25th IVR World Congress
LAW SCIENCE AND TECHNOLOGY
Frankfurt am Main
15–20 August 2011

Paper Series

No. 080 / 2012
Series C
Bioethics / Medicine / Technology / Environment

Munenori Kitahara

The Fusion of Law and Information Technology

URN: urn:nbn:de:hebis:30:3-249389

Conference Organizers:
Professor Dr. Dr. h.c. Ulfrid Neumann, Goethe University, Frankfurt/Main
Professor Dr. Klaus Günther, Goethe University, Frankfurt/Main; Speaker of the Cluster of Excellence "The Formation of Normative Orders"
Professor Dr. Lorenz Schulz M.A., Goethe University, Frankfurt/Main

Edited by:
Goethe University Frankfurt am Main
Department of Law
Grüneburgplatz 1
60629 Frankfurt am Main
Tel.: [+49] (0)69 - 798 34341
Fax: [+49] (0)69 - 798 34523

Munenori Kitahara, Hiroshima / Japan

The Fusion of Law and Information Technology

Abstract: In information society, legal norm communications have been never established in certain fields for a long time. That is, a few legal norms have never obeyed in the fields. Above all, legal norms which relate to data protection, information contents and information security, would often infringed. Most violation would be conducted by using information technologies. Information technologies would often be used in these infringing incidents. It can be said that these infringing incidents would have never been conducted without information technology. These infringing incidents include hacking actions, personal data abuse, personal information disclosure, unauthorized access, infringing copyrights, infringing privacy rights, and so on. A way of preventing those infringements is to raise the level of punishment against the violators. But, it will prove to be disappointing. Furthermore, it would be an ex post facto measure to the last. It would be needed to invent an ex ante measure, if it is possible. As the ex ante measure, the author proposes a fusion of law and information technology. An information technology will lead people to a lawful deed when they conduct actions in using computers and networks. They say that information technology cures information technology. After all, the fusion will aim at realizing laws, and it will contribute to recover a social justice.

Key Words: Fusion, Law, Information Technology, Information Ethics, IT Audit, Cloud Computing, Information Filtering, Encryption Technology, Social Justice

I. Introduction

A few years ago, I tried to make up the system of the information society law in Japan[1]. The system is composed of twelve legal groups (laws) and fifty two acts. The information society law will form and run an advanced information and communications network society of 21st century. The laws would regulate information (contents), information processing devices (computers), and information circulation routes (networks). In the society people live most of their information lives. They receive online administrative, financial, educational, commercial services on the Internet, or the Cloud. On the other hand, they might meet across information accidents (computer crimes, cyber crimes): data protection right infringement; personal information abuse; privacy infringement; spoofing

[1] See, M.Kitahara, Information Society Law in Japan, in: *US-CHINA LAW REVIEW* Vol.8, No.1, 2011, 21-40.

identity; tampering with data; repudiation; information disclosure; denial of service; elevation of privilege and so on.

Information accidents would mostly performed by using information technologies. They say that a computer virus is a kind of computer program. Computer misuse is the collective term for a number of criminal offences committed by means of a computer, often through access to the internet[2]. The offences under a computer law are relevant to crimes involving the use of computers. Such offences can generally be distinguished into three categories. The first category is traditional type of criminal offence that may be committed using computers as the instrument of the crime. The second category concerns 'content-related crimes', where computers and networks are the instrument, but the content itself is illegal, such as infringing intellectual property and certain forms of pornography. The third category is offences that have been established to specifically address activities that attack the integrity, confidentiality, and availability of computer and communications systems, such as viruses and other malware[3].

In a part of the information society, legal norm communications would have not become established. The legal norms as information have had no effectiveness. In most violations of laws they have abused information technologies. There are no other ways than we defeat the opponents with the same information technologies. The information society law should introduce information technologies in order to recover the effectiveness of the law itself. This means that information technologies should control themselves in the law. They say that information technology cures information technology.

This paper has two main goals. The first one is to show the examples of the fusion of law and information technology in existing acts. The second one is to suggest the possibility of the fusions.

In this paper, I will first deal with the reflection of computer system to social systems (II). We can find some ethical technologies in the information technologies which will let us practice ethical deed (III). In the next section, I will show the fusions of law and information technologies (IV). Last, I will be able to present the security standard and architecture standard of information technologies (V).

[2] Andrew Murray, *Information Technology Law: The Law and Society*, Oxford Univ. Press 2010, 327.
[3] See, C.Reed/J.Angel(eds.), Computer Law, 6th ed., Oxford 2007, 553-554.

