeft ook de zwakte aan van de veronderstelling; immers, toegankelijke informatie vormt een noodzakelijke, maar geen voldoende voorwaarde voor deze kennis. Een bureaucratie is zeer wel in staat om de burger zodanig te bedelven onder informatie die kwalitatief en kwantitatief niet te 'verwerken' is, dat het recht op kennis slechts een fata morgana blijkt.

In het geval van juridische informatie is dit sombere beeld niet per definitie onterecht. Een paar cijfers ter illustratie. In 2008 verschenen in Nederland 3110 nieuwe regelingen (al dan niet wijzigingen op bestaande regelingen). Het gaat hier om wetten in formele en in materiële zin, dus niet om beleidsregels en andere soorten semi-regelgeving. Om op de hoogte te blijven van de materiële inhoud van alleen nieuwe wetgeving zou iemand in elk geval de memories van toelichting moeten lezen. In 2008 ging dat om 294 stuks. Om op de hoogte te blijven van de besprekingen in het parlement zou diegene maar liefst ruim 16.000 stukken moeten lezen.

Het bovenstaande is exclusief de relevante rechtspraak en literatuur, en exclusief verdragen en Europees recht. Natuurlijk schets ik hier een karikatuur, want van niemand kan verwacht worden dat hij álle nieuwe regelgeving en bijbehorende stukken bijhoudt. Toch is een schijnbaar redelijk begrensd gebied als de visserij al goed voor ruim 1000 kamerstukken in 2008 – dat is exclusief bijvoorbeeld de kamervragen en handelingen op dit gebied.

Opmaat naar een grondrecht

Een zoektocht in de literatuur naar – letterlijk – de beschrijving van een recht op toegang tot juridische informatie heeft niet veel opgeleverd. Als uitzondering hierop heeft Jamar het recht op toegang tot juridische informatie geconstrueerd als een deel van het transparantiebeginsel,[26] art. 19 van de

25 Overweging 16 van Richtlijn 2003/98/EG.
26 Jamar 2001, p. 3.

Universele Verklaring voor de Rechten van de Mens,[27] art. 19 van het IVBPR,[28] en het IVESCR.[29] Hij gebruikt het recht van toegang tot informatie (in de brede zin van het woord) en de impliciete veronderstelling van toegankelijkheid in het IVESCR om dit specifieke recht op te bouwen. Hij raakt daarbij bovendien aan de mogelijkheden die mark-up-talen bieden om die toegang te verbeteren ten opzichte van platte tekst.[30] Bovendien heeft hij oog voor de toegankelijkheid *sec* van juridische teksten, getuige het feit dat hij een initiatief van de Clinton-administratie aanhaalt waarin regelgeving voortaan moet worden opgesteld in 'plain English'; daarmee raakt hij aan wat ik in dit artikel quartaire toegankelijkheid noem.[31]

Hij gaat echter voorbij aan een aantal wezenlijke belemmeringen aan deze 'eenvoudige' oplossingen. Ten eerste is – ondanks een grote noodzaak om juristen begrijpelijker te laten schrijven – 'plain English' of duidelijk Nederlands niet zonder meer een oplossing. Definities van bepaalde begrippen die afwijken van 'common sense'-betekenis, zijn zeer gebruikelijk in het juridische domein. Duidelijke taal kan de foutieve indruk wekken dat de gebruikte woorden ook een gebruikelijke betekenis hebben, wat lang niet altijd het geval is. In een wetstekst kan 'links' gedefinieerd worden als rechtsonder en 'rechts' als linksboven – de vrijheid van definitie helpt het maken van compacte regelgeving en het inperken van interpretatiekwesties.[32]

Ten tweede is kwantiteit een serieus probleem. Om in termen van de eerder genoemde getallen te blijven: 16.000 kamerstukken in begrijpelijke taal zijn nog steeds heel veel stukken. Daarnaast valt het niet mee om die kamerstukken in onderling verband goed te plaatsen. De in vergelijking met de Europese wetgevingsprocedures nog relatief overzichtelijke gang van zaken in het Nederlandse wetgevingstraject leidt niet tot een heldere documentenstroom zonder kennis van dat traject. Dit betekent dat toegankelijkheid ook individuele documenten overstijgt. De tertiaire en quartaire vormen van toegankelijkheid betreffen ook die documentoverstijgende component.

Eén van de vormen waarin bijvoorbeeld het wetgevingsproces duidelijker kan worden gemaakt is aan de hand van een wetgevingskalender die het tijdsverloop, de instituties, de fases van het proces en de documenten die daarin een rol spelen overzichtelijk in kaart brengt. Dat is overigens, gezien de vele dimensies van het proces, geen sinecure. Waarschijnlijk is dat ook de reden dat zo'n kalender – behalve in een basale vorm – in Nederland niet bestaat.[33] In dat kader heb ik mij in eerdere instantie wel in minder diplomatieke bewoordingen uitgelaten over het Nederlandse hergebruikbeleid:

27 *Idem*, p. 6.
28 *Idem*, p. 7.
29 *Idem*.
30 *Idem*, p. 10.
31 *Idem*, p. 4.
32 Mommers en Voermans 2007.
33 Mommers et al. 2009.

'Keer maar om die Kliko!' luidde de opinie die ik voor het Tijdschrift voor Internetrecht schreef en waarvan de strekking was dat het letterlijk omkeren van een heel grote bak informatie op internet op zich prima is.[34]

Er zit wel een keerzijde aan die opinie. Voor de markt van zakelijke dienstverlening is het interessant om hergebruikinitiatieven op te pakken. Voor de particuliere markt is dit veel lastiger. Het democratische proces zou hier wel bij gebaat zijn. Het verbeteren van tertiaire en quartaire toegankelijkheid is wel noodzakelijk, maar vooralsnog duur. Pogingen om hierin met behulp van web 2.0-technieken verandering te brengen, zijn vooralsnog geen groot succes. Hoewel Wikipedia veel waardevolle juridische informatie bevat, is de specialistische evenknie Jurispedia niet voldoende compleet om werkelijk van nut te zijn voor rechtzoekenden.

Onder advocatenkantoren is weliswaar een groeiende belangstelling voor het gebruik van wiki's; maar een wezenlijke wijziging in de dienstverlening (waarbij meer kennis om niet wordt gedeeld) is nog niet te bespeuren. Ook de overheidsinitiatieven op web 2.0-gebied beperken zich vooralsnog tot consultaties in een zeer beperkt aantal wetgevingstrajecten.[35] Bovendien verloopt die consultatie feitelijk nauwelijks via internet: er is uitsluitend de mogelijkheid enige informatie in te zien en te reageren via een webformulier. Een overzicht van reacties (laat staan reacties op reacties) is er niet.

Gerelateerde grondrechten

Dit alles neemt niet weg dat er aanwijzingen zijn voor het bestaan van een grondrecht op toegankelijkheid van juridische informatie. In de paragrafen hiervoor is besproken hoe de primaire toegankelijkheid van het recht het afgelopen decennium sterk is verbeterd, en dat secundaire en tertiaire toegankelijkheid langzaamaan meer aandacht krijgt. Deze constateringen gelden de praktijk van toegankelijkheid. Maar bezien vanuit het recht kunnen in elk geval de volgende gerelateerde grondrechten worden genoemd:

– Legaliteitsbeginsel.[36] Het legaliteitsbeginsel houdt – in het strafrecht – in dat geen strafbaarheid mag worden toegewezen aan een bepaalde categorie feiten zonder voorafgaande wettelijke maatregel. In andere rechtsgebieden, met name in het bestuursrecht, geldt dat de burger moet kunnen anticiperen op nieuwe regelgeving.[37] Het beginsel is in feite ontologisch geformuleerd; zelf zegt het niets over de *kenbaarheid* van die wet-

34 Mommers 2008.
35 Zie http://www.internetconsultatie.nl/.
36 Art. 16 Gw; art. 7 EVRM.
37 Al wordt dat op sommige fronten verdraaid lastig gemaakt. De casus van de afschaffing van de WIR en vele belastingwetten die in no-time door het parlement zijn gejaagd illustreren dit.

telijke maatregel.[38] Zonder die kenbaarheid is sprake van 'geheim recht' en dat wordt naar algemeen erkende (althans Westerse) maatstaven niet als recht erkend. Toch wordt een epistemologische formulering van het beginsel in onder meer de Nederlandse Grondwet naar mijn mening node gemist. Daarnaast is de beperking tot het strafrecht dubieus. Recht moet bestaan én kenbaar zijn vóórdat het in werking treedt.

– Vrijheid van meningsuiting.[39] De gedachtevorming en vrije uiting daarvan rondom het democratisch bestel is gebaat bij een goede toegang tot juridische informatie. Die toegang zou zich niet moeten beperken tot de primaire en secundaire toegankelijkheid die vandaag de dag is gerealiseerd. In hoeverre de wetgever zelf verantwoordelijk is voor het realiseren van tertiaire en quartaire toegankelijkheid is niet zonder meer te zeggen. Het gaat sowieso vrij ver om vanuit het voor de overheid passieve grondrecht van vrijheid van meningsuiting een voor de overheid actief recht op toegankelijk maken van juridische informatie af te leiden. Vrijheid van meningsuiting vormt dus slechts een zijdelingse steun voor het recht op toegankelijkheid.

