ICT and Legal Principles: Sources and Paradigm of Information Law

Tuomas Pöysti

1 The Topic

The development of information and communication technologies (ICT) has led to significant social, economic and consequently legal changes. Technological change has one of its widest impacts on society and everyday life through information and communication technology (ICT). Biotechnology and bio-informatics play an increasing role. Law fulfils its functions in a certain technological environment and is thereby profoundly connected to technology through the construction of social reality and what is just in that reality. Law regulates particular technologies and solves conflicts and co-ordination problems related to those technologies. New technologies have had more powerful impacts on nature and on society and on our individual and organisational inter-relationships with others. This means that there are also new risks, which must be managed. Law is a method of technological risk management and plays a constantly increasing role in that regard. Even the content of normative ethics and morals seems to be impacted by technological change. The Information Age and network society is shaped by the rising significance of information ethics and network ethics which is a new individualist ethical approach to living together and interacting in networks and in the sharing of information.

These changes are about to be deepened and reinforced as our societies develop further towards inter-connected and inter-dependent, ICT–dependent network societies. This development results in increasing complexities and challenges for the regulation and application of law. Legal change linked to information and communication technology has created the need for a new regulatory paradigm, and, a systematic of law, which could govern the new information and communication, markets and provide for conflict resolution and the optimal implementation of fundamental rights and freedoms. The paradigm and systematic of law should also connect law to the new ethics of information processing, information sharing, security and responsibility in the ICT and inter-dependent world.

The paradigm needed for an effective legal and rule of law approach is modern or late-modern information law. Information law is the corpus of general principles regulating information processing, information markets, information infrastructure and communication.[1] Contemporary information law is a dynamic system of legal and ethical knowledge connected to the phenomena around information, information processing and communication. Information law is not only a set of rules systematised under this particular heading but also an

---

1 On the definition of information law, which has contributed to the author's understanding of it, *see*, *e.g.* Saarenpää Ahti, *Oikeusinformatiikka*, in Oikeusjärjestys 2000, ed. by Risto Haavisto, osa I. 2. täydennetty painos, Lapin yliopiston oikeustieteellisiä julkaisuja, Sarja C 31, Lapin yliopistopaino, Rovaniemi 2002, p.1-59. and Seipel, Peter, *Den nya datarätten*, in Lex ferenda. Rättsvetenskapliga studier av forskare vid Stocholms universitet. Ed. Jan Rosén. Juristförlaget. Stocholm 1996, and Dommering, Egbert J., *An Introduction to Information Law, Works of Fact at the Crossroads of Freedom and Protection*, in Dommering Egbert J. & Hugenholtz P. Bert, Protecting Works of Fact, Copyright, Freedom of Expression and Information Law, Information Law Series 1, Kluwer Law and Taxation Publishers, Deventer-Boston 1992.

approach to legal scholarship and information and information systems theory in network society. It is close to a method and it is easily part of legal theory.

This way of viewing information law does not preclude treating the study and systematisation of the general principles of certain information-processing and communication-related acts and rules, which escape the boundaries of the traditional public – private distinction and other systematic frontiers, under the rubric of information law. In this perspective information law is that part of legislation and law which concerns information collection, information processing, and the use of information and communication. In Finnish legal literature Professor *Timo Konstari* has particularly developed information law in the latter sense, as a clear area of positive law with its own general principles under formation. In both cases, information law has its own general principles.[2] *Anna-Riitta Wallin* would prefer this area of law to be called information and communication law because of the significance of communication and since information is used and often acquires its significance in communication. The subject for study in this kind of information and communication law would be the informational and communication relation.[3]

In my understanding the general principles are the foundations of information law and an essential part of its paradigm. The principles of information law are also meta-rights, that is, formulations of positions and factors, which are important in the various fundamental rights and freedoms in the context of a network society. They represent meta- or second-level rights and thus reveal the background, aims and fundamental justifications behind the fundamental rights in the information context and behind the rules of general legislation and of particular statutes with more limited scope of application. By serving as such formulations and communications of the principles of informational justice, they also guide the interpretation of law in hard cases. Information law in this sense and, the principles of information law, cover communication as well. Thus, a systemic body of law can cover both individual and mass communications and their combinations, and overcome the frontiers between different types of media.

The paradigm of information law is a multidisciplinary analysis and understanding of the phenomena surrounding information processing, communication and information and communication markets and surrounding the general principles of information law. The general principles of information law are also the most important second-level rights related to information and communication, that is, messages about rights and systematic perspectives on rights in network society aiming at optimal realisation of fundamental rights and freedoms. The main principles and meta-rights of information law are:

---

2 *See, e.g.* Konstari Timo, *Matkalla kohti eurooppalaista tietosuojaa*, Tietosuoja 4/1997, p.18-22 and Konstari, Timo, *virallisen vastaväittäjän lausunto Tuomas Pöystin väitöskirjasta Tehokkuus, informaatio ja eurooppalainen oikeusalue*, Lakimies 2000, 264-275, which is the official opponent's opinion on Tuomas Pöysti's doctoral dissertation**.** *See* also, Wallin, Anna-Riitta & Konstari, Timo, Julkisuus- ja salassapitolainsäädäntö, Laki viranomaisten toiminnan julkisuudesta ja siihen liittyvät lait, Jyväskylä 2000, p. 32.

3 *See* Wallin, Anna-Riitta, *Yritystoiminnan ja julkishallinnon avoimuus informaatio- ja viestintäoikeudellisesta näkökulmasta*, in Kulla Heikki et. al. (ed), Viestintäoikeus, WSOY Lakitieto, Helsinki 2002, p. 123-146, at 143-146.

1 The right to information and freedom of information;

2 The right to communication and freedom of communication;

3 The right to knowledge and freedom of knowledge;

4 The right to public and private self-determination;

5 The right to privacy;

6 The right to efficiency in the markets and in public administration;

7 The right to information security; and

8 The right to quality and good governance.

I will discuss shortly in this article some of the paradigmatic features and sources of contemporary information law, and, place it in the context of the changes precipitated by on-going technological development. Space constraints do not allow systematic analyses of all these principles so I will focus on the right to information and freedom of information, and the right to information security which are all informative examples and, which, together with the freedom of communication and the right to privacy, establish essential elements of the constitution of information liberty. My aim in this article is also to assess briefly how legal certainty in a material sense is promoted and safeguarded by these principles in a society characterised by rapid technological change and legal change. The principles of information law aim particularly to represent a sustainable, conserving and security-creating element in a legal and technical environment characterised by rapid changes, technical complexities and significant uncertainties.

2 The Right to Information and the Freedom of Information

2.1 Overview of the Freedom of Information

The individual and community second-level (meta-level) right to information is together with the freedom of communication among the constitutive foundations of democracy and of individual and group identity, integrity and the right to self-determination.[4] Information and access to information is needed in order to

4 The significance of freedom of information and the free flow on information is increasingly recognised in the various policy documents. Freedom of information and free flow of information is stated as a fundamental principle of democracy in the OECD Guidelines of information systems and network security, *see* the explanation of democracy–principle, OECD Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security, recommendation of the OECD Council, 25 July 2002. In Finnish social sciences and information management literature, Timo Kuronen has written an excellent analysis of the meaning of informational freedom and freedom of access and utilisation of informational

understand oneself (who am I, where do I come from) and to determine my relationship to others. Access to information serves also the efficiency of markets, the quality of products and services and the quality and efficiency of public administration.[5] The right to information has both an individual and a community dimension; thus, there are collective rights to information belonging to a group of persons, a community, and individual rights to information. Freedom of information and the meta-right to information is a fundamental material principle of information law.[6] It resides in the background of several explicit fundamental rights and freedoms of several institutions of positive law. It is a default position of law and information ethics to information. There are several explicit provisions, which constitute and give support to the all-encompassing principle of law and justice. As a principle of justice it is also a foundation of legislative policy and macro- and micro-level information policy and, it forms the rationale of many rules of law.

