

AHTI SAARENPÄÄ
Institute for Law and informatics
Faculty of law
University of Lapland
Finland
asaarenp@ulapland.fi

Stockholm 18.11.2008

THE IMPORTANCE OF INFORMATION SECURITY IN SAFEGUARDING HUMAN AND FUNDAMENTAL RIGHTS

1. Law, society and state

Law is necessarily a dynamic force in society: Legal principles, the legal culture and legislation all change regularly. Ultimately, the practice of the law courts changes as well.

When society changes, legislation is often the first of the above elements to react – sometimes even a bit too readily. For the most part, it is enough to interpret old

legislation in a new way in a new environment. This works better in the realm of civil law than in the case of criminal law.

In this light, it comes as no surprise that the Finnish Supreme Court has recently – after a vote – deemed that, pursuant to the principle of legality, sending text messages does not constitute a disturbance of domestic privacy. After consulting relevant drafting work and considering the impact of telephone calls and text messages, the Court determined that calls and messages have different statuses. The law must be changed here. It is no longer in keeping with the times.¹

Recognising and acting on the need for a wholly new body of legislation involves rather more effort. We are even slower to notice changes in legal principles and slower still to detect changes in our legal culture. The philosophy of knowledge teaches us that *knowledge resides in structures* and that structures change slowly. The legal culture in its different forms is no doubt a premier example of this maxim.²

On balance, law is at once a dynamic and a conservative phenomenon. The legal profession counts amount the most conservative. Legal life is dominated by routines. And conservative legalism is naturally the basic attitude of the legal profession and the independent judiciary towards the arbitrary application of political and other forms of power.

Change in a society and change in a state are different matters. This is yet another distinction we fail to appreciate. The state is usually the slower of the two to change. The development of society and the state may differ markedly

¹ This decision (KKO:2008:86) can also be criticised with good reason. It observes the principle of legality in an extreme fashion by combining the positions presented when the bill was heard before Parliament and, on the other hand, playing down the importance of the tone signalling the arrival of text messages.

² Here I view the legal culture as a crucial factor affecting the professional skills of the lawyer. The key components of the culture, as Swedish legal historian *Kjell Åke Modéer* has observed, are the leading legal principles, the content of the Constitution, the quality of legislation, the ways in which disputes are resolved and the infrastructures available to lawyers. I would add to this list – as an equally essential element – the lawyer's conception of society.

from one another. States rarely change; societies do so more often. We can see both types of change in the world around us today.

2. The constitutional state and the Network Society

In the Nordic countries today we speak of the modern *European constitutional state*. It is an old concept that has taken on new vitality with the conclusion of human rights treaties and the establishment of the European Union.³ The point of departure in any case is the individual and his or her right to self-determination.⁴ The rights of the individual in different life situations are protected much earlier and more vigorously than before.

The information superhighway is a metaphor familiar from the Information Society. Information networks have become the new information superhighway. The same image is more than applicable in describing the constitutional state. We are fully justified in speaking of a *legal superhighway* that should provide the most direct route from human and fundamental rights to the interpretation of individual provisions in the law.

On this highway, different appellate remedies and a fair trial play minor roles and are most often “too little too late”. The distinguishing features of the constitutional state have changed. The depth of sources in law has become more important than earlier⁵. This development has rarely if ever been given due attention in legal education, despite the fact that law has traditionally been one of the planning sciences.⁶

³ It was rare in Finland to hear any mention of the constitutional state before the country joined the *Council of Europe*. The silence on this issue had everything to do with foreign policy. However, we did speak a great deal about the legal civilised state in largely the same meaning.

⁴ The importance of the European Personal Data Directive cannot be overstated in this connection. Among other things, it made *the law of personality* part of the core of regulation in the EU. The rights of the individual figure more prominently than before.

⁵ On the level of legal provisions, this has been acknowledged by the Constitution giving courts the right to assess the constitutionality of an applicable provision in a particular case. In contrast, there is no separate constitutional court in Finland and the constitutionality of legal provisions cannot be tested in a court independently of ongoing proceedings.

⁶ In this perspective, talk of *proactive law* is rather misleading. Law and legal science are by nature proactive. Legal science that focuses on monitoring legal practice is thus skewed to a certain extent.

The society that we live in today is no longer an information society but a *Network society*. We work in a digital environment that uses information networks. Services, the market, information and communication are increasingly tied to networks. Whereas the Information Society was a society just getting its sea legs where the potential of IT and network communications were concerned, the Network Society binds individuals, communities, government and different professions to a digital environment.