– Toegang tot de rechter en rechtsbijstand.[40] Het recht op een rechtsingang is vooral voor de strafrechter expliciet bepaald. Het reikt echter verder, zoals bleek uit onder meer de Kadi-zaak[41] en de Bosphorus-zaak.[42] Het betreft dan zaken waarin een sanctie van de VN Veiligheidsraad die geïmplementeerd moet worden door nationale jurisdicties niet gepaard gaat met een afdoende rechtsingang om tegen die sancties op te komen. Nu zijn zowel de feitelijke rechtsingang als rechtsbijstand slechts ten dele verwant aan het recht op toegang tot juridische informatie. Er zijn echter zeker situaties denkbaar waarin de *kenbaarheid* van de rechtsingang tekort schiet (terwijl die er wel ís). Daarnaast kan het recht op toegankelijkheid van juridische informatie betekenis hebben voor de noodzaak van rechtsbijstand.

38 Voor een uitgebreide bespreking van het verschil tussen een ontologische en epistemologische benadering van het recht, zie Mommers 2002.

39 Art. 7 lid 1 Gw; art. 10 EVRM.

40 Art. 15 lid 2 en art. 17 Gw; art. 6 en 13 EVRM. Het recht op rechtsbijstand is geregeld in art. 18 Gw.

41 HvJ EG 3 september 2008, gevoegde zaken C-402/05P & C-415/05P, (Kadi/Al-Barakaat v. Raad).

42 EHRC 2005/91 Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi ('Bosphorus Airways') tegen Ierland.

– Openbaarheid van bestuur.[43] Juridische informatie vormt in principe een deelverzameling van de documenten waarop het regime met betrekking tot openbaarheid van bestuur betrekking heeft. Van de formele rechtsbronnen valt rechtspraak hier echter niet onder, en vaak is er een specifiek regime voor de overige formele rechtsbronnen. Dat openbaarheid van bestuur toch een rol speelt bij de toegang tot juridische informatie heeft vooral te maken met de wijze van totstandkoming van bijvoorbeeld wet- en regelgeving. Documenten die geen onderdeel zijn van het primaire wetgevingsproces kunnen wel bijzonder belangrijk zijn voor de interpretatie van primaire rechtsbronnen, en daarmee een belangrijke rol spelen bij de toegankelijkheid van juridische informatie.

– Bescherming van de persoonlijke levenssfeer.[44] Dit grondrecht vormt een mogelijke beperking op toegang tot juridische informatie. Dit is onder meer actueel geworden door de wens om meer rechtspraak openbaar te maken via internet, met het risico dat privacyrechten van betrokkenen worden geschonden.[45] Ook casus zoals de Bavarian-zaak (waarin een Engelse bierbrouwer toegang wil tot de notulen van een overleg tussen de Europese Commissie en een brancheorganisatie) dragen bij aan de juridische explicitering tussen (grond)rechten; waaronder het recht op bescherming van gegevens van natuurlijke personen en het recht op toegang tot documenten.[46]

– Evenzo vormt auteursrecht een potentiële beperking van het recht op toegang. Secundaire rechtsbronnen, zoals literatuur, zijn vaak het exclusieve domein van uitgevers van zakelijke content. Deze professionele informatie is doorgaans duur, en daarnaast slecht toegankelijk voor een lekenpubliek. Een voorbeeld van bronnen waarvan de 'ontoegankelijkheid' daadwerkelijk juridische complicaties oplevert door een botsing van een recht op toegankelijkheid met het auteursrecht, wordt gevormd door 'private' regelgeving. Dit is onderwerp van de bijdrage van Stuurman in dit liber.

---

43 Zie bijv. verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie *PB L 145 van 31.5.2001, blz. 43–48*; zie bijv. ook de Nederlandse Wet openbaarheid bestuur. Zie ook COM (2008) 229; proposal for a regulation of the european parliament and of the council regarding public access to European Parliament, Council and Commission documents.
http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=196983

44 Art. 10 lid 1 Gw; art. 8 EVRM; voor implementatie van het recht in 'gewone' regelgeving zie bijv. 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, *OJ L 281, 23/11/1995 p. 31-50* en de Nederlandse Wbp.

45 Zie VMC-studiecommissie Openbaarheid van rechtspraak (Commissie De Meij), 'Toegang tot rechterlijke uitspraken', maart 2006, afgedrukt als katern in *Mediaforum* 2006-4.

46 Kranenborg 2007.

Deze onvolledige opsomming laat zien dat het recht op toegankelijkheid de nodige constituenten kent, en bovendien dat de technologische faciliteiten die de primaire toegankelijkheid van het recht mogelijk maken, uiteindelijk ook vragen oproepen over de hogere-orde vormen van toegankelijkheid. Nu het recht voor iedereen daadwerkelijk toegankelijk is (in de zin van primaire en secundaire toegankelijkheid) wordt eens te meer duidelijk dat die primaire en secundaire toegankelijkheid niet volstaan in het licht van bestaande grondrechten.

De zuiver-ontologische lezing van het legaliteitsbeginsel is dan ook de voornaamste barrière in het vestigen van een grondrecht op toegankelijkheid van juridische informatie; immers, pas wanneer een epistemologische lezing van datzelfde beginsel wordt gehanteerd, wordt het noodzakelijk om te zorgen voor een vorm van articulatie van juridische informatie die kenbaarheid in brede kring mogelijk maakt. Die articulatie hoeft overigens niet noodzakelijkerwijs de vorm van toegankelijkheid van juridische informatie te hebben; deze kan ook geschieden door laagdrempelige rechtshulp. Zelfs de epistemologische lezing van het legaliteitsbeginsel leidt dus niet noodzakelijkerwijs tot de vaststelling van een recht op toegankelijke juridische informatie.

Conclusie

Er zijn diverse aanwijzingen dat er een grondrecht op toegankelijkheid van juridische informatie bestaat. Deze zijn te vinden in gerelateerde rechten, de vestiging van Europese en nationale rechtsregels, en in een snelle technologische ontwikkeling die heeft geleid tot een noodzakelijkheidsbesef van de toegang tot rechtsbronnen via internet. Gevolg daarvan is dat juridische bronnen verbeterd vindbaar zijn via allerlei overheids- en commerciële portals. Daarmee zijn die bronnen echter nog niet toegankelijk voor een breed publiek.

Er is geen doorslaggevende reden voor het bestaan van een grondrecht op toegankelijkheid te geven. Het dichtst in de buurt komt de epistemologische interpretatie van het legaliteitsbeginsel: zo'n interpretatie zegt immers dat rechtsregels voor hun toepasselijkheid niet alleen dienen te *bestaan*, maar dat zij ook *kenbaar* moeten zijn. Het recht op toegankelijkheid van juridische informatie lijkt in eerste instantie een conditio sine qua non voor deze kenbaarheid, maar kan ook verlopen via laagdrempelige rechtshulp.

De reikwijdte van een recht op toegankelijkheid van juridische informatie en van toegankelijke juridische informatie is niet gemakkelijk te bepalen. Zoals in deze bijdrage uiteengezet, omvat het recht op toegankelijkheid verschillende niveaus, die minder of meer vergaande consequenties kunnen hebben. Het is niet gemakkelijk om toegankelijkheid boven het secundaire niveau – dat voor een belangrijk gedeelte al is gerealiseerd – te veronderstellen, zonder een duidelijk beeld te moeten schetsen van de aard van die hogere niveaus van toegankelijkheid, en de mate waarin zij aan moeten sluiten bij diverse doelgroepen met verschillende kennis- en opleidingsniveaus.

In feite gaat het recht op toegang tot juridische informatie om primaire en secundaire toegankelijkheid, en het recht op toegankelijke juridische informatie om tertiaire en quartaire toegankelijkheid. Dat de huidige tertiaire quartaire toegankelijkheid voor brede lagen van de bevolking tekortschiet, is gemakkelijker te constateren dan er een oplossing voor dat probleem te realiseren is. De vestiging van een grondrecht, gebaseerd op een epistemologische lezing van het legaliteitsbeginsel, zou een goede start zijn om articulatie van het recht serieus aan te pakken. Als immers dan de toegankelijkheid van het recht tekortschiet, kan de burger zich gemakkelijker verschonen in gevallen waarin dat recht onbegrijpelijk is, en heeft de wetgever een duidelijke 'incentive' om die toegankelijkheid te verbeteren.

Verwijzingen

Bernet & Berteloot 2006
H. Bernet en P. Berteloot (2006), EUR-Lex: A multilingual on-line website for European Union law, in *International Review of Law Computers & Technology*, 20(3), p. 337–339.

Jamar 2001
S.D. Jamar (2001), The Human Right of Access to Legal Information: Using Technology To Advance Transparency and the Rule of Law, in *Global Jurist Topics*: 1(2), p. 1-13.

Kranenborg 2007
H.R. Kranenborg (2007), *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie. Over de openbaarheid van persoonsgegevens*, proefschrift Universiteit Leiden, Deventer: Kluwer.

Kranenborg & Voermans 2005
H.R. Kranenborg and W.J.M. Voermans (2005), *Access to Information in the European Union; A Comparative Analysis of EC and Member State Legislation*, Groningen: Europa Law Publishing.

Mommers 2002
L. Mommers (2002), *Applied legal epistemology: building a knowledge-based ontology of the legal domain* (Ph.D. thesis).

Mommers 2008
L. Mommers (2008), 'Opinie – Rechtsbronnen op het internet: keer maar om die Kliko!', in: *Tijdschrift voor Internetrecht* 2008(6), p. 155-156.

Mommers 2009
L. Mommers, W.J.M. Voermans, W.I. Koelewijn and H.H. Kielman (2009), 'Understanding the Law: improving legal knowledge dissemination by translating the contents of formal sources of law', in: *Artificial Intelligence and Law* 2009(17), Springer Netherlands, p. 51-78.