II. The Features of Information Society Law

1. The Reflection of Computer System to Social Systems

At the beginning of 1990s, many business entities were obliged to take a second look at the information-oriented investment with the change of economic conditions. In this age, there occurred a tendency which even should be known as a new computer idea. The concept of computer system had made a radical change. The new concept was composed of four ideas: down-sizing; open system; distributed computing; networking; end-user computing.

Most organizations had not become to maintain the information processing section. . Therefore, it stopped adopting the personnel of the computer system and information-related sections. Because the main frame computers were changed into the small-sized computers, the special computer engineers became unnecessary for the business entities. The maintenance cost was the largest practical reason. But, even the small-sized computers could make much larger performance than the large-sized computers with the progress of computer technology and software technology. Simultaneously, normal office workers, who were not specialists with high-level knowledge and technology, could operate the computers sufficiently with favor of software technology. This is the idea of end-user computing. Everyone of organization, even if he is an amateur of computer, could operate the small-sized computers, after learning the fundamental knowledge and technology . The new idea was necessary in order for organizations to survive.

In the age of the large-sized and wide-used machine, just the large machine which is called the mainframe had information processing function. In other words, the processor and the storage unit were installed in just the central host computer, around which the small-sized computers that were called a terminal emulator were installed. Just the keyboard and the monitor were installed in the terminal emulators, which were connected mutually with network.

2. Information Technology Controlled with the Information Technology

The infrastructures of information society are “information,” “information processing devices,” and “information circulation routes.” Software and contents technologies will relate to the information. Computer and machine technologies will relates to the devices. Networking and internet technologies will relate to the routes.

The information society law should introduce the information technologies in order to raise the effectiveness of the law itself. This introduction might be permitted only to

the information society law. For example, electronic signatures acts introduce cryptographic techniques in order to make it possible for anyone to make easy use of strict certification functions using electronic certificates and to enable the safe supply and use of network services. An unauthorized computer access prevention act uses a firewall technology, which implements information security policies. And minor protection acts would oblige providers to apply a filtering or blocking technology to child pornography information on the Internet. This means that information technologies should control themselves in the law. It is really the fusion of technology and law.

III. IP Technology and Ethical Deed

1. Ethical Technology

The Internet is the only sphere that establishes ethics in itself by its own technology. A firewall router uses access control lists (ACL) and other methods to ensure the security of the private network. PAP (Password Authentication Protocol) that allows PPP peers to authenticate one another, does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PGP (Pretty Good Privacy) allows secure files and message exchanges. L. Lessig said that code is law[4]. I would say that code is ethics.

2. Ethical Deed and IP Technology

An end-user has nothing to do with the unlawful computer access and the computer virus. As the ethical deed, there is no way for the user other than constructing the firewall to the host computer or installing an anti-virus software. It is not possible to hope any more. If it is a timid user, it is already wax without becoming nature as for the Internet. However, the IP technology is offering a new technology. That is a quarantine network system. This system serves a severe authentication, and protects the user from the threat of unlawful computer access, virus and worms. People use the same password on different systems. People are going to rely less and less on passwords. So, a new password system is being developed.

Network administrators must be able to deny unwanted access to a network and allow authorized users to access necessary services. Security tools such as passwords, callback equipment, and physical security devices are helpful. However, they often lack

[4] Lawrence Lessig, *Code (Version2.0)*, Basic Books 2006, 5.

the flexibility of basic traffic filters and the specific controls that most administrators prefer. For example, a network administrator may want to allow users access to the Internet, but not permit external users Telnet access into the LAN.

Routers provide the capability to the filter traffic, such as blocking Internet traffic, with access control lists (ACLs). An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols. This module will introduce standard and extended ACLs as a way to control network traffic and explain how they are used as part of a security.

ACL technology can refuse the access from the networks and hosts which the sites think of undesirable. With the technology, the sites should limit the access right. Moreover, the sites could deny many processes (commands)—ping, telnet, http, ftp, and so on.

ACLs are also used in firewall routers. A firewall is an architectural structure that exists between the user and the outside world to protect the internal network from intruders. In most circumstances, intruders come from the global Internet and the thousands of remote networks that it interconnects. Typically, a network firewall consists of several different machines that work together to prevent unwanted and illegal access.

3. Difficulty of the Ethical Technology

These new technologies become the assistance of user's ethical deed. Or, it is the one that becomes taking the place of an ethical deed. It is in the relation of the trade-off with the perfection of the technology and the ethical deed. That is, the higher the standard of perfection in the technology becomes, the lower the level of an ethical deed might become.

I don’t think that the Internet users could install these technologies to their own PC by themselves. It, however, is desirable that these technologies should be pre-installed into the PCs. Or, these technologies should be provided in the way how end-users could use in the PCs. But, they need some knowledge of the technologies.