The right to information and freedom of information are necessary conditions to the construction of the image and understanding of oneself (Self) and in social relationships in the private sphere with other individuals and in public interrelationships. Without the right to information and freedom of information our understanding of ourselves as individuals and our participation in various human relationships would be severely limited. The right to information and freedom of information are fundamental indicators of the possibilities for self-respect and awareness and participation in a society. The fundamental moral and ethical justification of the right to information lies in this constitutive nature of information rights and informational freedom. Freedom of information and the right to information are the anti-thesis of oppressive or colonialising paternalism and denial of one's voice, however good the intentions of this paternalism might be. The principles underlying the right to information and freedom of information consider every individual and every community as sovereign, capable and worthy of self-understanding, critical questioning and self-decision. The right to information and freedom of information are moral and ethical principles which lay the foundations of contemporary information ethics and the ethics of community-building and participation.

The freedom of information and the meta-right to information means:

1) Individual and collective access to information.

2) Freedom of information from property rights and restrictions on utilisation, that is, possession of information as a commodity of the public domain.

---

resources to democracy, *see* Kuronen Timo, *Tietovarantojen hyödyntäminen ja demokratia*, SITRA, Helsinki 1998.

5 In economics literature empirical evidence is presented to support these theoretical claims, see *e.g.*, Jin, Ginger Zhe and Leslie Phillip, *The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards*, in The Quarterly Journal of Economics 2003, 409-451.

6 *See*, on this Dommering, Egbert J, *An Introduction to Information Law*, op. cit. and, Pöysti Tuomas, *Tehokkuus, informaatio ja eurooppalainen oikeusalue*, Forum Iuris, Helsinki 1999, p. 381-385 and 404-406.

3) Free flow of information.

The freedom of information as a legal, political and moral principle is not the same as the provision of information free of charge. The link between the pricing of informational products and services and the freedom of information is the prohibition against preventing access to information by unreasonably high prices. In several instances, the freedom of information principle, however, requires, that information is provided free of charge, or, at least, at an affordable price covering only the direct costs of disseminating the information.

The information policy of contemporary network societies or information societies is founded on the principles of the right to information and the freedom of information. Information policy is not often used in Scandinavian or European legal or political contexts to describe the principles according to which production and dissemination and access to information of various types is organised in a society. Nevertheless, the principles of the right to information and freedom of information are inherently the constitutive elements of information policy and permanent criteria for evaluation of the impacts and effectiveness of information policy. Information policy is a significant element of a wider principle of good governance. Good constitutional governance in a society and organisation and good corporate governance in the private sector set certain criteria for the content of information policy requiring the greatest right to information and freedom of information possible. The changes related to the development of information and communication technology and the resulting rise of network society accentuate information policy issues. Information policy and information and communication strategies have gained in importance but have also become more and more explicit among policies, not least within legal regulation. The trend towards open and explicit information policy as a legislative goal and systemic principle of law is particularly visible in the domain of public sector freedom of information or publicity legislation.

The right to information and freedom of information with their corollary principle of free flow of information have wide institutional foundations in the constitutional rules and enacted laws of various sectors. The ultimate foundations of the general freedom of information principles lie in the fundamental right of freedom of expression, which according to Article 10 of the European Convention on Human Rights and Article 11 of the EU Charter of Fundamental Rights is the right to receive and impart information without prior interference. This principle on the fundamental right to communication, behind which there is a wider institution and principle on the right to communication, establishes the free flow of information as an element of the freedom of communication and also requires wider freedom of information. Freedom of expression and communication would be meaningless if there were no information, free to be used in communication. The English version of the EU Charter captures very well this point even in the heading of Article 11: that article addresses freedom of expression and information. Further constitutional support for the principle of freedom of information can be derived from the social and civilisation rights protecting and promoting rights to culture, civilisation and knowledge and the freedom of research and university education. These social and civilisation rights, which establish a constitutional

policy and policy-level obligation for the legislature to promote the values represented in civilisation rights, require information and its freedom as their basic elements.

The rules representing and implementing the right to information and freedom of information can be classified as emerging general information law rules covering both the public and private sector, public information law rules covering the governmental sector, private information law rules governing the public domain in the private sector and private information law rules covering the private domain which is under individual privacy. It is noteworthy that the public and private domains are not subject to a distinction between public and private law. There is an important public domain whose foundation rests on the rules and principles of private law, such as copyright law. This is a systematic challenge, since the doctrine and legal policy of private law easily tends to focus on the narrow private interests or considerations of efficiency of markets and neglects the general public interest. This is especially true in the field of copyright law, which exists not only to protect the exclusive rights of copyright holders but also to promote the creation and dissemination of and access to information. There are also public information law rules, like the right of a party to administrative proceedings to have access to his file, which regulate the confidential relationship between an authority and a private party and which do not constitute any public domain information. The public and private domain divide is also present in the general information law rules which by their scope of application and regulatory paradigm cover both public and private law relationships.

As a general principle of law and justice the freedom of information and the meta-right to information overcomes the public – private distinction in the systematic of law. However, informational freedom and the right to information exhibit different appearances and interpretations in the public and private domain and in public and private information law. The history of the institutions representing the idea of freedom of information, whether they are doctrines or enacted rules and principles of law, is different in different fields of law. Nevertheless, these rules, principles and doctrines form a sufficiently coherent common stance towards the relationships of information, liberty, freedom and responsibility. The meta-right to information and the freedom of information are principles of law, not rules unless so enacted in law. As a principle its weight might differ in various situations.

Information law is shaped by the tension between the freedom of information and the general right to information as commons and the limitations and exclusive positions and rights to information.[7] Practical information law is finding both a theoretical, abstract balance between informational freedom and the position of information as commons, and the restrictions of this freedom, and the concrete application of this balance in practical cases and legal and ethical problems.

---

7 On this fundamental tension and conflict of information law, *see* Dommering, op.cit. and Pöysti, op.cit.

2.2 Access to and Freedom of Legal Information: Towards Universal Service of Legal Information

The first element of informational freedom is the general right of access to legal information, that is, information about law and norms set by contract before entering into a contractual relationship or modifying an already existing relationship. The principle of access to legal information is among the foundations of the rule of law. Norms are supposed to be public and thus secret legislation or hidden norms are not accepted as valid. The publication of norms is a necessary condition of validity within the concept of the rule of law applicable in Western countries. The fundamental idea is that individuals must be able to align themselves with the requirements of the norm voluntarily, that is, by using their own individual will. Publicity of norms and access to legal information is thus among the conditions of effective use of individual self-determination and is one of the most fundamental principles of justice and respect of human dignity endorsed by human rights norms and the constitutional traditions of Western countries.

The principle of access to legal information is an inherent requirement of the principle of no punishment without law endorsed in Article 7 of the European Convention on Human Rights. The principle of access to legal information is also founded on the constitutional duties of publishing the laws enacted. In Finland this constitutional obligation is stipulated in Section 79 of the new Constitution, which entered into force in 2000:[8] the Government shall without delay (after the confirmation of the act by the President of the Republic) publish it in the Statute Book of Finland. An act may enter into force only on the date of its publication at the earliest, but constitutional practise allows an act to have retroactive application provided, that such application does not limit fundamental rights or violate the no punishment without law principle. Section 79 of the Constitution shall be read together with Section 80 of the Constitution, which requires that all rules concerning the principles of rights and obligations of individuals shall be given by an act of law, which shall be published. Section 80 requires that an act provide general provisions on the publication of decrees, which the President of the Republic and the Government may issue on the basis of an explicit and narrowly defined authorisation in the Constitution or in an act. After the entering into force of the new Constitution, a new Act on the Statute Book of Finland (188/2000) was adopted. The new act formally recognises electronic publication as the valid form of publication. There is an electronic version of the Statute Book of Finland, and, in cases of urgency, the publication of an act or decree in the electronic version is sufficient for the entry into force of the act or decree. The new Act on the Statute Book of Finland also reinforced the obligations to publish decrees and legal rules given by other authorities than the Government and Governmental ministries.