Mommers & Voermans 2007
L. Mommers and W.J.M. Voermans (2007), 'Overbruggend wetgeven in Europa. Over termen, definities, concepten en het koppelen van Europese en nationale regelgeving', in: *RegelMaat* 2007(6), p. 231-243.

Zwenne 2009
G.-J. Zwenne, 'Over kopieerbeperkingen in elektronisch bekendgemaakte besluiten', in: *Tijdschrift voor Internetrecht 2009(2)*, p. 31.

Towards transparency as a basic human right

Ignace Snellen■

Summary

Transparency is becoming one of the essential characteristics of the information age. It opens new avenues to self-fulfilment and democratization, provided that it is recognized as a basic human right and guaranteed by the national constitutions and international institutions.

In this paper the techniques by which transparency is enhanced, and some examples of the effects, opportunities and threats of transparency are indicated. It is argued that transparency has to be guaranteed not only by ordinary laws but also by national constitutions and international arrangements.

The transitions are specified transparency has to pass through in order to realize its full potential. A transition from ordinary law to constitution, from access to documents to access to data, from the vertical relation between citizens and states to the horizontal relation between citizens and private institutions in the public sphere, and from national governments to international institutions.

A provisional indication is given of the importance of transparency as a basic human right for the development of the full potential of citizenship in a democratic society through fighting unwanted consequences of 'information asymmetry'.

Introduction

During the last centuries, political philosophers and lawyers have formulated basic human rights as a protection against an overpowering state, as a claim on the state with respect to provision of basic necessities to be delivered by the state, as well as a condition to participate in democratic deliberations and policy making. They are called basic human rights, because they are in principle inalienable rights connected to the existence of the human personality. They are quintessential for the personal and social functioning of citizens in a modern democratic society.

■ Ignace Snellen is professor at Erasmus University, Rotterdam. The author would like to thank professor Corien Prins and professor Peter Cornelisse for their valuable suggestions and references.

A fully developed 'Information Age' without transparency as a basic human right is, in my opinion, unthinkable. Transparency in the information age will have various appearances and serve different purposes. In this paper the focus is on transparency as a precondition for the development of the full potential of citizenship in a democratic society.

Some basic human rights create a 'state free' sphere, within which citizens can develop their personality according to their nature and their possibilities, and as equal to their co-citizens, without interference of state authorities. The rights that create a 'state free' sphere are so-called 'classical' basic human rights. Examples are the freedom of speech, the freedom of organization, the freedom of the press, the right of privacy, and confidentiality of mail. Their function is to give protection against the state.

Other basic human rights have a more 'social' character. They oblige the state, albeit often without legal enforcement, to take care of the basic necessities of the citizenry such as decent housing, health care, education, a minimum income, etcetera.

A third category of basic human rights can be recognized as 'democratic' rights. To this category belong, amongst other ones: the right to vote, to be eligible for election, to participate in political decision making, the right to establish political organizations, or to join these. The gist of this paper is that transparency has to belong (belongs) to the category of basic human rights. As such it may bridge the classical, social and democratic basic human rights. This is the more important since in many countries, the state retreats from the guaranties promised by their social constitutional rights.

This paper is primarily focused on the transparency of the state, or more widely on the transparency of a public sector, which in one way or another is supported or controlled by the state. The question discussed in this paper is, whether a complete and in principle unhindered freedom of information (*with respect to documents, information, and data*) has to be recognized as a basic human right. If the answer is positive, the next question is whether this basic human right belongs only to individual persons, or also to collectivities. Many applications of this basic right will be exercised mainly on behalf of a collectivity. It will often be exerted by interest groups on behalf of citizens.

The discussion about public sector information is almost completely dominated by considerations of privacy, intellectual property rights, users' rights, and inter-organizational data sources and data exchanges. Prins remarks in this respect: "…a clear tendency can be detected not only in the US but also in the EU towards an expansion and reinforcement of intellectual property rights at the expense of freedom of information.

In this context it is of pivotal interest to "include principles and guarantees on access to public sector information [in a broad sense – IS] in the constitutional catalogue of fundamental rights""[1] If transparency, guaranteed by the constitution, is the rule, then privacy considerations and other consti-

1 Prins 2004.

tutional rights have to be balanced out with it. Restrictions added by clauses and by subjective rights, such as intellectual property rights, based on ordinary laws, have to be treated as exceptions on this rule. And according to a basic rule of legal interpretation exceptions and restrictions added by clauses always have to be interpreted restrictively. Here lies the significance of the recognition of transparency as a constitutional right. Point of departure is the 'right of way' of transparency as basic human right.

From an international comparative study[2] with respect to developments in Sweden, Germany, France, Belgium. The United States, and Canada it appears that only two of these countries (Sweden and Belgium) recognize a constitution based – instead of only a law based – right of access to government information.[3] The Swedish constitution recognizes a right of access to documents. The Belgian constitution recognizes a right of access to documents, as well as data, on which policies are based. It is important to realize that transparency of public sector information can be more than the right to be informed about the documents, information and data used to develop a policy. At least as important are the relevant documents, information and data *not used* during the development and implementation of a policy.

This paper is written on basis of the conviction that recognition of transparency as a basic human right might be one of the most important contributions of the information age to the development of democracies.

Dutch experience

In February 1999 the Dutch government installed a commission on 'Basic Human Rights in the Digital Age', called the Commission Franken, after its Chairman, a professor at Leyden University.[4] The Commission was installed to consider whether protection of the confidentiality of mail, telephone and telegraph, as formulated in the Dutch Constitution, had to be redefined and extended to other forms of electronic communication. A second consideration to install the Commission was to advise the Dutch government on the desirability of formulating in the Dutch Constitution new basic human rights for the information age, such as a basic human right of freedom of information.

For a recognition of transparency as a basic human right, the following aspects are of direct importance: digitalization of information, which allows to distribute information almost for free; miniaturization, which reduces the cost of electronic information and communication devices; and the convergence of data processing technologies. According to the Commission, there

2 Alis Koekkoek a.o. (2000), Bescherming van Grondrechten in het Digitale Tijdperk, (Protection of constitutional rights in the digital age).

3 Recently freedom of information is recognized also by the constitution of Norway.

4 The author of this paper was a member of this Commission.

are no technical or financial obstacles to, in principle, unlimited access to government (or public sector – IS) information.

Transparency is indeed recognized as a (dominant) phenomenon of modern societies, but the reactions to growing transparency are in practice to a larger degree inspired by defensive considerations of privacy, than by attempts to develop the possibilities for the citizens to improve their democratic participation.[5]

In this paper, focus is on transparency, not primarily as a dimension of the information society, but as a candidate basic human right. Constantly growing transparency as a dimension of the information society leads to the urgent question whether the opportunities and threats, the pleasures and pains, of this transparency are equally divided between citizens and the state, between citizens and public sector organizations (such as schools, hospitals, etcetera) and between citizens themselves. The questions to be answered are:

– Is the division of opportunities and threats of transparency in modern societies unequal to such an extent, that legal protection of vertical (citizen versus state) and of horizontal (citizen versus public sector organizations or other citizens) transparency is required by its recognition as a basic human right?

– Can democracy in the information society develop and grow without recognition of transparency as a basic human right?

First, the technological and social developments and applications will be discussed, which lead to a growing transparency in the relations between citizens and the state or public sector organizations, as well as between citizens amongst each other. Secondly, the effects of this growing transparency will be illustrated by examples, which give an indication of the direction of the transparency developments in the information society. Thirdly, the opportunities for supporting the democratic potential of transparency in the coming, and partly already existing, information age will be discussed. And lastly, the recommendations of the Dutch Commission as to the creation and recognition of a fundamental right with respect to access to government information and data will be clarified and critically discussed.

5 On his first day in office President Obama issued an Executive Order on transparency of the Federal Government. However, executive privilege can be claimed to withhold presidential documents from the public if the "deliberative processes of the executive branch would be impaired."
In Estonia early involvement of the public with legislative processes (labeled TOM: "today I decide") failed because of lack of interest with the bureaucracy.
The Dutch minister of Justice installed "digital consultation" with respect to laws and regulations on 6-24-2009 for a test period of 2 years.

Digitalizing, 'informating' and data-mining as transparency enhancing techniques

Because of the transition from analogous to digital signal processing, at every instance a moment of 'storage' of the information and communication signals is introduced. The difference between a moment of storage and permanent storage is a gradual one. The digital storage capacity is growing ('Moore's law'), and thereby, the moment comes closer of a practically unlimited storage capacity, and permanent saving of information and communication signals.

If this growth of storage capacities is connected to the 'informating' characteristics of information technology, one realizes the growth of transparency to which the information society will lead. 'Informating' means that computers not only register primary data, but at the same time also 'metadata', i.e. data with respect to, e.g., the time and circumstances in which the primary data were acquired. Not only the content of the cell phone conversations can be saved, but also the place where the call took place, with whom, the duration of the call, the way in which the call was paid, etcetera. Shoshana Zuboff, who introduced the term 'informating', rightly pointed to the 'Panoptic Power of Information Technology':

> "The action of a machine is entirely invested in its object, the product. Information technology, on the other hand, introduces an additional dimension of reflexivity: it makes its contribution to the product, but also reflects back on its activities and on the system of activities to which it is related."[6]

> "It provides a deeper level of transparency to activities that had been either partially or completely opaque."[7]

While Zuboff refers especially to the world of automated production organizations, her observations are also valid for every kind of computer applications in the information society at large. Informating has found its counterpart in data-mining. While informating takes place in an implicit way, data mining is a purposive activity characteristic for the information age. Through forms of data mining data are connected to each other, to derive regularities or law-like patterns out of them. In data mining continuously refined mathematical techniques are used. Connecting data-repositories and relational databases has led to qualitative leaps in the creation of relevant information about the situation and activities of groups of the population. The data, on which the analytical approaches of data mining are applied, may be created by direct observation, indirect observation, or new ways of information transfer. In the following sections, examples of these modalities of data creation are mentioned.