Therefore, all the Internet users require some understanding of ICT in compliance with information ethics. All users must consider the information ethics to access Internet with freedom.

IV. The Fusion of Law and Technology

1. eMail Technology and Law

An email technology has been introduced into the Electronic Consumer Contracts Act. The article 2 (definitions) defines the electronic consumer contracts as follows:

"In this Act, an 'electronic consumer contract' means a contract that is made between a consumer and a business entity by electromagnetic method through a visual browser of a computer in cases where the consumer manifests his/her intention to make an offer or to accept the offer by transmitting his/her intention through his/her computer in accordance with the procedures prepared on this visual browser by the business entity or its designee."(1)

"In this Act, 'electromagnetic method' means a method using electronic information processing system or other types of information communication technology."(3)

"In this Act, 'electronic acceptance notice' means an acceptance notice to the offer of a contract which is, among electromagnetic methods, given by means of transmission through a telecommunication line connecting a computer, etc. (meaning a computer, a facsimile device, a telex or a telephone, the same shall apply hereinafter) used by the party dispatching the acceptance notice to the offer of the contract with a computer, etc. used by the offer or of the said contract."(4)

The email technology uses SMTP (Simple Mail Transfer Protocol) and POP (Post Office Protocol) in TCP/IP.

2. Encryption Technology and Law

The Electronic Signatures and Certification Business Act has introduced encryption technologies[1]. The purpose of this Act is to provide the presumption of authentic establishment of electromagnetic records by electronic signatures. In the Act, any electromagnetic record that is made in order to express information shall be presumed to be established authentically if the electronic signature is performed by the principal with respect to information recorded in such electromagnetic record. The authenticity and electronic signature of the electromagnetic record can be verified by the public key cryptosystem.

Japanese electronic signatures act (Act on Electronic Signatures and Certification Business) has the following provisions:

Article 1 (Purpose)

The purpose of this Act is to promote the distribution of information by electromagnetic forms and information processing through ensuring the smooth

utilization of Electronic Signatures, and thereby to contribute to the improvement of the citizens' quality of life and the sound development of the national economy, by providing the presumption of authentic establishment of electromagnetic records, the accreditation system for designated certification businesses and other necessary matters, with respect to Electronic Signatures.

Article 2 (Definitions)

(1) The term "Electronic Signature" as used in this Act means a measure taken with respect to information that can be recorded in an electromagnetic record (a record that is prepared by an electronic form, a magnetic form or any other form not perceivable by human senses and that is used for information processing by computers; hereinafter the same shall apply in this Act), and which falls under both of the following requirements:

(i) A measure to indicate that such information was created by the person who has taken such measure; and

(ii) A measure to confirm whether such information has been altered.

(2) The term "Certification Business" as used in this Act means a service that, in response to either the request of any person who uses the business (hereinafter referred to as the "User") with respect to the Electronic Signature that he/she himself/herself performs or the request of another person, certifies that an item used to confirm that such User performed the Electronic Signature pertains to such User.

(3) The term "Specified Certification Business" as used in this Act means a Certification Business that, among Electronic Signatures, is performed with respect to an Electronic Signature that conforms to the criteria prescribed by ordinance of the competent minister as an Electronic Signature that can be performed by that person in response to the method thereof.

But, in these provisions, we can find no provisions to introduce an encryption technology into the act. The hint can be found in the ordinance for enforcement of the act (art. 2). That is, there is provided of the security of electronic signatures and the difficulty of electromagnetic records. In addition, the difficulty shall be depended upon the factorization in prime numbers of integer, and the calculation of discrete logarithm.

These hints suggest that we are forced to use an encryption technology in order to establish and send electromagnetic records.

3. Filtering Technology and Law

In the Act Concerning Environment for Children to Safely Use the Internet, information providers shall be obliged to provide filtering technologies. This Act focuses on measures to protect minors from harmful information and explicitly provides for the direction of future efforts with respect to a vision of the environment for the Internet utilization.

4. Internet Technology and Law

The Internet is the only sphere that establishes a lawful action in itself by its own technology. A firewall router uses access control lists (ACL) and other methods to ensure the security of the private network. PAP (Password Authentication Protocol) that allows PPP peers to authenticate one another, does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PGP (Pretty Good Privacy) allows secure files and message exchanges.

5. Data Audit Technology and Law

By implementing a data audit technology, a data controller can grasp a lifetime of personal data, which will contribute to the effectiveness of a data protection act. It might be possible to grasp a personal data flow by attaching a logical IC tag to the personal data. The logical IC tag will play the same role as the header of an IP packet.