In European Community law the principle of legal certainty and the principles of sound administration, which are used by the Community courts to assess the legality of the acts of European institutions, including legislative acts, include the requirement of prior publication. These principles also prohibit the

8 Act 731/1999.

retroactive dating of a publication or legislative act itself. The Court of First Instance has, for example, found in the *Opel Austria Case*, that the Council violated this principle when it adopted on 20 December 1993 a regulation imposing anti-dumping duties on certain products of General Motors Austria. The Council had violated the principle of legal certainty among other things by deliberately back-dating the relevant issue of the Official Journal. The regulation was sent to the publication office on 3rd or 4th of January, and according to the text of the regulation, it was due to enter into force on the day of its publication. On the request of the Council the regulation was published in the Official Journal of 31st December even though it was sent after that date to the publication office.[9] The case shows that the general principles of law and their vigorous application by the courts provide safeguards for even elementary principles on the rule of law, when considerations of expediency would otherwise lead the legislature and government to bypass them. The case also shows that the principles of proper publication and publicity are not necessarily self-evident in practise.

There is a long historical tradition of publicity and publication of legal rules in Nordic countries. The application of the principle of access to and publicity of information about legal rules is situational. There has been a way of publishing and distributing information about legal rules specific to each period, which has been the most efficient in the particular conditions of the time. In early societies the publication consisted merely of common discussion or shared stories in the meeting of the community in a session of court and public decision-making, at ting.[10] Later, publication in printed form became the principal channel of publication. In Finland, the new Act on the Statute Book of Finland ushers publication methods into the era of electronic information even regarding the formal publication of laws. Concurrently, there is a clear strengthening of the demand of efficiency of constitutional rights and obligations. This means that formal publication of the Statute Book is not sufficient, and there is a wider constitutional basic duty of publication of legal rules and legal information.

This duty of publication expands towards a principle of universal service concerning legal information. The juridical foundation for this enlargement is the duties of public authorities to assure the observance of fundamental rights, which means among other things, that fundamental rights must be effective in practise.[11] There is also a wider trend in the law and practise concerning freedom of information and access to information towards universal public service. Also

---

9 Case T-115/94, Opel Austria v. Council, [1997] ECR II-39.

10 *See* on the historical development of publicity of norms Peter Blume's dissertation *Fra tale til data, studier i det juridiske informationssystem*, Akademisk Forlag, Copenhagen 1989, which is a fascinating story about the change of legal information dissemination from ancient times to the early stages of information society. *See* also *e.g.* Statens Offentlliga Utredningar SOU 1988:64, *Integritetsskyddet i informationssamhället*, 5. Offentlighetsprincipens tillämpning på upptagningar för automatisk databehandling. Slutbetänkande av data- och offentlighetskommittén., p. 19 in which the principles of publicity and transparency are traced back to the medieval ting tradition.

11 This positive duty of public powers to assure and promote the observance and respect of fundamental rights is based on Article 1 of the European Convention on Human Rights, and, in Finnish constitutional law on Section 22 of the Constitution of Finland.

the principle of publicity of government documents and government information is evolving towards universal information service and similar trends are discernable in the legal developments occurring within private information law. The direction towards universal public service is visible in the practises concerning publicly available legal information databases in Finland, Sweden and other Nordic countries and in the European Union. In Finland, the FINLEX –database has been expanded and opened for public access free of charge on the Internet. The new FINLEX contains, among other things, consolidated texts of major legislation in force. The European Union has greatly developed its Eur-Lex portal and publication of consolidated versions of European regulations, directives and treaties.

Traditionally, access to legal information has been a principle of law applicable within public information law in the relationships between a public authority (public powers) and private parties. There are also principles and doctrines of private law, particularly contract law, which require adequate access to applicable contract rules as a condition of validity of contract or as an element of required reasonableness of contractual obligations. One of the oldest institutions to that effect is the doctrine of unpredictable and severe conditions of contract, which is developed by the Supreme Court of Finland to review standard clauses of contracts. This doctrine implies not only theoretical access but also the practical availability of contract conditions. Nordic consumer law and recent European Community consumer protection directives and the directive on electronic commerce require the clear availability of terms of contracts prior to ordering or contracting. Efficient access to relevant contractual information is, thus, a requirement of information policy imposed by law. This requirement has, apart from influencing marketing and information policy, also wide implications for the user-interface design and communication with the consumer in the applications of electronic commerce.

2.3 Public and Private Access to Information and Informational Liberties in Informational Privacy Law

The informational privacy laws are one of the cornerstones of general information law applicable both in public and private relationships. Informational privacy laws define the rules and principles concerning informational privacy, integrity and security of identity, and, thus, often appear as counter-weights to or colliding rights and interests with freedom of information. The terms informational privacy and informational privacy law are, although of Anglo-American origin, intentionally used here. Informational privacy is a wider institution than the laws concerning the processing of personal data or data protection for short. Informational privacy legislation consists of legislation concerning processing of personal data, the criminal and civil liability of defamation and other acts infringing privacy and the legislation concerning surveillance and confidentiality of communications.

The management of conflict between privacy-related interests to restrict information processing and the free flow of information, and finding a just balance, is the core task of informational privacy laws and their application. The

EC Personal Data Directive (Data Protection Directive)[12] nevertheless defines free movement of personal data as one of the principal objectives of the Directive[13] and, prohibits restrictions of the free flow of personal data between Member States on the grounds of the protection of privacy.[14] The European Court of Justice has also in its preliminary ruling concerning the Personal Data Directive emphasised the principle of free flow of personal data between the Member States as the objective according to which the provisions of the Directive shall be interpreted.[15] The personal data directive constitutes as such the general principle of the free flow of personal data, provided that the requirements of privacy protection are duly taken into account.

In addition, Article 11 of the Personal Data Directive establishes the rights of the data subject to access data concerning himself, which is an access right in the private domain. Article 10 of the Personal Data Directive requires further that the data subject shall have access to information concerning the controller of personal data, the purposes of processing and any further information, which is necessary for guaranteeing to the data subject the fair processing of data.[16] Further information means, among other things, the identification of recipients of data, if personal data is transferred further, and information about the existence of the right of access and the right of rectification of data. Section 10 of the Finnish Personal Data Act (523/1999), which implements the Personal Data Directive, requires that the information to which the data subject has a right of access according to Article 10 of the Personal Data Directive - the statement of the contents of the personal data register and the purposes of processing - shall be kept available for everyone. Basic information about the contents and purposes of personal data processing thus belongs to the public sphere and there is a general right of access to such information.

The Directive and, the Personal Data Act in Finland promote the drafting and publication of privacy policy statements as part of a good processing practise. These statements provide an additional, information policy level access to information serving the needs of individual self-determination and the control of legality and fairness of processing. Privacy policy statements and the publication of general information about the purposes of processing and processed data also form the basis of openness and transparency of personal data processing practises in the public domain and enable control of the fairness of data processing through public debate.

---

12 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.

13 *See* recitals 3 and 7-9 of the Personal Data Directive.

14 Article 1 (2) of the Personal Data Directive.

15 *See*, *e.g.* joint cases C-465/00 C-138/01 and C-139/01. Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v. Österreichischer Rundfunk, [ECR 2003] I-4989, paras. 39 – 43.

16 Article 10 of the Personal Data Directive.

2.4 The Right of Access to Government Information and Freedom to use Government Information

Access to information and freedom of information have their strongest foundation in the Swedish and Finnish legal tradition in the principle of access to documents and information held by public authorities. This right of access to information has been part of constitutional tradition since the Freedom of Press Act of 1766. The origins of this right were in the openness and public participation of the community in sessions of the local court and administrative body - the ting.[17] Historically, the emergence of the principle of access to public documents and publicity related to the fight against the absolutist form of government, the rise of democracy and economic liberalism.[18] In Finland, the constitutional status of the right of access to the documents and information of public authorities and the principle of publicity has significantly strengthened with the reform of fundamental rights entering into force in 1995 and with the Constitution of 1999. Publicity and the right of access to documents and information are according to Section 12 (2) fundamental rights, which may only be specifically limited by compelling reasons by an Act of Parliament. A limitation of publicity shall comply with the general principles concerning limitations of constitutional rights, such as the principle of proportionality, necessity and a specific, narrow drafting of the exception. Access to government documents and information is a subjective right directly regulated in the Constitution.