---

6 Zuboff, 1988, p. 322.
7 *Idem*, p. 9.

Transparency through direct observation

Tracking, tracing, monitoring, and surveillance are facilitated by new electronic possibilities. Some examples: the observation of money traffic by banks and other money institutions, the discovery of the place where a telephone call via a mobile apparatus takes place, the tracing of movements of personnel and guests in hotels via the use of electronic keys, global positioning systems (GPS) on police cars or trucks to spot their positions, the use of badges which communicate with sensors in buildings, eavesdropping devices, closed circuit television networks, electronic bracelets to guard the movements of prisoners serving their time at home, and so-called 'loyalty programs' maintained by shop keepers, etcetera. And in the near future an ubiquitous 'tagging' of goods and people will take place.

Transparency through indirect observation

The possibilities to reconstruct behaviour patterns from electronic databases are continuously growing, e.g. matching of databases, and of 'front end verification' and 'profiling' as detective approaches to fight fraud. Geographical Information Systems (GIS) deserve a special note in this respect. They are very strong tools to analyze and integrate data about the growth and development of problematic situations. By relating geo-information stored in GISs with administrative data about the activities of governments and private parties, very informative and convincing analyses and charts can be constructed with respect to the spread of those problematic situations.

Transparency by electronic data transfer

Examination of information in a situation of manual storage and transfer of data is much more complicated – if at all feasible – than in a situation where Electronic Data Exchange (EDI), XML, Internet and e-mail are readily available as carriers of communication. A single key punch may suffice to inform a huge amount of people. With the creation of applications on web sites, and the providing of interactive services, an approach is chosen that will appear to be irreversible and will lead to ever growing progressive disclosure of information.

Some examples of the effects of transparency

Without a claim to be exhaustive, some opportunities and threats of growing future transparency may be brought forward. But before that, some examples may be given to illustrate how much transparency has become self evident in societal exchanges and in some relationships between state, public sectors and society.

A first (Dutch) example is sentencing practice. The wide differentiation in penalties by judges for the same misdemeanors became visible through the application of information technology. The transparency of this situation led to the threat of a growing harm to the legitimacy of administration of justice. Judges and public attorneys drew the conclusion from this fact that a further transparency and justification of the administration of justice had become necessary. The publication of a standardized penalty base on the website of the Public Prosecutor followed. Since then, citizens have known the exact consequences of traffic offences.

The greater transparency of administration of justice had as a different consequence that politicians tend to encroach more intensively upon priority setting and effectiveness of judicial administration. Tensions between the Executive and the Judiciary are growing as well.

A second example are the welfare barometers which are produced in many cities – often with the help of Geographic Information Systems. From the presentation of these welfare barometers not only emerges the relative deprivation of certain quarters of the city or of certain groups of the population, but also the relative effectiveness and the (un)balance of the policies of city government. Those welfare barometers are starting points of policy interventions by local politicians, as well as pressure activities by interest groups.

A third example are the overview activities and the interferences by medical insurance companies with respect to the prescription behaviour of medical professionals. On the basis of protocols, benchmarks and analyses, the prescription behaviour of individual doctors can be compared with those of their medical colleagues. An analogous case of these control activities of medical insurance companies can be found in the control activities of central governments and provinces with respect to local governments and municipal services.

A fourth example is Closed Circuit TV as a surveillance technique. CCTV shares with other surveillance techniques:

a. they surpass barriers of distance and darkness. Space satellites observe and zoom in on a level of a few square meters;

b. they surpass barriers of time. A registered image can be stored without time limit and consulted later on;

c. the observations can take place inconspicuously;

d. normally the observations take place without consent of the observed persons, which does not necessarily mean that they take place against their will;

e. the orientation of the surveillance technologies is generally more preventive than repressive;

f. it is possible that a categorical discrimination (e.g. skin color) is built in into surveillance devices;

g. technology provokes self-censorship and self-control with the observed persons;

A commonality between these examples is that they make clear which power shifts are gradually and surreptitiously taking place between state and society, and how this progress could be checked through transparency.

Opportunities and threats through transparency

Threats emanating from growing transparency of the information society get much more attention than its opportunities. Threats are mainly perceived in increased possibilities of constant surveillance and control: control of central government over local governments (e.g. through performance indicators), of governments over private initiative in the public sector, and of governments over their citizens. Negative effects on privacy and on chances of developing one's abilities as a citizen are stressed.

A possible loss of solidarity, on which the system of collective insurance in many civilized countries is based, is seen as a very serious threat. Transparency of genetic predispositions will without any doubt lead to exclusion of risks. It is even questionable, whether one can still speak about risks in a situation of genetic discovery of medical predispositions. The calculation of risks will be replaced more and more by statistical certainties based on genetic research. The nature of insurance itself may (will) change in its essence through the transparency, created by genetics.

If one compares the attention to the possible commercial exploitation of transparency with the attention to the possibilities of its democratic application, one is struck by the unbalance between both. The attention for the possibilities to use information at the disposal of the government for democratic purposes lags behind commercial interest. However, the potential use of information at the disposal of governments for the growth and development of democracy is very promising. As Prins remarks: "…the social and democratic value of information is a key factor in determining the government's role and position in an information society".[8]

The more government policies are based on information acquired through forms of direct and indirect observation, and through electronic data transfer, as mentioned above, the more the aspirations and expectations of the citizens, and certainly also of the representatives of their interests, will increase to make their independent analyses on these sources of information.

Pressure will also grow, not only to refer to and make analyses on *documents*, on which a (proposed governmental) policy is based, but also on *databases* – used and not used! – which may have, or could have, played a role in

8 Prins 2004.

the position chosen by a government or public sector organization. Further on in this paper more will be said about this.

Finally, the potential of surveillance technologies to give the public space back to the people deserves to be mentioned. Such a free disposition of the public space by the citizens is an essential condition for participation in cultural and social life. By the deterioration of safety in the public domain, many citizens – especially women and older people – have practically lost the possibilities to this participation. Defenders of privacy – such as the Dutch privacy protection authority – object against road pricing, because the necessary surveillance technologies have as a consequence that 'public spaces are no longer places, where people can move and behave freely and unconstrained.' Those defenders of privacy conveniently overlook that now already more than half the population, by lack of application of electronic surveillance devices, dare to use certain public spaces only by clear daylight. In this case physical safety of large parts of the population is sacrificed for informational safety of parts of the population. The message is, that transparency could prove to be the cement of a society, instead of a threat.

Access to documents, information, data and (calculation) models

The Commission 'Basic Human Rights in the Digital Age', mentioned above, showed to be a proponent of a basic human right of access to information resting with the government. The Commission considered that such a right fulfills an essential function for the personal and social functioning of the citizens, and that the existing legislation with respect to freedom of information is developed to such an extent that one may conclude that there is sufficient public support for such a basic human right.

The existing freedom of information legislation is limited to *documents* on which governmental policies are based. The extension to a basic human right, the Commission is aiming at, relates also to *information,* not necessarily in the form of documents, at the disposition of the government. Electronic communication facilities, such as Internet, enhance the possibilities to share this information with citizens. The Commission expects from this an intensification of the democratic constitutional state. As it indicates: "Digital provision of information by the government can support the traditional forms of democratic control and lead to revitalization of the democratic process."[9] The Commission aimed not only at policy and accounting information, but also at data collections, background studies, research reports and statistical data. These knowledge repositories can play a major role during development of policies and decision making. By giving the citizens a legal claim on such knowledge repositories their citizenship is fully recognized.

9 Commissie Grondrechten in het Digitale tijdperk 2000.

Only one member of the Commission[10] opposed the position chosen by the Commission. According to his opinion, the preparation of decision making, and the political weighing and settling of interests have to be protected. The more information forms the substance of decisions, the more carefully the access to this information has to be guarded. According to this member of the Commission: "A right of access to information resting with the government will make the preparation of decisions by the bureaucrats more and more politically relevant." From a point of view of constitutional law, this is, according to this member of the Commission, undesirable.

Two arguments could be raised against the position of this member of the Commission:

1. The monopoly position of the bureaucracy with respect to the sources of information, resting with the government, would be strengthened, and through this the political influence of the bureaucracy on the decision making processes. Putting information at the disposal of the citizenry would, on the contrary, create a valuable countervailing power.

2. The chances for politicians to hide or neglect unwelcome information would be enhanced. In view of the transparency of the digital age the tendency to manipulate information to reach political goals is in the short or long run counterproductive. The worldwide distrust of the citizenry in politics may not be fuelled further.