We participate in society through networks. Where the individual is concerned, we can speak of a right to use information networks, data processing equipment and information tools. Correspondingly, government must take responsibility for providing a functional information infrastructure. The essential link between e-government and the legal Network Society is graphically and impressively reflected in a Finnish court decision handed down in 2006. The issue was the right of a disabled person to receive screen magnifier and voice synthesiser software from the municipality as social assistance in order to be able to use information networks.

The Supreme Administrative Court set out the grounds for its affirmative judgement (KHO:2006:18) in the following terms: “In light of the fact that public and private services are becoming increasingly and primarily network based, A’s request for assistive devices does not constitute support for a hobby but, rather, will enable him/her to function socially, to live independently and to cope in his/her daily routine.” Here, the Court was very much abreast of the times.

The crucial components of a lawyer’s professional skills today are *legal information literacy* and knowledge of *the legal requirements and the impacts associated with processing information*. The marks of a skilled lawyer have changed accordingly. Lawyers are the computer operators of legal life.

Where information-processing skills are concerned, we have customarily operated with the concepts of publicity, confidentiality and the obligation to maintain confidentiality. What we have seen emerge more recently alongside these as essential additions to the lawyer's tools are *copyright*, *data protection* and *information security*. A good lawyer simply cannot come to grips with the digital environment without a sound knowledge of how these three processes work.

Needless to say, there are still those who try to get by without the requisite skills. The Finnish Data Protection Ombudsman *Reijo Aarnio* has aptly spoken of a deficit of expertise in these areas. I agree with him on this issue.

3. Information security

In embarking on a closer look at information security, it is first essential that we connect the development of *society* and of the *state*. The society we live in today is a network society; the state we call home is a constitutional state. Where attention is trained exclusively on the changes in IT in society, law is in danger of becoming a lower-level – if still well selling – planning technique. Only a deeper-going assessment of changes in a state and society can fulfil the criteria for good science.

This new interaction of state and society changes law significantly: One can see legislation, legal principles and the legal culture all changing. The meeting of old and new is conspicuous.

If nothing else, our world of legal concepts is being rapidly reshaped. Much of what we do we now do on networks – in new ways, using new concepts and, to some extent, applying new principles. It is directives in particular that constantly

introduce new concepts, ones that are essential in practice. The conceptual world of the lawyer has changed substantially.⁷

One of the new basic legal concepts is *information security*. It is an addition to the “family” of securities, one that has even prompted a reaction or two among lawyers.⁸

In Finnish legislation information security has even been defined: “Information security means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data systems can be used by those who are entitled to use them”. This definition in the Act on the Protection of Privacy in Electronic Communications falls short of the mark. It lacks one essential element – *law*. The legislators have forgotten themselves.

The Network Society compels us to reflect on the legal significance of information security in a new way. On the technical end, we have been slow to wake up to the realities of information security and the need to study it closely. Where its legal ramifications are concerned, we have been even slower; the legal significance of information security has not received much attention.⁹

One sees the term “information security” used but the attempts to assess its meaning in detail have been few and slow. On the European policy level, we have even gone so far as to think that *best practices* would suffice. This is not the right way ahead in a constitutional state. A crucial segment of the functions of

⁷ In all, lawyers have had to add more than 150 new terms to their toolbox since the Personal Data Directive was adopted. The magnitude of this deluge can be explained in part by the way in which modern directives define the terms they use. The legislator generates terms; previously, this was largely the task and province of legal science. In other words, the life course of terms has changed.

⁸ The legal literature also uses the term ‘*data security*’, typically with the same meaning as ‘information security’.

⁹ In Finland, information in the public sector is primarily regulated by good practice in information management as laid down in the *Act on the Openness of Government Activities*. It requires that government information systems be designed to be secure. Section 18 of the Act describes information security in general and is provided in the Appendix to this article.

the Network Society would be left dependent solely on various practices that lack up-to-date legal frameworks.¹⁰

Let us go on to examine information security in terms of various dimensions of law. This approach is typical of, indeed essential to, the modern constitutional state.

4. The legal dimensions of information security

The logical starting point here is *human and fundamental rights*. Electronic communications, e-commerce and information management – all core processes of the Network Society – require an environment where information is secure. We exercise our fundamental rights to an increasing extent on networks.