More detailed provisions concerning access to documents and information of public authorities and the provisions on secrecy are in Finnish law in the Act on the Openness in Public Authorities (621/1999), hereinafter the Openness Act of Finland. This act is a mixture of administrative law tradition of publicity and contemporary principles and paradigms of network society. The act aims to be a general code of information and information management law in public administration. Information management, communication and information security rules are, in the systematics of the act, attached to the principle of access to documents and information, which aims to secure the efficiency of the access rights and also to maintain access rights as the leading principle concerning information management by public authorities.[19] There are several specific information management rules, which aim to facilitate easy access to public information and the efficient implementation of the right to information. Technical and social change resulting from the development of ICT is reflected in the provisions about communicational strategy and information policy as well as in the rules concerning good information management practise. The Openness Act of Finland is, thus, a network age access-to-information act in which the efficiency of access rights in network conditions is paid particular attention. The

---

17 *See, e.g.* Timo Konstari, Asiakirjajulkisuudesta julkisessa hallinnossa, Suomalainen lakimiesyhdistys, Helsinki 1977, p. 37 and SOU 1988, op.cit. p. 19.

18 Konstari, op.cit., 20 – 24.

19 Anna-Riitta Wallin, legislative counsellor of the Ministry of Justice and the principal drafter of the Openness Act, and Professor Timo Konstari call this a choice of perspective within information law, *see* Wallin & Konstari Julkisuus- ja salassapitolainsäädäntö, op. cit.

Act represents even a wider trend to regulate communicational strategies in the freedom of information legislation. The act actively develops the principle of the right of access towards an obligation of universal public information service.

The traditional right of access functionally serves to control the actions of public authorities. As such, however, it does not define very precisely the communicational strategy, which the government and public administration in general should follow. There are, according to Professor *Timo Konstari*, developing further the analyses of *Kenneth Abrahamson* the following different options for communicational strategy:

1 Secrecy, in which the public documents and information are kept secret.

2 Discretionary publicity in which the authority or a higher authority decides which documents and to which extent information is public.

3 Classical, public publicity and the right of access to information principle, in which documents are public and everyone requesting a document has a right to receive it except in cases defined by law in which the document is secret.

4 The active publicity principle, which can be called an information principle, in which the authority actively publishes its documents and provides tools for identification of information but in the publication it is for the authority to decide which documents to publish.

5 The communication principle in which private parties and public authorities are in mutual communication and exchange information actively and in which the public authorities not only publish actively but participate actively in communication and in which the authority and private party are equal and mutual partners in communication.[20]

The communicational strategies relate to the question of minimalism and maximalism in the development of the right of access.[21] Development of the Swedish and Finnish access legislation, and, also the development of access to information in European Community/European Union law, can be seen as changes in the stance towards different communicational strategies and also to the question of minimalism and maximalism. The Freedom of Press Act of 1766 finalised the transfer from secrecy rule to a classical publicity principle. Later, a certain cautiousness is attached to the classical passive publicity principle, which

---

20 *See* Konstari ,Timo, Asiakirjajulkisuudesta, op.cit., p. 3, and Abrahamson Kenneth, *Samhällskommunikation, om kontakten mellan myndigheter och medborgare*, Lund 1974, p. 181-208.

21 On minimalism and maximalism as approaches to the scope and functions of access-to-rights, *see* Seipel, Peter, *Access Laws in a Flux*, in Seipel, Peter (ed.), Law and Information Technology, Swedish Views, Statens Offentliga Utredningar SOU (Swedish Government Official Reports) 2002:112, 88-98, p. 95-98.

remains an important tool in the control of government. The 1999 Openness Act of Finland takes a significant step further in the communicational strategies. The active publicity principle is defined as the main principle of access law while still recognising the importance of the classical, passive publicity principle. The act mandates and promotes publication of information in information networks and requires active publication of materials and information. The act also sets the communication principle as a policy aim, and the new Administrative Procedures Act (434/2003) further strengthens this general policy objective of promoting active possibilities of participation and consultation. The communication principle is clearly inherent as a legally required communication strategy in the rules of the Openness Act to provide information on the matters pending and concerning the active information service of public authorities. There is also a Government Decree on Openness in Public Authorities and Good Information Management Practise (1030/1999), issued on the basis of the Openness Act, and this Decree contains particular provisions of communicational policy of public authorities. The Openness Act and its implementation have taken a much more maximalist approach to the media and method of publicity. The act also aims to tackle the problem of fluidity of information flows through its rules concerning good information management and the documentation and establishment of information networks as one the principal media of access.[22] Fluidity is an essential and accepted part of the communication principle. In its widest application, the communication principle means (1) active e-citizenship and participation as the form of democracy in public administration and (2) change of access to universal public information service available to all.

The principle on the right of access to documents and information has had a surprisingly rapid and fairly successful arrival in the law of the European Union, becoming as it has a general principle of Community law and a constitutional principle of the European Union. Today Article 41 of the EU Charter of Fundamental Rights recognises the right of access as a Union-level fundamental right. The EU Charter is not yet directly legally binding but it represents the formulation of the current understanding of fundamental rights in the Union, which shall be applied as generally accepted legal principles of Community law. The current Article 255 of the EC Treaty, furthermore, states explicitly the right of access to European Parliament, Council and Commission documents and, thus, the right of access is a Treaty-based principle in Community law.[23]

---

22 The Government has recently produced a report to the Parliament on the implementation of the Openness Act. The report states that the new act has strengthened publicity and access particularly in the Ministries, and the availability of information has increased and the attitudes in public administration have become more openness-friendly. The good information management practise provisions were not the subject of evaluation, since there has not yet been enough time to gain practical experience of their application. The information management obligations had a long transition period. *See, valtioneuvoston selonteko eduskunnalle julkisuuslainsäädännön kokonaisuudistuksen täytäntöönpanosta*, VNS 55/2003 vp.

23 Before the inclusion of Article 255 in the EC Treaty, there has been a certain ambiguity in the case law of the European Court of Justice as to whether the right of access is a general principle of Community law. The Court of Justice avoided in its case law, the taking of a direct position on this question, *see* Lenaerts Koen, *In the Union we trust: trust-enhancing*

Access to documents and information started to emerge as a principle of Community law as a result of the growing distrust towards governments in general and towards the significant deepening of European integration in particular and of the increased activity and influence of civil society and non-governmental organisations at the national, European and international level.[24] For the implementation of the Declaration, the Council and Commission adopted a Code of Conduct in which the principle of widest possible access of the public to the documents held by the Commission and the Council was established. On the basis of the Code of Conduct, the Commission and the Council adopted their own decisions implementing the Code of Conduct and the European Parliament adopted its own decision on transparency. Before the inclusion of Article 255 in the EC Treaty, the decisions on the right of access were adopted on the basis of the institutional autonomy and internal organisation power of each institution. Following the adoption of these decisions, several cases appeared in the Court of First Instance and in the Court of Justice in which the Community courts were essentially asked to assess whether the right of access to information was a general principle of Community law. Such categorisation would authorise the Community courts to assess the legality of the exceptions provided for in the decisions. The position taken by the Community courts was ambiguous and cautious even though in several judgements the courts significantly strengthened the realisation of transparency.[25] In *Hautala v. the Council*, Advocate General Léger suggested to the Court the recognition of a fundamental right of access to information held by Community institutions.[26] This right of access is, according to the Advocate-General derived from the most essential political foundations of the Member States of the Community. The Court did not explicitly endorse this opinion, neither in its judgement nor in its subsequent judgements prior to the inclusion of Article 255 of the EC Treaty by the Treaty of Amsterdam.

Community courts have taken a clear position that exceptions to access must be interpreted strictly and there shall be sufficient and acceptable reasoning justifying an exception.[27] Community courts have also underlined in their practise the connection of the principle of access to democracy and the democratic character of European institutions and its particular function to enable closer participation in the decision-making process, greater legitimacy of the institutions and administration, which is more effective and accountable to citizens.[28] By this the courts have rapidly imported general doctrines of public access legislation into the Community legal order and created a strong foundation for the application of the principle now enshrined in Article 255 of the EC Treaty and in the European Charter of Fundamental Rights. The Court of

---

principles of community law, in Common Market Law Review 2004, 317-343.