On the contrary, the growing transparency of the citizenry for the government has to be compensated by a matching transparency of the government and the public sector themselves for the citizens. The access to the documents and information, resting with them, has to be complemented by access to *administrative data*, also resting with them. Administrative data are created by the implementation of policies. In a former part of this paper 'informating' is mentioned; the reflexivity introduced by the use of computers during the implementation of policies. Computers are used to register cases processed by street level bureaucrats at labour exchanges, social security offices, housing departments, police departments, etcetera. Through the phenomenon of 'informating', discussed above, all kinds of comparisons can be produced on the basis of registered data. When the administrative data created at those offices are made available to the citizens, they can be compared with statistical data about unemployment, numbers and needs of subsistence clients, the housing situation in regions and city quarters, etcetera.

By comparison of these geo-data with statistical data, and administrative data, citizens and their interest organizations can check whether the efforts of the governments to alleviate societal problems are in proportion with their relative seriousness, when compared with other regions and city quarters. Geographic Information Systems (GIS) may play a very important role in

10 Later on Minister of Justice.

this respect. They enable analysis and presentation of comparative data in a multidimensional way, in a very convincing manner. To be effective, access to those data requires that they are physically, financially and intellectually accessible; it means, according to a member of the Commission, that there may be no physical barriers or delaying tactics, no financially prohibitive charges, and clear presentation and understandable language.[11]

However, the effect of transparency as a basic human right in the digital age has to encompass more than only access to information and data kept by governments. The more collective tasks, formerly fulfilled by governments, are autonomized, outsourced, privatized or left to private initiative, the more reason there is to oblige the institutes, which have taken over those tasks, to make their policies and practices transparent on the same footing as governmental organizations. Not only the information they are prepared to provide (maybe with a view to public relations), but also the data they use for policy development, or they create during policy implementation, have to be made available. The so-called vertical overview of citizens over governmental policies and activities has to be completed by a horizontal overview of citizens over the policies and activities of schools, hospitals, social housing companies, and the growing number of non-governmental organizations (NGOs).

If this step is not taken, the scope of democracy in the Western world will be decreasing instead of increasing. Participation of citizens in democratic processes is dependent on transparency of information and data, the lifeblood of democratic deliberations and decisions.

Transparency and economics

The political legal vision on transparency as basic human right, developed in this paper, will make itself felt also in the sphere of economic behaviour between private parties. The technological development forces to the realization that transparency as as normative concept has to be related to a much larger range of activities than political legal ones. The more complex societies become, the more the general 'digital divide' of information and knowledge among citizens, clients, and customers increases, and the more the need for transparency among private parties in the economic realm grows. This can be demonstrated by confronting expected consequences of the acceptance of transparency as a basic human right with some fundamental economic tenets about 'information asymmetry' among private parties. In this paper this confrontation takes place at a conceptual level. Empirical research will be necessary to fill out this confrontation in practice.

During the past decades, neo-classical economic theory has undergone a fundamental development with respect to the reception of cognitive and psychological elements in market and organisational relations. The names of

11 Bovens 1999, p. 113.

Coase and Williamson and of some recent Nobel Prize winners are connected to this. They have indicated that the classical economic theory starts from the mistaken assumption of a frictionless relationship between supply and demand on the market, as if there would be no transaction costs and no difference in level of knowledge and information between them. On the contrary, they ascribe to the parties on a market an 'information asymmetry': some relevant information is known to some parties, but not to all of them. When entering a contract relation the one party has more and better information than the other party. This not only determines the attitude of both parties, but it also leads to an unbalance in their power relation, as far as transactions are concerned. Apart from that, such a kind of situation leads to an inefficient allocation of public resources, which can be considered as 'market failure'.

The corrections that have been made on the neo-classical theory by Coase, Williams and others draw attention to forms of lack of transparency which are endemic in highly developed economies and societies. They are related to:

- The relationship between private parties, e.g. a principal and an agent. Even if a hierarchical or authoritative relationship exists between a principle and an agent, both run the risk that their counterpart takes advantage of the lack of knowledge of the real situation to minimize their own effort. (There is no reason to focus only on the risks of the principal. The agent runs a risk as well, due to his possible ignorance.)

- Transaction costs: to these costs belong the costs of finding the correct information, the costs incurred by negotiations and decision making, and the costs connected to surveillance (maybe even enforcement) of compliance.

- 'Moral hazard': the chance that the counterpart adjusts his behaviour to the degree of risk he runs. When the risks are covered, the ensured party may fail to minimize the damage through taking preventive measures, show 'free-rider' behaviour, or to over consume/over supply.

- Opportunism: refers to the incomplete and distorted disclosure of information, especially to calculated efforts to mislead, to distort, disguise, obfuscate, or otherwise confuse. It is responsible for real or contrived conditions of information asymmetry, which vastly complicate problems of economic organization.[12]

- 'Adverse selection': by manipulating and withholding information the agent can create too rosy a picture of his performance and attain that he is undeservedly selected from a pool of possibly suitable candidates, or gets special favours. This has of course a negative influence on the efficiency of the organisation.

12 Based on the Wikipedia lemma.

As the world and societies become more complex, information asymmetries are playing a more important role, and the need for transparency in the economic sphere becomes more pressing. The information density around people, their activities and their organizations is growing exponentially. The information asymmetry is not limited to parties on a market but extends to all kinds of contractual and trust relations in a complex society. For example, principal agent relationships exist between citizens and politicians, between non-elected officials and politicians, and between public sector organizations and their constituencies. In some sectors, the information asymmetry is decreasing because of the technological developments (as mentioned in the first part of this paper), and because more and more people have access to all kinds of relevant information.

Because of the developments sketched above, the need for knowledge and information is also increasing exponentially. Inequalities exist as far as the access to information is concerned. This determines the chances citizens have to develop themselves and to participate fully in a democracy. Transparency, needed in the information age because of these circumstances, has to be adapted also to the level for which it is destined.

At the *micro level* of individual agents and individual decisions, where account managers, in direct contact with clients, shape the policies of the organisation to which they belong, the required transparency encompasses, amongst other things, insight into the decision support systems and databases used, clarity about the 'winning profile', contained in a regulation or an organisational policy, and information about the different dimensions of the discretion of the official, as well as an overview of the state of the case handling procedure.

At the *meso level* of private organisations and institutes in regions and sectors of society belong schools, hospitals, welfare institutes, housing corporations, and other organisations. Formerly they were part and parcel of the domain of the state, or at least they were financed by the state. Many of these organisations have recently been given a degree of autonomy, or they were privatized. Governments have outsourced large parts of public administration to be protected from political responsibility for mistakes in the operational sphere. Especially the transparency of those organisations that operate between law and power, and between politics and markets, deserves to be guarded. Although they may be private parties, their performances in all internal and external relations will have to become transparent. The transparency of ICT applications through open source, for example, fits into this approach.

At the *macro level* of systems, infrastructures and architectures with a national, international, or sectoral scope, transparency is more necessary than ever before. Infrastructural systems transgress national borders and require adaptations, which create very complex interdependencies. The current 'financial and credit crisis' shows how important (lack of) transparency of the relationships and obligations between financial institutes, and for their supervisors, is for the functioning of the macro-level financial system.

Transparency at the macro system level forms a framework within which information and knowledge get their significance.

In practice and with respect to certain transactions the need for transparency in situations of 'information asymmetry' is gradually recognized. The home owner is not legally exculpated any more, when he does not inform the buyer about hidden defects. Through regulations of informative labeling tags will become common practice everywhere. In case of financial products, where small print often plays a decisive role, conditions are not necessarily accepted on face value.

Conclusion

There is still a long way to go towards the recognition of transparency as a basic human right. At least four transitions have to be made. The first transition is from recognition of access to government information in *ordinary laws* to recognition in *national constitutions*, and finally to an *internationally* recognized *basic human right*. A second transition is from free access to *documents* to free access to *data collections*, used or unused for policy development and policy implementation, and finally to *administrative data* as a reflection of the implementation of policies. A third transition is from transparency as a basic human right in the relationship *between the citizens and the state (vertical overview)* to transparency as a basic human right in the relationship *between citizens amongst each other(horizontal overview)*. And finally, a fourth transition to be made leads from full access to information at the disposition of *governments* to full access to information at the disposition of institutions belonging to the *public sector.*

This final transition has become necessary because many activities of the government have been outsourced to private institutions, under the aegis of New Public Management.

Analysis of the consequences of transparency as a basic human right through assessment of the resulting information symmetries and asymmetries seems a viable way to go. The more the complexity of the information society will grow, the more the information asymmetries will tend to increase, if no measures are taken. Modern approaches, as the ones used in economic theories, may enhance the awareness of such developments and their positive and negative consequences. Recently (July 9, 2009) the Dutch government has installed a State Committee to advise about necessary adaptations of the Dutch Constitution to modern times. The role of transparency as basic human right belongs at the agenda of this State Committee.

References

Bovens 2005
M.A.P. Bovens, 'De digitale rechtsstaat' (The digital constitutional state), in: M. Lips, V. Bekkers & A. Zuurmond (eds) *ICT en Openbaar Bestuur*, Lemma, Utrecht, 2005.

Bovens 1999
M.A.P. Bovens, 'Informatierechten' (Information Rights), in: *Nederlands Tijdschrift voor Rechtsfilosofie en Rechtstheorie* 1999(2), p. 102-124.

Commissie Grondrechten in het Digitale Tijdperk 2000
Commissie Grondrechten in het Digitale Tijdperk, *Grondrechten in het digitale tijdperk*, (Constitutional Rights in the Digital Era), The Hague, 2000.

Koekkoek 2000
Alis Koekkoek a.o., *Bescherming van Grondrechten in het Digitale Tijdperk*, (Protection of constitutional rights in the digital age) Final Report of Investigation committed by the Ministry of Justice, 2000.