The development of *information government* is leading to a situation where public electronic services are more than merely an alternative to manually delivered procedures. This being the case, the channel of communication between the average citizen and officials had best be a secure one.¹¹

Using a service electronically is utterly different than using a service manually. The path a citizen takes to reach a government official is not, at least not wholly, the responsibility of that official. Yet, viewed as information processes, services provided by the government begin as soon as an individual contacts or tries to contact a government official.

¹⁰ In legal perspective, best practices are a peculiar approach, as they lack a direct link to the relevant legislation and generally lack a connection to the relevant standards as well. It is a different matter again that EU security policy and the related decision to continue the work of ENISA (the European Network and Information Security Agency) provide positive signals that we are waking up to the importance of information security.

¹¹ Like *Victor Mayer Schönberger*, I use the expression ‘information management’ to refer to a state of public administration – one more sophisticated than the earlier e-government – in which we embrace the use of interactive information processes implemented on networks.

Yet, we should not embrace the view that only information government has an information security dimension. As a new element in the information infrastructure, information networks necessarily prompt the fundamental question of how and to what extent legislation on different infrastructures should be enacted. This seems to be forgotten in discussions of benefits, drawbacks and censorship. When it comes to legislation, we have thus far lacked a uniform approach to information networks as an *infrastructure*. We have acquired nothing less than a new infrastructure intended for the masses. That is a real change in society.

For example, the directives on electronic communication – important as they are where the use of networks is concerned – are mainly a continuation of the earlier telecommunications directives and not really new instruments drafted and adopted for a new infrastructure from the standpoint of citizens' fundamental rights.¹² These rights might best be described, using a term familiar from the work of *Mario Losano*, as being caught in a “turbulence of directives”.¹³

Information security for the new infrastructure is thus a significant issue in the realm of fundamental rights: *We should have access to a secure information superhighway*. Yet this is but one, albeit important, component of legal information security. We must take a look at the other aspects of information as well.

An apt metaphor here, like “information superhighway”, is the “path of information”, a term used in research on information. In a digital environment, even the platform to which information is attached and how it is attached have a significant bearing on our rights. And we confront interesting legal issues throughout the lifespan of information, including its being archived and

¹² There has been no general consideration of enacting legislation on infrastructures in the ongoing updating of these directives either.

¹³ Mario Losano's article “Turbulenzen im Rechtssystem der modernen Gesellschaft - Pyramide, Stufenbau und Netzwerkcharakter der Rechtsordnung als ordnungsstiftende Modelle” (Rechtstheorie1/2007) is one of the seminal assessments to appear in recent years of the change in law. The article is based a presentation given by Losano when he received an honorary doctorate from Hannover University.

destroyed. This issue is not a new one as such, but it takes on a heightened importance in the constitutional state and the digital environment in which we must work today.¹⁴

A telling case of the importance of the path of information and information security is *I v. Finland*, heard before the European Court of Human Rights.¹⁵ The decision, handed down in 2008, involves a situation in which hospital staff had noticed from patient records that a member of staff had contracted HIV. When the word spread, the person was ostracised and was ultimately forced to resign.

The case was brought before the ECtHR because the domestic courts had rejected claims for damages, the grounds being that it could not be shown which person or persons on the staff had used the patient records inappropriately. The courts were looking for a single party responsible for the wrongdoing without considering the information system and how it had been maintained.

The incident occurred in the early 1990s. The relevant legislation in force at the time was the Personal Data File Act. In keeping with the Council of Europe's Data Protection Convention and the OECD's data protection guidelines, the Act obligated the controller of a personal data file to ensure information security. In the focal case, the event logs did not show who had used the system and thus that obligation had not been met. In other words, at the end of the day, Finland had failed in its obligation to maintain information security.

The decision of the ECtHR is a clear demonstration of the importance of information security as a human right. It also sends a message telling us how we should read the Personal Data Directive. The right to information security is a right that all citizens enjoy when data concerning them – and not only sensitive data – are being processed. Given that the right to privacy is a fundamental right,

¹⁴ For example, the Ministry of Justice and its subordinate authorities in Finland have begun to use open office software (open source code) in the name of transparency. Without extensive system descriptions, closed source code is ill suited where good government is the aim. The decision was made in 2006.

¹⁵ *I v Finland* [2008] ECHR 20511/03 (17 July 2008).

information security can be seen as a right safeguarding a fundamental right. Information security has changed – or at least is in the process of changing – *from a technical aid to a legal value*. This change is a crucial development.