24 Lenaerts, op.cit., 318.

25 Lenaerts, op.cit., p. 321.

26 Case C-353/99 P Hautala v. Council [1999] ECR II-2489.

27 *See, e.g.*, Joined cases J-174/98 P & C-189/98 P, Netherlands and Van der Wal v. Commission [2000] ECR I-1, Case C-353/99 P, Hautala v. Council, op. cit.

28 *See e.g.* case C-41/00 P, Interporc Im- und Export GmbH v. Commission [2003] ECR I-2125, para. 39.

Justice has also used the principle of proportionality as a tool to further limit and control the discretion left to the Community institutions to apply the exceptions the transparency decisions allowed them. Derogations from the general rule of access must remain within the limits of appropriateness and be necessary for achieving the aim in view. This means that there is an obligation to the Community institution to consider a partial access to information if some parts but not the whole document fall within the exception of access.[29] Community courts have also accepted proportionality in the sense of reasonableness of the administrative burden caused by the obligation to give partial access. In exceptional cases in which the partial access and the resulting blanking out of the parts would be exceptionally heavy and exceed what could be reasonably required, there is no obligation to grant partial access. That principle places greater emphasis on administrative efficiency and expediency than what the rules and doctrine of Finland's Openness Act allow.

Following the inclusion of Article 255 in the EC Treaty, the European Parliament and the Council have adopted the so-called Transparency regulation, the regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents. The preamble of the regulation states the general functions and justifications of the access to documents, which were already expressed in the reasoning of the Community courts. The purpose of the regulation according to its Article 1 is to ensure the widest possible access to documents, to establish rules ensuring the easiest possible exercise of this right and to promote good administrative practise on the access to documents. The transparency regulation aims to establish an access-friendly (publicity-friendly) information management practise and information infrastructure within the Community institutions and as such it has several features in common with the Finnish Openness Act. Article 11 obliges the institutions to provide public access to the register of documents in electronic form in order to make the access right effective. Article 12 of the regulation even obliges the institutions, as a matter of principle as far as possible to make documents directly accessible to the public in electronic form. Electronic access to documents has in fact developed very rapidly and covers, for example, the majority of the Council's documents. The regulation also defines the exceptions to the rule of access. Access to a document shall be refused where disclosure would undermine the protection of the public interest as regards public security, defence and military matters, international relations, the financial, monetary or economic policy of the Community or a Member State. Access shall also be refused to documents where disclosure would undermine the protection of the individual's privacy and integrity. Unless there is an overriding public interest in disclosure, access shall also be denied where the disclosure would undermine the protection of commercial interests of a natural or legal person, including intellectual property, court proceedings or legal advice, the purpose of inspections, investigations and audits. Access to documents internal to institutions shall also be refused if the institution's decision-making process would be seriously undermined and there is no overriding public interest in disclosure. The exceptions contain broad categories, which often fall under secrecy according to Finland's Openness Act

29 *See, e.g.* case T-14/98 Hautala para. 87 and Case C-353/99 P, Hautala para. 31.

or Sweden's Secrecy Act (sekretesslagen). There have been some concerns that the broad and vague formulation of the exceptions leave too much discretion to Communityinstitutions or may undermine the general principle of access.[30] Here the principles and lines of interpretation taken by the Community courts in case law prior to the regulation are still valid and informative. Exceptions shall be interpreted strictly and exceptions may not be disproportional. The Community courts are expected to take a clearer and stricter line since access to documents has been elevated clearly to a general principle of Community law in the EC Treaty and is a fundamental right in the Charter.[31]

In the future, if the new Constitutional Treaty, whose content was accepted by the Inter-Governmental Conference at the level of Heads of States or Government in 2004, is ratified and enters into force, the constitutional status of the publicity principle will be significantly further strengthened. The EU Charter of Fundamental Rights will become a legally binding part of the constitutional treaty and Article 255 will be replaced by Article I-49 (3) of the Constitution. The article provides for access to documents, regardless of their medium, to all Union institutions, agencies and bodies.[32] Some of the contents of Article 255 will become Article III-305,[33] requiring institutions, bodies and agencies to ensure transparency in their work. The article will place a particular duty on the European Parliament and Council to publish the documents of the legislative procedure. In addition, as open as possible decision-making and the right of individuals and their associations to participate in consultations prior to Union decision-making are incorporated as fundamental principles of the democratic life of the Union.[34] The Constitutional Treaty, together with the provisions already included in regulation 1049/2001, is a further step towards active public access to information and, ultimately, towards the communication principle as the leading communicational strategy of the Union.

Related to the evolution in Community law, it is also noteworthy that access-to-government information (freedom of information) legislation has been expanding in the Member States as well. There is, for example, a new Freedom of Information Act in the UK, which, even though it does not constitute a Nordic type of right of access, represents a significant expansion of transparency and freedom of information held by public authorities.

Community law has also made a major contribution to the development of the principle of freedom of information by adopting the European Parliament and Council Directive 2003/98/EC on the re-use of public sector information,[35]

---

30 *See*, *e.g.*, the opinions of the Finnish Parliament's Constitutional Law Committee on the original Commission proposal and a draft version in the Council working group, PeVL 6/2000 vp. and PeVL 31/2000 vp.

31 Lenaert, op.cit.

32 *See the draft consolidated Treaty establishing the Constitution for Europe*, document CIG 86/04.

33 The inter-governmental conference agreed on consecutive numbering in arabic numerals of the Constitution. Therefore, the numbering will be revised.

34 *See* Articles I-45, I-46 and I-49 of the draft Treaty on the Constitution for Europe, CIG 86/04.

35 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

hereinafter the Re-use Directive. The Re-use Directive establishes the principles of fair and equal rules concerning commercial and other re-use and exploitation of public documents and information held by public authorities. The Directive strengthens, even though it does not require the Member States to establish, the principle of the freedom to use public sector documents and information commercially and for other purposes. The Directive does not change the legislation concerning the material rules concerning right of access to information. The focus of the Directive is on the delivery of documents and information to which lawful access has been guaranteed by national law and, on the principles concerning the pricing of delivery of the documents. The Directive promotes at the level of European law the freedom of use – and free flow - dimensions of the freedom of information and information falling under the general right of access, and, requires the Member States, as far as possible, to provide also electronic access to public and re-usable public sector documents and information. The right to information and the freedom of information consists, thus, of the right of access to information held by public authorities and the right to re-use and exploit the documents and information of public authorities. The aim of the Directive is to contribute to the development of the European information markets and increase the efficiency of the information markets and thereby contribute to economic growth. The public information held by authorities or bodies comparable to authorities is seen as a potential resource for commercial activities, particularly in the provision of digital contents.

The background of the Directive is the United States' experience with the federal Freedom of Information Act, which has contributed to development of commercial activities, providing added value to informational resources held by the administration. The Commission wanted to introduce the same principles in the European Union. During the early drafting of the policy there were ambitions to even legislate on access to public sector information but finally the Directive came to focus on the internal market law aspects of the utilisation of public documents and information held by the administrations of the Union and its Member States. The directive follows the policy lines developed in the Commission's Green Book "Public Sector Information – a Key Resource of Europe".[36] The Member States have to implement the Re-use Directive before 1 July 2005. The Re-use Directive takes a maximalist position on the opening of public digital content resources electronically to the private sector for commercial and other exploitation, and, attaches an economic, information markets dimension to the principle of publicity. Therefore, the Re-use Directive is also a strange act in the eyes of traditional access lawyers attached to the constitutional law tradition of publicity. Essential parts of the Directive are namely particular competition law or law establishing the economic constitution of the information markets.