Prins 2004
C. Prins, 'Access to Public Sector Information, in Need of Constitutional Recognition?', in: G. Aichholzer & H. Burkert (eds), *Public Sector Information in the Digital Age*, Edward Elgar, Cheltenham, UK, 2004.

Zuboff 1988
S. Zuboff, *In the Age of the Smart Machine*, Oxford, Heineman Professional, 1988.

Public access to standards: some fundamental issues and recent developments

Kees Stuurman■

Introduction

'Access' seems to be a critical word in relation to technical standards and standardisation. In the process of standard setting, access to the process by 'all parties concerned' is one of the basic rules for formal standardisation. Furthermore, during the process, access by industry to technological solutions is a key issue, often impeding the process of setting standards under – at least – 'acceptable terms' (RAND, FRAND, …).[1] Once the standard is set, access to its contents by both industry and the public at large is key for various, sometimes conflicting reasons. Those reasons include the financial viability of standardisation bodies and, in case of standards used in legislation, the fundamental rights of access to legislation.

The issues at stake will be explored particularly in view of recent case law in The Netherlands and litigation that is currently pending in the USA. In the analysis it will be shown that the aspect of 'access to standards' is situated at the crossroads of fundamental rights (including IPR's, freedom of information and constitutional duties).[2] Furthermore, it will be shown that copyright licensing of standard documents as a source of income by national standards can be endangered by the constitutional requirement to make legislation publicly available. In view of recent case law, at least in the Netherlands, government intervention might be required to safeguard the continued use of reference to standards in legislation. Given the European background of most of the relevant standards, without such intervention, there might even significant pressure on the European 'New Approach', which is founded on applying the outcome of private standardisation procedures in public rule making.

■ Kees Stuurman is full professor at the Tilburg Institute for Law, Technology and Society (TILT), Tilburg University. He is partner of Van Doorne attorneys, Amsterdam.

1 'RAND' stand for: 'Reasonable and Non Discriminatory' terms for licensing. 'FRAND' stands for 'Fair, Reasonable and Non Discriminatory' terms for licensing of Intellectual property rights in certain elements of a standard.

2 It is important to note that not only constitutional requirement regulate the access to standards. See for example the WTO Agreement on Technical Barriers to Trade in which it is set out that all technical regulations that have been adopted shall be published promptly or made available to interested parties otherwise (art. 2). This regulation, however, provides a different point of view to the issue of 'access'. It is primarily drafted to create a level playing field for access to standards rather than ensuring public access in a constitutional perspective which will be the focus of this contribution.

It is this mixture of conflicting legal standards and economic considerations that makes this topic interesting. It is my hope and expectation that it will also align with Aernout Schmidt's interests.

The issue of 'public access'; caught between copyright and constitution

Copyright licensing of standard documents is a major source of income for most national standards bodies. This source of income can however be endangered by the constitutional requirement to make legislation publicly available. This might ultimately result in loss of copyright.

On the other hand, a regulatory strategy which builds on reference to standards can be endangered when access to the relevant standards is, often due to copyright in the standards, not in conformity with constitutional requirements for access to legislation. This is clearly demonstrated by a recent decision (31 December 2008) of the District Court of The Hague. Should this Dutch court decision be upheld in appeal, at least in the Netherlands a government intervention seems required to ensure that reference to standards can result in binding legal requirements.[3]

In the next sections, we will take a closer look at both the constitutional aspects and (the role) of copyright. As will be discussed in more detail below, for Member States of the European Union the issues at stake are not merely national. In most cases, reference is being made to standards with a European background (i.e. set by the European standards bodies). Increased pressure on standard bodies to lower the barriers for access to standards (without adequate compensation) will put significant pressure on the European 'New Approach', in which the cooperation between European lawmakers and private standard bodies is key.

Public access to standards and constitutional requirements

The adage 'ignorance of the law is no excuse' is usually supported by constitutional requirements to make legislation publicly available. The question to what extent these requirements also apply to technical standards has been debated for decades. Schepel and Falke refer to relevant Austrian case law even going back to 1966.[4][5]

3 The parts of this publication in which this decision and the (possible) consequences thereof are being explored, are based on my annotation (in Dutch) of the decision of the District Court of The Hague of 31 December 2008 ('Knooble'), AMI/Tijdschrift voor Auteurs-, Media- en Informatierecht (Journal for Copyright, Media and Information Law), 2009/2, p. 72 – 75.

4 See: Schepel & Falke, 2000, p. 164-165.

5 See as well: Stuurman 1995, p. 161 ff.

In the early 1990's the European Commission has taken a clear stand on the matter of public access to standards. In its 1992 Communication on Intellectual Property Rights the Commission stated that: "(…) where compliance with a standard or a part of a standards is referred to in Community legislation, either as a mandatory requirement or as one which confers a particular status under Community law, the contents of that standard are made available to all interested parties on a fair, reasonable and non-discriminatory basis".[6]

In this case, the Commission did however not act on the basis of concern about constitutional requirements. In essence is was a competition law issue related to IPR rules (then) set by ETSI (the European Telecommunications Standards Institute).[7] In most cases, access to standards used in legislation on a "fair, reasonable and non-discriminatory basis" will probably not be enough to satisfy the constitutional requirements for public access to legislation.

Reference to standards is the most common way of using standards in legislation. In discussing this issue it is important to keep in mind that reference to standards can take several forms. In particular the distinction between mandatory and non-binding standards is relevant.

Especially in case standards should be complied with on a mandatory basis, it could be argued that these standards should also be made publicly available. In a few countries those standards are indeed being published and accessible for free. However, in the majority of the EU member states, there is only the possibility of free consultation at the premises of the national standards bodies, in some cases extended with access in (a number of) libraries. In the year 2000, Falke and Schepel concluded that only in Finland, Germany and the United Kingdom there is a sufficient number of libraries where standards can be accessed to "really lay constitutional worries about public access to standards to rest".[8]

Today, nine years later, even this – relatively sombre – conclusion is probably too optimistic. With the introduction of the internet, the phrase 'access' has become more encompassing and one could seriously doubt whether nowadays access to standards in a library in printed form only, is a fully adequate way of complying with the relevant constitutional requirements. Internet access to public sector information is becoming the 'standard'.[9]

Key issue in this respect is whether 'mere' reference to standards will give these standards the status of legislation, and hence make them subject of constitutional publication requirements. In a recent courts case in the Netherlands the answer to this question was affirmative.

---

6 COM (92) 445 final. The document can be accessed at: http://ec.europa.eu/enterprise/standards_policy/reference_documents/index.htm.

7 Falke & Schepel, p. 176 ff.

8 Falke & Schepel, o.c., p. 165.

9 See e.g. the recitals of the Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, OJ L 345, 31.12.2003.

A Dutch (test)case: Knooble vs. State and NNI

In a decision of the 31st of December 2008, the District Court of The Hague decided that the reference to standards of the NNI (Netherlands Standardisation Institute) as contained in the 2003 Dutch Buildings Decree and the regulations based thereupon, are not binding. This is due to the fact that, by this reference, these standards have become general binding rules and hence should have been made public in accordance with Dutch constitutional requirements.[10] The current practice, in which the contents of the standards are not being published and can only be obtained (against payment of a fee) from NNI (as copyright holder or distributor for other standards bodies) is considered inadequate in view of the constitutional standards for publication of legislation.

Another interesting element of this case is that when the standards will be published in accordance with the constitutional requirements this will, in accordance with Article 11 Dutch Copyright Law (DCA), result in the loss of copyright for NNI (or other copyright holders) and hence the possibility for NNI to generate income from the publication of standards. Since NNI is in part financed by selling standards, the financial viability of its organisation will then be at stake. In its current decision, the District Court did not yet anticipate upon these consequences, since Article 11 DCA only applies to documents that actually *have been* published in accordance with the aforementioned constitutional requirements.

Obviously this decision has far reaching consequences, most likely even outside the scope of the building legislation. Early 2009, the State has announced it will appeal the decision of the District Court. As indicated in the title of this section, this court case is a test case, i.e. it has been started after consultation of the parties involved. This does not impair the significance of the case; the outcome will be binding. It might still take several years before a final decision has been reached. It is not unlikely that the case will be up for future review by the Dutch Supreme Court as well.

Background

As a starting point, NNI's standards are set by 'all parties concerned'. NNI supports this process, but it does not contribute to the contents of the standards. After this process is concluded, including public consultation, the standards' contents are adopted by NNI. Subsequently, the standards are (in a certain layout determined by NNI and exclusively mentioning their name) published by NNI, allowing for NNI's copyright (art. 4 DCA) and hence giving NNI the exclusive right to further publication and reproduction.

10 The Court largely follows the analysis and conclusions of Mirjam Elferink, as set out in her dissertation (Elferink 1998). The State has argued differently. In a response to parliamentary questions resulting from Elferink's dissertation, the Minister of Justice indicated at the end of the '90's that in his opinion, reference to NNI standards did not make them binding but only provide a result that could be achieved alternatively as well (the relevant Building Decree also contains a so-called equivalency provision).

A licence to the standards documents can be obtained upon payment of a fee (averaging 62 Euros per standard).