Moreover, as the matter went to the ECtHR, we can put forward – albeit cautiously – the generalisation that information security is to be seen as a human right for individuals when data concerning them are being processed.¹⁶ The case is also a clear indication that as our society has changed, the ECtHR has become a crucial legal observer of developments in IT and law too.

5. Restrictions on fundamental rights

Whenever we speak about fundamental rights, we must address the issue of the circumstances under which these rights may be curtailed. The context of human and fundamental rights is constantly changing with changes in society and the state. Again, we must recognise that democracy is not static.

One of the most legally charged situations today where fundamental rights are concerned is data protection in working life. In most countries personal data in working life and thus information security are governed by general legislation on data protection. Finland is a noteworthy exception: we have a special law on privacy – not only data protection - in working life.¹⁷

The act regulates the testing and technical surveillance of employees as well as monitoring of their email. The point of departure is that an employee is entitled to a measure of privacy in the workplace, as elsewhere. What was an extensive right of control for the employer has become respect for the privacy of the

¹⁶ It should be pointed out that the date of the original infringement does not render the decision any less important. It in fact shows that we have long been in the situation noted by the ECtHR. In practice, such abuses of information systems are commonplace.

¹⁷ See closer *Saarenpää* The right to be left alone in the workplace. Tensions between rights and obligations pp 261-278 in *Saarenpää* (ed) *Legal Privacy* (2008).

employee. For example, an email received or sent by an employee may be traced and opened only when he or she is absent and the message is essential to the company's operations. An additional requirement here is that the company's email system must allow for messages to be rerouted when an employee is not in the workplace.

Email is of course only one form of communication. Every bit as important as the content of a single email message is the information on the size of messages and their recipients. The Act on the Protection of Privacy in Working Life does not permit monitoring of these details.

When examining the path of information in the workplace, one must remain mindful of the fact that email is only one of the information systems there. Event logs, for example, figure significantly as sources of surveillance information.¹⁸ The use of such logs for this purpose is not permitted in Finland. The scope of the *Act on the Protection of Privacy in Electronic Communications* extends to event logs.

The legislation is to be amended in the autumn of 2008, however, to allow the monitoring of log data where an employee is suspected of industrial espionage. The impetus for the amendment is a single case of espionage in a prominent company. In a review, a majority of experts in the Parliament's Constitutional Law Committee opposed the amendment but when economics and law are pitted against one another, the former tends to prevail, and that proved to be the case here as well.¹⁹ At this writing the fate of the bill is still undecided.

¹⁸ For example, a study carried out in Sweden in 2003 demonstrated that event logs were used to a significant extent to monitor employees' activities.

¹⁹ The Committee heard eight legal experts, of whom only one supported the proposed amendment, and even then with reservations. I was among the experts who opposed it. My statement ended with the following words: "It must also be pointed out that modern IT offers effective information security solutions for managing trade secrets. The requirement that a restriction of fundamental rights should be essential is thus not, in my view, met in the present case. Poor business management that overlooks opportunities to use sophisticated forms information security should not be an adequate reason for restricting the fundamental rights of individuals in working life".

It is interesting that the Constitutional Law Committee classified the identifying information used in email communications as information falling outside the core of fundamental rights. This view plainly clashes with the broad conception of personal data.

6. Towards more sophisticated legal information security

In the realm of professional expertise, an understanding of information security has been, and continues to be a no man's land: It has never been recognised as part of the legal culture and responsibility for it has been left to management and IT professionals. For them the issue has until very recently been a new one and one of relatively minor importance.

Law and security have not met in the right way in the development of software and computer systems. In practice information has been viewed as raw material, not as a collection of rights. At the end of the day, the weak link in information systems is the curious operator at the terminal. As *Paavo Haavikko* put it: people often have a strong will but a weak nature.²⁰

In Finland, government is waking up to the significance of information security. For example, the National Audit Office has on many occasions stressed the importance of information security. In a similar vein, the Parliamentary Ombudsman has emphasised the need for a better information security act as part of an overall policy of better regulation.

In spring of 2008, I was asked to evaluate the legal regulation of *basic registers*. In my report, I proposed, among other things, that a general information security law be enacted.

²⁰ This is how Paavo Haavikko, a well-known Finnish writer, described a king in his novel. The expression is a fitting description of the present-day efforts to increase surveillance in society using IT.