The implementation of the Directive in Sweden and particularly in Finland will be a difficult task in a technical and systematic perspective even though the substance of the Directive fits fairly well the main line of policy and principles of legislation. The Community law principle of legal certainty and other

36 COM (1998) 586 final, *Public Sector Information – a Key Resource of Europe, Commission Green Book on the Use of Public Sector Information in the Information Society*.

Community law principles concerning implementation of Community directives require that the Directive be implemented by clear and legally binding legislative acts either by primary legislation or by delegated legislation. General principles and non-binding, soft law recommendations and established administrative practise alone would not necessarily fulfil the requirements of appropriate implementation. The Openness Act in Finland is silent on the pricing of the delivery of documents and information. There is a separate Act on the General Criteria Governing the Charges to be Levied on the Official Functions (150/1992), hereinafter the Act on Charges Criteria, laying down the general principles and powers of the pricing of central government official functions in which a charge is to be levied.

According to the Act on Charges Criteria, services in which the demand is based on rules of law or decree, i.e. products and services of a public law nature, shall be priced so that the charged fee corresponds to the production and delivery cost. Other services, which are produced on the basis of voluntary demand, are to be priced following the principles of good business management and judgement, that means, a price similar to the market price shall be charged. Each ministry has the power to decide which services and products belong to these two main categories as well as the exact price to be set as a fee following the general principles of the Act. The Act does not specially regulate information deliveries and the systematic of the legislation is based on the principle that the Act, as general legislation, does not make direct references to particular types of services. If this principle were to be followed, the implementation of the Re-use Directive would take place in terms of particular charge regulations. Assuring sufficient unity and even the proper implementation of the Directive is then a major technical task. This alternative, however, also leaves open the prices charged for information deliveries by municipal authorities since the Act on Grounds of Pricing is applicable only to central government services and is not applied to municipal charges. Another alternative would be to develop a particular act on the charges and procedures for information delivery or to attach such rules to the Openness Act. The latter alternative would fit the general systematic principle of concentrating all the main rules concerning public sector information management in the Openness Act. This solution would also provide for the opportunity to clarify some of the open issues in the pricing of governmental information and systematically align the decisions on prices with the main principles of public sector freedom of information legislation. According to the recent Government report on the reform of the openness legislation, the authorities tend to charge for the delivery of copies under the Openness Act according to business management principles even though the purpose of the act is that only the direct costs of producing the copy should be charged.[37] This example shows that there is a need for a horizontal, but particularly information-related general legislation addressing all the issues related to the freedom of information and the production of governmental information for information markets.

---

37 Government report to the Parliament on the implementation of the general reform of the public access to documents and information and secrecy legislation, VNS 5/2003, op. cit.

2.5 The Freedom of Information in the Private Information Law

The right to information as access to information and a right to reuse and exploit information are evolving but already fairly well established principles in Community law and, particularly in the law of Nordic countries. The right to information and the extent to which information is free for exploitation and re-use is a far more controversial topic in private information law, particularly under the copyright and related rights regime. The controversy arises from the different stances towards copyright and its relation to technological possibilities and limitations and to other rights and freedoms.

There are three major ways or background theories for understanding copyright and putting it into the overall context of the legal order.[38] The critical point of difference between the various theories is the centre of the copyright system and whether it is maximalist or minimalist in the safeguarding of the exclusive rights of the copyright holder. One particular difference is how the limitations and exceptions to copyright are seen and justified in the various theories, which function as paradigmatic models for justification and argumentation in copyright law. Each of these paradigms also implies a different stance towards the change following from the development of ICT and how copyright law should change as a result of ICT–related changes.

First among these paradigms is the author-centred or natural rights paradigm. At the centre of it is the notion of the author, and, it tends to be maximal in its protection of the exclusive rights of the copyright holder. Justification of copyright under this approach is based on the requirements of the general principles of justice and morality, which require that the inventor shall have exclusive rights to the fruits of his creativity. Copyright, ultimately, does not depend on the law, but is derived from the fundamental principles of justice and morality.[39] Copyright particularly protects creativity, and, since the personality of the author is at play in the creation, the wider dimension of copyright is protection of personality. The author-centred paradigm with natural rights tendencies may be reinforced by explicit references to protection of copyright as a fundamental right. Article 17 (2) of the EU Charter on fundamental rights includes a provision on the protection of copyright as part of the protection of the right to property. It remains to be seen whether this leads to a fairly author-centred reading of international and European copyright norms and accommodates natural rights–type thinking in the deep structures of legal policy and argumentation, or, whether reference to copyright protection serves to simply inform that the right to property protects also immaterial, intangible property. The natural rights or the author–centred paradigm sees the development of ICT and the resulting digital environment mainly as posing risks to the realisation of natural rights of the author or right-holder. Therefore, the protection of copyright must be strengthened in the digital environment. The

---

38 This analysis of the various ways to understand the foundation and functions of copyright is inspired by the analyses of Guibault, Lucie M.C.R. *Copyright Limitations and Contracts. An Analysis of the Contractual Overridability of Limitations on Copyright*. Kluwer, the Hague 2002.

39 On the natural rights paradigm, *see* Guibault, Lucie, *Copyright Limitations*, op.cit., p. 8-9.

limitations and exceptions to copyright, which are recognised in the paper-based, analogue world, are explained mainly by technical reasons, and they should not be transposed as such to the digital environment.[40] The use of technical protection measures are seen as the natural right of the copyright holder, and, consequently, the excessive use of them, even to the extent of the use falling under the limitations of copyright, is not seen as a problem.

The second paradigm is the utilitarian understanding of copyright. In this model, the primary function and objective of copyright is to promote general utility of most people and society as a whole by encouraging the production and dissemination of works of culture and facts to society.[41] The production and dissemination of works is encouraged mainly by creation incentives through the exclusive economic rights of utilisation. The limitations of copyright may also serve, in this perspective, important utilitarian needs, but what finally counts is the overall utility calculus. In the debate, the utility calculus is often reduced to an economic welfare calculus, in which the role of copyright is to provide proper incentives to maximisation of welfare. The utilitarian approach accepts the copyright only to the extent that it serves utilitarian purposes, beyond that point there is no justification for copyright. The utilitarian model is, in theory, neutral concerning minimalist or maximalist tendencies of copyright protection with regard to changes and challenges arising from ICT and digitalisation. In the utilitarian model, the tension between various tendencies must be solved by overall utility and welfare calculus, which ultimately is the task of the lawmaker. In the practical legal policy debate and in official documents, however, the utilitarian value of expanded copyright is often taken for granted, without an open and critical application of utility calculus. In Finnish law, the recent government proposal to amend the Copyright Act and Chapter 49 of the Penal Code for the implementation of the European Parliament and Council Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, hereinafter the INFOSOCDirective, the functions and justifications of copyright law are attached to the utilitarian model from which also the need for strengthening the protection of copyright is derived as a natural conclusion.[42]

The third paradigm is the balancing model, which sees the function and justification of copyright law as striking a balance between various social goals and moral virtues and the legitimate interests of various stakeholders. The exceptions to and limitations of copyright are not technical features and obstacles following the conditions prevailing in certain technical environment. The exceptions and limitations are rather for deliberate protection and recognition of various other fundamental rights and moral values than the mere

---

40 Regardless of the doctrine, there seems to be a common understanding that the solutions of the analogue and paper-based world cannot be applied without modifications in the digital environment, Guibault, Lucie, *The Nature and Scope of Limitations and Exceptions to Copyright and Neighboring Rights with Regards to General Interest Missions for the Transmission of Knowledge: Prospects for Their Adaptation to the Digital Environment*, UNESCO, e-Copyright Bulletin, October – December 2003, p. 1.

41 Guibault, Copyright Limitations, op.cit. p. 10.

42 *See, Hallituksen esitys eduskunnalle laiksi tekijänoikeuslain ja rikoslain 49 luvun muuttamisesta*, HE 28/2004 vp., luku 1, johdanto.

protection of property. Copyright limitations are, in particular, the positive recognition and protection of freedom of expression and the right to disseminate and access knowledge and the freedom of information and free flow of information.[43] A balancing paradigm requires always an overall weighing between the various legal and ethical principles at stake in the particular situations falling under copyright law. The balancing model can also, thus, be called a justice all-things-considered paradigm. The balancing model openly and explicitly sees the principle of freedom of information and free flow of information as derivatives and background principles of fundamental rights.