As a matter of principle, Knooble B.V., a Dutch consultancy company in the building industry, finds it unacceptable to have to pay for standards imposed by the State in the Building Act and legislation based thereupon. In a summons issued on the 21st of September 2006 Knooble summoned both the State of the Netherlands (Ministry of Housing, Spatial Planning and the Environment) and NNI, generally claiming the following. First, a declaratory judgement is claimed stating that certain NNI standards are not binding because they form general binding rules that have not been made public in accordance with Article 89 of the Dutch Constitution and Articles 3 and 4 of the Publication Act; or at least NNI standards or their contents are not part of the Building Act and the 2003 Building Decree. Second, a request was made to rule that the relevant NNI standards, or at least their contents are free of copyright on the basis of Article 11 of the DCA. In addition it was claimed that the written or digital form of the relevant NNI standards (or at least their contents), including new versions, should be available for no more than a reasonable fee covering reproduction costs, and free of any copyrights.

The latter claims were denied since the relevant standards had not yet been published in accordance with the constitutional requirements, and hence article 11 DCA was not (yet) applicable. The District Court did award the first claim by deciding that the relevant standards are not binding because they form general binding rules that have not been made public in accordance with Article 89 of the Dutch Constitution and Articles 3 and 4 of the Publication Act.

Binding nature of standards: the effect of equivalency provisions

A crucial element in the District Court's argument is the conclusion that the 'equivalency provision' included in the 2003 Building Decree does not impair the binding character of the relevant NNI standards. On the basis of such an 'equivalency provision', the relevant legal requirements may also be complied with differently than by following the relevant standards. Nevertheless, according to the District Court these standards are a part of the legal reference framework. I understand these arguments insofar as the Court concludes that knowledge of the relevant NNI standards is inevitable, even for complying with the relevant legal requirement by other means than applying the relevant standards.

Indeed, in many cases in which an alternative is offered by a equivalency provision, access to the relevant standards will be essential to determine which level of safety, security, health care etc. the legislator is actually requiring. In that sense, equivalency provisions often merely provide 'pro forma alternatives'. Compliance with the relevant technical standards provides a presumption of evidence (i.e. it is up to the government to show non-compliance), whereas, in case the alternative approach is taken, the burden of proof is shifted. In the latter case it is up to those applying the alternative approach to give evidence of conformity with the relevant legal norm.

US case law: Veeck vs. Southern Building Code Congress International (SBCCI)

In 2003, the US Supreme Court denied reviewing a decision of the U.S. Court of Appeals for the Fifth Circuit concerning copyright in model codes.[11] The case focussed on the issue of copyright with respect to private model codes used by reference in local ordinances that were adopted by two municipalities. Although no technical standards at stake, from a legal point of view, the issues were very similar.

The key issue that was addressed in this case is to what extent copyright can be used to restrict individuals for making copies of the model codes that were incorporated by reference in the municipal codes of Anna and Savoy, two municipalities in the State of Texas. In this case, the copyright in the relevant material was owned by Southern Building Code Congress International (SBCCI), a non-profit organisation that creates model codes, including fire prevention, gas, mechanical, and plumbing codes. Peter Veeck, an individual operating a non-profit website providing free information about North Texas, bought digital copies of the model codes and put them on his website identifying these documents as the building codes of the two municipalities. Veeck did not indicate that the codes were SBCCI's codes nor made reference to SBCCI's copyright. After having received an infringement letter from SBCCI, Veeck filed a declatory judgement action against SBCCI, which counterclaimed for, amongst other things, copyright infringement.

The U.S. Court of Appeals for the Fifth Circuit (in a *reversed decision*) ruled that "(..)in continuing to write and publish model building codes, SBCCI is creating copyrightable works of authorship. When those codes are enacted into law, however, they become to that extent "the law" of the governmental entities and may be reproduced or distributed as "the law" of those jurisdictions."[12]

In reaching its conclusions, the Court observed that: "Veeck copied the building code of the towns of Anna and Savoy, Texas, based on their adoption of a version of the SBCCI model code. The codes are "facts" under copyright law. They are the unique, unalterable expression of the "idea" that constitutes local law."[13] (....) While the Supreme Court has not stated directly that laws are "facts," it has broadly observed that, as with census data, "the same is true of all facts – scientific, historical, biographical and news of the

11 Veeck v. S. Bldg. Code Cong. Int'l, Inc., 293 F.3d 791 (5th Cir. 2002) (en banc), cert. denied, 539 U.S. 969 (2003).

12 Court decision, par. 49.

13 Court decision, par. 43.

day. 'They may not be copyrighted and are part of the public domain available to every person.'"[14]

The conclusions of the U.S. Court of Appeals illustrate the widely applicable rule that statutes, regulations, but also court decisions, are excluded from copyright protection.[15]

As a major element of its defence, SBCCI stated that, when copyright was denied, it will lack the revenue to continue its public service of code drafting. SBCCI hence needs copyright's economic incentives. In response, the Court not only pointed out that it is not the sole purpose of the copyright law to secure a faire return for an author's creative labour, but it also dealt with SBCCI's argument in far more detail, observing that:

"First, SBCCI (....)has survived and grown over 60 years, yet no court has previously awarded copyright protection for the copying of an enacted building code under circumstances like these. Second, the success of voluntary code-writing groups is attributable to the technological complexity of modern life, which impels government entities to standardize their regulations. (...). The self-interest of the builders, engineers, designers and other relevant tradesmen should also not be overlooked in the calculus promoting uniform codes. As one commentator explained, it is difficult to imagine an area of creative endeavor in which the copyright incentive is needed less. Trade organizations have powerful reasons stemming from industry standardization, quality control, and self-regulation to produce these model codes; it is unlikely that, without copyright, they will cease producing them. Third, to enhance the market value of its model codes, SBCCI could easily publish them as do the compilers of statutes and judicial opinions, with "value-added" in the form of commentary, questions and answers, lists of adopting jurisdictions and other information valuable to a reader. (...)could also charge fees for the massive amount of interpretive information about the codes that it doles out."[16]

For the US, *Veeck* is a next step, but it does not provide answers to all issues at stake. Precedents more favourable to standard setting organisations exist elsewhere.[17] The discussion is likely to continue.

---

14 Feist, 499 U.S. at 348, 111 S.Ct. at 1289; Court decision, par. 45; See for a broader overview of US copyright issues at stake in using the result of private standards in legislation: L.A. Cunningham, Private standards in public law: copyright, lawmaking and the case of accounting, Boston College Law School, Legal studies, research paper No. 60, March 2, 2005 (http://ssrn.com/abstract=677647).

15 For the European Member States, see: Schepel & Falke, o.c., p. 169 ff.

16 Court decision, par's 66-69.

17 Brodoff 2005 refers to PMIC v. AMA, 121 F.3d 516 (9th Cir. 1997) en CCC v. Maclean Hunter, 44 F.3d 61 (2d Cir. 1994). (See: http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/SDO%20Legal%20Issue%20Forum%20-%20Archives/2005%20Legal%20Issues%20Forum/Brodoff-Panel%204.pdf).

Copyright in standards: a valid presumption?

The (possible) loss of copyright when standards have become a part of 'the law', and especially the assumed consequence (loss of revenues), presumes that basically, standards (i.e. standards documents as the representation of standards) can be protected by means of copyright.

Copyright generally requires that the relevant 'work' (e.g. a written document) is 'original', a concept usually further elaborated on in case law. In the Netherlands, under the DCA this means that a work must have its own original character and must bear the personal stamp of the producer.[18] The 'original character' required means that the form of the work may not have been derived directly from another work. A 'personal stamp' means that the form as chosen is the result of human creative effort, and thus of creative choices, and therefore the product of the human mind.

Arguments against the adoption of copyright claims particularly concentrate on striving for standardisation of design and structure of standard documents, the use of common technical conventions and the often limited freedom of choice in adequately representing the technical choices contained in the standard. In addition, an important factor is that in drafting standards documents, the technical specifications should be unambiguous so that they can be applied uniformly.

The arguments in favour of copyright protection do hence not seem to be convincing under all circumstances. Nevertheless it is generally assumed that standard documents are protected by copyright law.[19] As regards Dutch copyright, I agree with Elferink that as a rule, NNI standards documents will be eligible for copyright protection.[20]

How to proceed?

How to overcome the fundamental tension between the constitutional right of (free) public access to legislation and the (economic) exploitation rights of standards bodies? In the Netherlands, the government has, so far, taken the position that in case the relevant statute holds an equivalence provision, a reference to standards does not imply that they become general binding rules, because the result could have been achieved otherwise. In this approach there is no conflict; the relevant standards do not have to be made public in the same way required for legislation, hence allowing for exploitation of standards by national standards bodies. The sustainability of this

18 Dutch Supreme Court, 30 May 2008, LJN: BC2153, C07/131HR (Endstra-tapes).

19 See for the EU Member States: Schepel & Falke, p. 169 ff.

20 Elferink 2007, p. 83. Elferink has previously investigated this question in her dissertation and concluded at that time (1998) that it was "highly doubtful" that the NNI standards would be protected by copyright. (Elferink 1998, p. 167). Also see: Stuurman 1995, p. 437 ff.

approach will be decided by the The Hague Court of Appeals, and probably ultimately even the Dutch Supreme Court, in the currently pending appeal of *Knooble*.

Following a decision of the German Supreme Court (Bundesgerichtshof), the German government was forced to adapt legislation in order to safeguard copyright for standards (and hence their exploitation by DIN) that are being referred to in official publications. Already in 1990, the German Supreme Court decided that reference to DIN standards can also fall under the scope of paragraph 5 Urheberrechtsgesetz (German Copyright Act, GCA) on the basis of which 'Amtliche Werke' ('government documents') are free of copyright.[21] In 1998, the German Constitutional Court (Bundesverfassungsgericht) denied to reverse the case in appeal, as was requested by DIN. Following that decision, the German legislator has intervened and a new subsection 3 has been added to paragraph 5 GCA on the basis of which the copyright of private technical standard is not lost when referring to these documents in legislation. This 'assistance' to private standardisation bodies like DIN is linked, however, to a compulsory licence which is based on every publisher's right to obtain a licence under appropriate conditions.[22] This approach probably ensures an improved accessibility to technical standards but leaves the fundamental issue (no copyrights in legislation) unresolved.