6. Email Filtering Technology and Law

SaaS for email primarily involves cleaning spam, phishing emails, and malware included in email from an organization's incoming email stream, and then delivering that clean email security to the organization so that it is effectively not repolluted[5].

This is accomplished by using either Secure Socket Layer (SSL) or Transport Layer Security (TLS) on network communications at the transport layer[6].

7. Web Content Filtering Technology and Law

In the Cloud, a SaaS provider scans for malware threats and ensures that only clean traffic is delivered to end users. SaaS providers supplement that URL filtering with the examination of HTTP header information, page content, and embedded links to better

[5] Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'REILLY 2009, 220.
[6] Ibid.

understand site content. SaaS for web content also involves scanning outbound web traffic for sensitive information (e.g., ID numbers, credit card information, intellectual property) that users could send externally without appropriate authorization (data leakage protection). Web traffic is also scanned for content analysis, file type, and pattern matching to prevent data exfiltration[7].

V. The Security and Architecture Standard of Information Technology

1. The Security Standard of ICTs

Biometric systems are increasingly being considered as better fool-proof methods of ensuring security in several areas ranging from national security to credit card processing, as opposed to traditional methods such as alphanumeric passwords and personal identification numbers[8].

The Biometric Consortium is to develop widely acceptable standards for the application level and device level interfaces that are independent of the operating systems and vendors, and to be able to support a variety of biometric applications. Due to the sensitivity of information contained in biometric systems, it is expected that such systems will be attacked by intruders both from within and outside the country[9].

2. The Architecture Standard of ICTs

Assurance and security mechanisms need to be provided for the information stored in the biometric systems both in stored and transit modes. It is important to understand the design principles underlying the architecture and management of biometric systems so that appropriate mechanisms can be used to secure such systems.

In order to maximize the level of security provided buy biometric systems, multimodal systems are being considered as better alternatives to relying on a single biometric for identification and verification purposes. Multimodal biometric systems utilize multiple signatures of the same individuals obtained from different sensors. Information (signatures) obtained from multiple sensors can be fused together to improve the performance of identification and verification systems and compensate for lack of sufficient features from the signature obtained from a single sensor. Information fusion

---

[7] See, Yaman Akdeniz/Clive Walker, Whisper Who dares: encryption, privacy rights and the new world disorder, in: Y. Akadeniz et al.(eds.),*The internet, Law and Society*, Longman 2000, ff. 317.
[8] Tim Mather/Subra Kumaraswamy/Shahed Latif, ibid., 221.
[9] M.E.Whitman/H.J.Mattord, *Reading and Cases in the Management of Information Security,* Course Technology 2006, 63.

can take place while extracting features, while matching the scores obtained from different modalities, or while making decisions. Results obtained from information fusion suggest that the reliability of biometric systems can be significantly improved by combining two or more biometric signatures[10].

VI. Conclusions

This paper aimed at introducing information technology into laws. That is to say, laws might use information technologies for the legal systems to become effective. I would try make up a cooperation between law and information technology.

There might be certainly various problems about the fusion, however. First, technologies will regulate technologies. Second, the collaboration will force the users to use specific computer systems with the information technologies implemented. Third, the fusion will have to cope with the evolution of technologies. Last, there will be left the problem of standardizing the technologies.

Information society, increasingly, depends on computer systems to behave acceptably in applications with extremely critical requirements, by which she means that the failure of systems to meet their requirements may result in serious consequences.

There is good news and there is bad news. The good news is that computer system technology is advancing. Given well-defined and reasonably modest requirements, talented and diligent people, enlightened and altruistic management, adequate financial and physical resources can be built that are likely to satisfy certain stringent requirements most of the time. The bad news is that guaranteed system behavior is impossible to achieve. There can always be circumstances beyond anyone's control. Besides, people are fallible. Thus, there are always inherent risks in relying on computer systems operating under critical requirements[11].

The technology's ultimate social and personal consequences will be determined in large measures by how the tension between the two sides off itsnature—liberating and controlling—comes to be resolved[12].

The law must evolve to reflect how both society and technology evolve, for the truth is that neither the tech-deterministic school nor the socially-mediated school are

[10] Ibid., 64.
[11] P.G.Neumann, *Computer Related Risks,* Acm Press 1995, 4.
[12] Ibid.

completely correct. The information society is rooted in connections between people enabled by, and mediated by, digital technology[13].

Address:
Munenori Kitahara
Faculty of Economic Sciences, Hiroshima Shudo University
1-1-1 Ozuka-Higashi 1-chome, Asaminami-ku, Hiroshima, JAPAN 731-3195

[13] Andrew Murray, ibid., 574.