It is fairly easy to make a choice between different paradigms if copyright law is put into the wider context of the legal order as a whole and in the context of good constitutional governance in which there is a systematic aim for the assurance of the optimal realisation of fundamental rights. The requirement of coherence, which is still a very weighty principle in law, calls for having a look into the legal order as a whole.[44]

The construction of isolated sub-systems, which over-emphasise a particular right or utilitarian virtue, is not optimal in the wider context of assuring the efficiency and coherent application of all fundamental rights and freedoms. The natural rights paradigm or the author-centred copyright system is absolutist in terms of copyright protection. Within its field of application copyright law has absolute priority over other interests and requires efficient and over-riding protection. For such a claim there is no legal support in contemporary constitutional thinking or convincing moral justification in contemporary information ethics. It is not even supported by utilitarian welfare calculus, since chain creation and free flow of information are not easily fit into the thinking of author-centred copyright even though they are the current forms of creativity and necessary conditions for the creation and dissemination of knowledge. The author-centred paradigm sees the protection of the copyright in absolutist terms, which does not correspond to the ways in which protection of property and other rights are seen in contemporary constitutional thinking. Weighing and balancing between different rights and principles is a fundamental feature of

---

43 Guibault, *Copyright Limitations*, op.cit, p. 109, Guibault, *Nature and Scope*, op.cit., p. 1-2.

44 In Finnish legal literature there is an interesting debate between Professors Kaarlo Tuori and Thomas Wilhelmsson about the nature of general doctrines of law and the place of coherence in it in contemporary, post-modern or late-modern law. Thomas Wilhelmsson *sees* contemporary law and its general doctrines as small, empathic tales which are constructed on the contradictions and frictions of legislation and which can promote the interests of the weaker party in law. Wilhelmsson is sceptical towards the possibility of constructing major systematics and a general doctrine of law covering the entirety of private law. Tuori has criticised this way of thinking since it according to Tuori fails to recognise the significance of coherence, predictability and equality as general values of positive law and for which the general doctrines of law are important elements in the overall understanding of legal order and the guidance of interpretation of law in the concrete application of law. *See* Tuori Kaarlo, *Sosiaalisesta siviilioikeudesta myöhöismoderniin vastuuoikeuteen* (From social civil law to late-modern law of liability), Lakimies 2002, 902-013, which is a book review of Thomas Wilhelmsson's book *Senmodern ansvarsrätt, privaträtt som redskap för mikropolitik*, Kauppakaari, Helsinki 2001 and, Wilhelmsson's response in Wilhelsson, Thomas, *Yleiset opit ja pienet kertomukset ennakoitavuuden ja yhdenvertaisuuden näkökulmasta*, Lakimies 2004, 199-224.

argumentation within human and fundamental rights. Particularly, the right to property, which is the foundation of economic rights, related to copyright, is not an absolute right; indeed, there is even a responsibility towards society in the use of property. Such constitutional principles justify the doctrines of fair use and similar institutions in the application of contemporary copyright law aiming at balancing the positions of various parties' legitimate interests and contribute to the building of an ethic of information sharing.

The utilitarian model functions well in the legislative policy debate concerning the ideal model of copyright. The utilitarian model is less informative in the interpretation and application of copyright law, since in the Scandinavian approaches to argumentation in courts the argumentation may not and cannot be simply utilitarian calculus but must be bound to legal materials in accordance with the accepted models of argumentation and principles concerning the sources of law. In the legislative policy arena, the utilitarian model overtly reduces the functions of copyright to the building of welfare for the community as a whole, which may lead to giving too little latitude to individual rights and interests. The utilitarian model functions also less well as a justification of the moral rights of copyright, which have their ultimate foundation in the protection of individual integrity and personality. The utilitarian model is based on utility, it is not justice-oriented, and if wealth and welfare are not the only values, then the utilitarian model cannot stand alone as the justification and model of legal policy and argumentation in copyright issues.

The balancing model or the justice all-things-considered model fits best the requirements of overall coherence and duly taking into consideration the various aspects of different fundamental rights and legitimate interests. The balancing model also provides a functioning model for both legislation and the application of law.

The information law perspective on copyright policy and copyright law aims, thus, to promote the reading of copyright in the light of balancing between various interests. The tragedy of contemporary copyright law is that it often inherently adopts the author-centred paradigm either straightforwardly as a requirement of fundamental rights or international copyright conventions or principles of justice, or, as the consequences of the utilitarian model of computing the overall welfare interests of society. The weakness of the balancing model follows partly from the difficulties around it and from the fact that on the international level there is no clear consensus on the correct balance between copyright and its limitations and exceptions. Information law as a paradigm of law then calls for a critique of thinking and for opening the argumentation and perspectives to recognise the various other interests related to information. In the situation where ICT and the resulting digitalisation have changed radically the context of application of copyright law and call upon a change in law, the information law reading helps to re-establish the balance in the copyright regime and thereby contribute to the formulation and realisation of informational justice.[45]

---

45 On the need to re-establish this balance in times when there is an expansion of copyright, *see e.g.* Guibault, *The Nature and Scope*, op.cit.

Notwithstanding the different paradigmatic models of justification and in view of the systematic centre of copyright, there are some commonly agreed foundations for the freedom of information and free flow of information in the system of copyright. According to the Bern Convention for the Protection of Literary and Artistic Works, copyright protects expressions of creative works, not information as such. The 1996 WIPO Copyright Treaty does not aim to alter this fundamental point of departure in copyright law. Article 2 of the WIPO Copyright Treaty states that copyright protection extends only to expressions, not to ideas, procedures, or the method of operation or mathematical concepts as such. The rationale of this rule and distinction is very simple: the copyright protection covers a particular form and expression, constructed in a work, not the information itself, which is supposed to flow freely. Works are the media-carrying information, and, thereby protection of works with limitations also promotes the production and flow of information.

The expansionist reading and application of copyright and related rights seems, however, to currently threaten this point of departure and dilute the principle of free flow of information. The *sui generis* right to databases in European Community law according to Directive 96/6/EC protects mainly significant investments in the creation and collection of vast amounts of new data. The protection is mainly for the investment, not the appearance as such. An expansionist application of the criteria of substantive investment may lead to protection of information itself under the Databases Directive and, this may limit even significantly the freedom of information and free flow of information.[46] There are also trends within copyright law itself, which read the criteria of creativity in the light of investment and therefore, copyright approaches unintentionally the protection of information model.

A particular challenge to the freedom of information and to its free flow of information corollary arises from the legal protection of technological protection measures. In Article 11 of the WIPO Copyright Treaty and in Article 6 of EC Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, hereinafter the INFOSOC –Directive, there is a requirement to give effective legal protection against circumvention of technological measures which the copyright-holders use in order to prevent unauthorised use of protected works. Technical protection measures enable holders of the copyright to protect information even beyond the protection of copyright under the law and thereby change the copyright balance by denying access to works in situations, which fall under the copyright limitation. In that case the protection of anti-circumvention measures creates *de facto* a new right for the copyright holders to create by contract additional, protected property rights. There has been quite a lot of concern and debate about this risk,[47] and these concerns had some impact on the formulation of Article 6

46 There are already concerns about this, *see .e.g.* Maurer, Stephen M., Hugenholtz P. Bernt & Onsrud Harlan J., *Europe's Database Experiment*, Science 2001, 789-790.