In *Veeck vs. SBCCI* the United States Court of Appeals, Fifth Circuit not only denied SBCCI's copyright claims, but it also referred to the possibilities of amending SBCCI's business model in order to make organisations involved in standardisation less dependent on the mere exploitation of standards. Many standards bodies have incorporated elements of such alternative business strategies in their market approach already. Nevertheless, they often seem to remain largely dependent on the results of exploiting standards documents.

In this matter, economic considerations can to a large extent be instrumental in finding a proper solution for an adequate balance between on the one hand the fundamental right to access standards that have become a part of the current body of law, and on the other hand a continued production of standards by the private sector. Adequate financial support by governments could in principle ensure both free access to standards referred to in legislation as well as economic viability of standards bodies. In the EU, a solution leading to free access to standards for the public at large can only be achieved in cooperation between the Member States. This is due to the fact that, to an increasing degree, in national legislation reference is made to standards that have not (exclusively) been developed within the relevant national standards bodies, but are translations of the European standards as developed by the

21 BGH 26 April 1990, GRUR, p. 1003-1005. See for more details: Elferink 1998, p. 143 ff. A claim from DIN against the ruling of the Bundesverfassungsgericht was rejected (BverfG, 1 BvR 1143/90 on 29 July 1998).

22 See also: Elferink 2007, p. 86 ff.

European standards bodies: CEN (the European Committee for Electrotechnical Standardization), CENELEC (the European Committee for Standardization) and ETSI. This is a consequence of the European 'New Approach'.

The 'New Approach' is a regulatory approach, adopted in 1985, in which European Directives are restricted to setting out 'fundamental requirements' (safety, environment, health care), whereas their technical specifications are achieved by reference to European standards. This is a new approach because, prior to its introduction, the development of the legal norms of European Directives took place in the political arena. This resulted in endless discussions about all kinds of technical details. In order to make some progress in drawing up European legislation, it was then decided to leave the practical aspects to the market.

Examples of 'New Approach Directives' include the European Directive on General Product Safety[23] and the European Machinery Directive.[24] Copyright with respect to the underlying European standards is claimed by CEN, CENELEC and ETSI. National standards bodies, such as DIN and NNI, sell (distribute) the standard documents on the basis of a licence from the European standards bodies. It should be mentioned that ETSI has developed a different approach in which the standards can in principle be downloaded for free from the ETSI website. Further use might be subject to restrictions. In this respect it is important to note that in particular in setting telecommunications standards, often large numbers of patents are relevant.

The European background of most standards that are being used by the legislator implies that national governments have to take the exploitation rights of the European standards bodies into account if they should want to ensure free public access to standards. If, for instance, the Dutch government wishes to publish a standard as part of a statute, then on the basis of article 11 DCA, NNI can no longer effectively claim its copyright with respect to the standard. The first consequence would be that NNI would loses income. Even more problematic would be the fact that the exploitation monopoly, outside the Netherlands, of in particular CEN and CENELEC could be affected as well. At any rate, the Belgian market for standards would come under pressure. An even wider effect might arise, since the translation of European standards to Dutch is sometimes limited to adjusting the front page, leaving the standard itself in English.

Certainly not all standards set by the European standardisation bodies are part of the 'New Approach'. Nevertheless, a loss of the possibility of exploiting these standards will sensitively affect the financial position of the European standards bodies. This will ultimately also put the New Approach under pressure. Clearly, any fundamental solution respecting that giving access to standards in accordance with constitutional requirements will result in loss of copyright, will demand a new 'European approach'.

---

23 Directive 2001/95/EC of 3 December 2001, OJ No L 11 of 15.01.2002.

24 Directive 98/37/EC of 22.06.98, OJ n° L 207 of 23.07.98, p.1.

References

Brodoff 2005
M. Brodoff, 'From A to Veeck. Standardization and the law', presentation at the 2005 ANSI Annual Conference, 2005.

Cunningham 2005
L.A. Cunningham, *Private standards in public law: copyright, lawmaking and the case of accounting*, Boston College Law School, Legal studies, research paper No. 60, March 2, 2005 (http://ssrn.com/abstract=677647).

Elferink 1998
M.H. Elferink, *Verwijzingen in wetgeving. Over de publiekrechtelijke en auteursrechtelijke status van normalisatienormen*, Kluwer, 1998.

Elferink 2007
M. Elferink, 'Auteursrecht op normalisatienormen *revisited*', in: D.J.G. Visser en D.W.F. Verkade (red.), *Een eigen oorspronkelijk karakter*, Amsterdam, 2007, p. 83.

Schepel & Falke 2000
H. Schepel and J. Falke, *Legal aspects of standardisation in the Member States of the EC and EFTA, Vol. 1, Comparative report*, Luxemburg, 2000, p. 164-165.

Stuurman 1995
C. Stuurman, *Technische normen en het recht*, Kluwer, 1995.

In de boekenreeks van de Graduate School of Legal Studies van de Faculteit der Rechtsgeleerdheid, Universiteit Leiden, zijn in 2009 en 2010 verschenen:

MI-156 N.M. Dane, *Overheidsaansprakelijkheid voor schade bij legitiem strafvorderlijk handelen*, (diss. Leiden), Tilburg: Celsus juridische uitgeverij 2009, ISBN 978 90 8863 034 7
MI-157 G.J.M. Verburg, *Vaststelling van smartengeld*, (diss. Leiden) Deventer: Kluwer 2009
MI-158 J. Huang, *Aviation Safety and ICAO*, (diss. Leiden) 2009 ISBN-13 978 90 4113 115 7
MI-159 J.L.M. Gribnau, A.O. Lubbers & H. Vording (red.), *Terugkoppeling in het belastingrecht*, Amersfoort: Sdu Uitgevers 2008, ISBN 978 90 6476 326 7
MI-160 J.L.M. Gribnau, *Soevereiniteit en legitimiteit: grenzen aan (fiscale) regelgeving*, (oratie Leiden), Sdu Uitgevers 2009, ISBN 978 90 6476 325 0
MI-161 S.J. Schaafsma, *Intellectuele eigendom in het conflictenrecht. De verborgen conflictregel in het beginsel van nationale behandeling* (diss. Leiden), Deventer: Kluwer 2009, ISBN 978 90 13 06593 0
MI-162 P. van Schijndel, *Identiteitsdiefstal*, Leiden: Jongbloed 2009
MI-163 W.B. van Bockel, *The ne bis in idem principle in EU law*, (diss. Leiden), Amsterdam: Ipskamp 2009, ISBN 978 90 90 24382 5
MI-164 J. Cartwright, *The English Law of Contract: Time for Review?*, (oratie Leiden), Leiden 2009.
MI-165 W.I. Koelewijn, *Privacy en politiegegevens. Over geautomatiseerde normatieve informatie-uitwisseling*, (diss. Leiden), Leiden: Leiden University Press 2009, ISBN 9 789087 280703
MI-166 S.R.M.C. Guèvremont, *Vers un traitement équitable des étrangers extracommunautaires en séjour régulier. Examen des directives sur le regroupement familial et sur les résidents de longue durée*, (diss. Leiden), Zutphen: Wöhrmann Printing Service 2009, ISBN 978 90 8570 419 5
MI-167 A.G. Castermans, I.S.J. Houben, K.J.O. Jansen, P. Memelink & J.H. Nieuwenhuis (red.), *Het zwijgen van de Hoge Raad*, Deventer: Kluwer 2009, ISBN 978 90 13 07029 3
MI-168 P.M. Schuyt, *Verantwoorde straftoemeting*, (diss. Nijmegen), Deventer: Kluwer 2009, ISBN 978 90 1307 156 6
MI-169 P.P.J. van der Meij, *De driehoeksverhouding in het strafrechtelijk vooronderzoek*, (diss. Leiden), Deventer: Kluwer 2010, ISBN 978 90 1407 158 0
MI-170 M.V. Polak (red.), *Inbedding van Europese procesrechtelijke normen in de Nederlandse rechtsorde*, Nijmegen: Ars Aequi Libri 2010, ISBN 978 90 6916 714 5
MI-171 E. Koops, *Vormen van subsidiariteit. Een historisch-comparistische studie naar het subsidiariteitsbeginsel bij pand, hypotheek en borgtocht*, (diss. Leiden), Den Haag: Boom Juridische uitgevers 2010, ISBN 978 90 8974-259-9
MI-172 H.H. Kielman, *Politiële gegevensverwerking. Naar een effectieve waarborging*, (diss. Leiden 2010). ISBN 978 90 8570 503 1
MI-173 K. Siewicz, *Towards an Improved regulatory Framework of Free Software. Protecting user freedoms in a world of software communities and eGovernments*, (diss. Leiden 2010).
MI-174 Laurens Mommers, Hans Franken, Jaap van den Herik, Franke van der Klaauw, Gerrit-Jan Zwenne (red.) *Het binnenste buiten.* (Liber amicorum prof. mr. A.H.J. Schmidt Leiden). Leiden: eLaw@leiden 2010.

Zie voor de volledige lijst van publicaties: www.law.leidenuniv.nl/onderzoek