Basic registers generally refer to national registers organised in terms of the basic units of society: individuals, communities and property. A significant proportion of the work in both the private and public sectors depends on the use of these registers; they are used to identify, distinguish and evaluate. Alongside traditional registers a range of registers has emerged that contain societally important data, e.g., motor vehicle registrations, taxation, criminal convictions and patient information.²¹ All of these registers have been created without our having a coherent conception of the importance of *basic data stores* and how they should be regulated.

In my report, I proposed that Finland should enact a law on data stores that would govern basic registers as well as a general law on information security. In addition, I suggest legislation introducing restrictions on the use of information tools.²² These three laws would furnish a basis for a new information security culture that would take its place as a part of democracy and the legal culture.

7. Conclusion

A democratic society and constitutional state that rely on information networks can be built only if accompanied by appropriate information security that ensures the smooth functioning and use of the infrastructure and provides legal protection for information throughout its life course.

On balance, we should have a right to information security on a par with our right to other forms of security. We find ourselves in the midst of a change to a new era in knowledge management. The responsibility for data protection and

²¹ Finland is changing over to a national social welfare and patient information archive, to be maintained by the Social Insurance Institution. The relevant act came into force in 2007 and the system is scheduled to be operational in 2011.

²² The question of regulating the use of information tools clearly stems from the expanded storage capacity of various mobile memory devices. For example, a single memory stick can hold most or all of an important register, even a national one.

information security should rest with higher management and not separate IT units. Similarly, data protection should be a standard focus of *internal auditing*.²³

This significant change in the legal culture of the constitutional state unequivocally requires that information security be included among our fundamental rights. It is an element of the essential social contract that underpins the Network Society. The routes that information and legal information follow should run parallel over their full length. Information networks are not solely or primarily a technical consideration where information security is concerned.

Accordingly, in my report I have proposed that information security should be expressly included among the *values protected by the Constitution*. This would alert even those who are not always quick to detect change to the transformation of legal culture that has occurred. This is perhaps a fitting way to conclude a presentation on the importance of information security in the constitutional state.

²³ This is the current direction in Finnish management. In a recent trial, the first of its kind to become public, an employee of the Finnish Tax Administration was sentenced to fines for browsing through tax data at work whose connection to his or her responsibilities was dubious. The incident came to light in an internal audit.

Act on the Openness of Government Activities

Section 18 — *Good practice on information management*

(1) In order to create and realise good practice on information management, the authorities shall see to the appropriate availability, usability, protection, integrity and other matters of quality pertaining to documents and information management systems and, for this purpose, especially:

(1) maintain an index of any matters submitted and taken up for consideration and any matters considered and decided, or otherwise make sure that their public documents can be easily located;

(2) draw up and make available specifications on their information management systems and the public information contained therein, unless granting access to such information would be contrary to the provisions in section 24 or in some other Act;

(3) when the introduction of information management systems or administrative or legislative reforms are being prepared, analyse the effect of the proposed reform on the publicity, secrecy and protection of documents and on the quality of the information contained therein, as well as undertake the necessary measures for the safeguarding of the rights pertaining to the information and its quality, and for the arrangement of the protection of the documents, the information management systems and the information contained therein;

(4) plan and realise their document and information administration and the information management systems and computer systems they maintain in a manner allowing for the effortless realisation of access to the documents and for the appropriate archiving or destruction of the documents, the information management systems and the information contained therein, as well as for the appropriate safeguarding and data security arrangements for the protection, integrity and quality of the documents, the information management systems and the information contained therein, paying due attention to the significance of the information and the uses to which it is to be put, to the risks to the documents and the information management systems and to the costs incurred by the data security arrangements;

(5) see to it that their personnel are adequately informed of the right of access to the documents they deal with and the procedures, data security arrangements and division of tasks relating to the provision of access and the management of information, as well as to the safeguarding of information, documents and information management systems, and that compliance with the provisions, orders and guidelines issued for the realisation of good practice on information management is properly monitored.

(2) More detailed provisions on the measures necessary for the realisation of the obligations provided in paragraph (1) shall be issued by Decree. However, more detailed provisions on the diaries of the courts and prosecutors shall be issued by the Ministry of Justice. Provisions may be issued by Decree on the powers of the Government to issue more detailed orders and guidelines on the technical specifications for data security arrangements and procedures for the safeguarding of information management systems and the information contained therein, ensuring the integrity and quality of the information and the transfer of information by way of data networks, as well as on the classification, within the State administration, of the pertinent documents, information management systems and the information contained therein.

(3) The provisions in the Archives Act (831/1994) and the provisions and orders issued on the basis of that Act apply to the duties of the archive service