47 *See, e.g.* Viceca Still's article in this volume of Scandinavian Studies in Law, and, Still Viveca, *Copyright in a Networked World - A Barrier to the Free Flow of Information?* in K. Brunnstein, P.P. Sint (eds.): Information Property, Intellectual Property and New Technology. KnowRight 2000 and Info Ethics 2000. Proceedings of the International Conference KnowRight 2000 and Infor Ethics 2000. Vienna 25th - 29th September, 2000.

of the INFOSOC –Directive. Article 6 (4) of the Directive seems to encourage a culture of ethics of information sharing on the basis of voluntary arrangements of the copyright holders in order to safeguard the interests underlying the limitations and exceptions to copyright. The article even seems to develop a copyright regime towards a limited application of the universal information service in which the right holders may be ensured a certain minimum level of service guaranteeing access to information falling under the protection measures. Member States have an obligation to promote such arrangements and they must act if there are not voluntary arrangements leading to the appropriate taking into account of the rights of access and use referred to in certain copyright limitations.[48]

According to the Government Proposal for the implementation of INFOSOC –Directive in Finland there would be an obligation for right holders to provide for access in certain cases if such access is not possible due to technical protection measures. The access provision obligation would be applied mainly for the benefit of certain public institutions. Eventual disagreements would be solved in the arbitration procedure.[49]

2.6 Towards Universal Freedom of Information as a Principle of Informational Justice and Fairness

The right to information, freedom of information and the free flow of information are general meta-level rights and principles of law. Strong institutions and fundamental rights implementing this constitutional-level legal solution are in the Scandinavian legal systems the right of access to documents and information held by the public administration, the fundamental right to freedom of expression and exchange of information as part of that (right of communication), protection for the free flow of information under a copyright regime and the general right to information concerning the purposes and contents of processing of personal data under the laws concerning the processing of personal data.

General information law seems to be evolving towards a wider right of access and freedom of information concerning the private sector as the fundamental requirements of informational justice and social responsibility and fairness in the markets. Fairness as a principle of justice requires a certain balance of informational positions and, particularly, the prohibition of abusive use of informational advantage to the detriment of the right of fair participation in the market and society. In the markets and under private law, the establishment of

---

Österreichische Computer Gesellschaft 2000, p. 23-31, Still Viveca, *Informationens fria rörlighet ur upphovsrättsligt perspektiv*, Oikeus 2000, p. 398-414, Still Viveca, *Oikeuksien hallinnointi- ja suojajärjestelmien sääntelystä ja vaikutuksista osapuolten oikeuksiin ja velvollisuuksiin,* Edilex 19.9.2001, and Koelman K.J., *A Hard Nut to Crack: The Protection of Technological Measures*, European Intellectual .Property Review, 2000, p. 272-288.

48 *See* recital 51 and Article 6 (4) of the INFODSOC–Directive.

49 *See* Government Proposal for the amendment of the Copyright Act and Chapter 49 of the Penal Code, HE 28/2004 vp, op.cit., detailed motivations of 50 c §, p. 127-128, and the proposed new Section 50 c of the Copyright Act.

informational advantage and use of informational power to one's benefit are accepted and even promoted as an incentive to efficiency, creativity, innovation and competitive advantage. There is no general requirement of sharing information and the choice between the open-sources types of software and materials and protected materials should remain within the individual autonomy of each user and participant in the markets. But certain fundamental principles concerning the fairness of participation in the markets require even the establishment of rules and principles concerning the use of informational power and conduct to deal with informational asymmetries in which one of the parties has a significant advantage in access to relevant information.

General economic law and, in particular, general and particular competition law provide a framework within which the informational asymmetries are balanced to correspond to general requirements of fairness. Thus, a general principle of law of marketing obliges the marketer to give sufficient and correct information about the product, and, in consumer marketing this requirement means that sufficient information about contractual conditions and the quality and usability of the product itself shall be given. Sufficiency of information is measured against the needs of the economic security of the consumer. Financial markets law requires prompt disclosure of facts and events having an impact on the financial markets on a fair and equal basis and prohibits the use of insider information. Prohibition of the use of insider information in the financial markets represents a wider principle of informational fairness. ICT as such does not change these principles, but their implementation alters the ICT-based working environment in which the ICT also provides the media for providing efficient access to information when disclosure is required. The user interfaces shall also provide optimal conditions for access to and understanding of information so that the principles of marketing law and consumer law are optimally realised. The implementation of these legal principles becomes, then, a question of information policy and management of business and of interface design and management in the e-commerce and investor relationship applications.

In the ICT-based network environment the standards concerning the network, the software code and the configurations of the hardware, that is, the infrastructure and system architecture, provide the *de facto* determinant elements of law. The code and system infrastructure become the *de facto* law. In such an environment, control over the standards and also market-based *de facto* standards is assuring the inter-operability of different applications. Configuration and inter-operability become necessary elements of informational fairness and efficiency of competition in the markets. Here information law concerning ICT systems and applications and competition law will increasingly converge to control the fairness and efficiency of basic technical conditions in the markets of ICT products and services and in the information and communication markets based on those products and services. The access to code and sharing of information necessary to establish inter-operability and efficient functioning of the markets becomes, then, legal institutions with which the fairness of *de facto* standards can be controlled.

The case *Microsoft v. Commission* in the European Courts, following Microsoft's appeal of the Commission's decision on the abuse of market power

by Microsoft will be the first significant test case of this approach in Europe. This case is very much about the nature of remedies, which can be used to ensure efficient competition, as well as about the nature of user interests. The Commission's decision ordered Microsoft, *inter alia*, to share some parts of its business secrets and intellectual property with its competitors in order to assure inter-operability of Microsoft's operating system and applications developed by its competitors. Microsoft denies the power of the Commission to use this kind of remedy and argues for much more extensive protection of its intellectual property.[50]

At least in principle the European Court of Justice has already stated in its case law that the principle of prohibition of abuse of dominant position and restriction of competition applies also to the restrictive or abusive use of intellectual property in exceptional cases even though the exclusivity of right is the core meaning of copyright and other intellectual property. According to established case law the refusal by an undertaking which owns a copyright to grant access to a product or service indispensable for carrying on a particular business is to be treated as abusive, if the following three cumulative conditions are satisfied: Firstly, that refusal prevents the emergence of a new product for which there is a potential consumer demand. Secondly, refusal is unjustified, and, thirdly, refusal excludes any competition on a secondary market. These are sound principles and correspond to the general principles of law and prohibition of the abuse of rights.[51] The efficiency of the markets and the required informational fairness warrant that the abusive positions by *de facto*, market-based standards should be subject to control by competition law. The most efficient remedy in such situations is access to information enabling inter-operability and fairness in the markets. In principle such a principle should therefore be recognised.

2.7 The Right to Information in the Design of ICT-systems and Software and in Information Management

The right to information and freedom of information are not just broad legal principles systematising legal norms or providing arguments for legal policy but

---

50 On the Microsoft case, *see* the Commission decision COMP/C-3/37.792), the publication of unofficial text of the decision without confidential elements, in document C(2004)900 final, available at the www-site of the Directorate General for Competition of the European Commission at the general gateway of the European Union, "http://www.europa.eu.int". On the Commission's arguments and approach, *see e.g.* speech by Mario Monti, Member of the Commission in charge of competition, SPEECH/04/212, 29.4.2004, and Commission MEMO/04/70, 24.3.2004. available at Rapid –database at "http:www.europa.eu.int". On the reactions of Microsoft, *see* Microsoft Reaction: European Commission's Decision in the Microsoft Case and its Implications for Other Companies and Industries, 21.4. 2004 available at "http://www.microsoft.com/presspass/legalnews.asp".

51 On the European case law *see, e.g.* judgments of the European Court of Justice in Case 238/87 Volvo [1988] ECR 6211, paragraph 9 and Joined Cases C-241/91 P and C-242/91 P RTE and ITP v. Commission (Magill ') [1995] ECR I-743, paragraph 50, and recently, in Case C-418/01IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG, Judgment of the Court (Fifth Chamber) of 29 April 2004, not yet published in ECR.

also legal and ethical principles guiding the design and management of ICT infrastructure. Explicit legal rules concerning planning, design and management of information and documentation architecture of the public administration are found in the provisions of Section 18 of Finland's Openness Act. Section 18 of the Openness Act establishes a general principle that access-to-information rights and other rights concerning information and information processing shall be taken into account in the planning, design and operation of ICT infrastructure and information management in general. Section 18 establishes some particular planning and documentation requirements in order to realise in practise the general principle of designing and maintaining infrastructure and adopting daily information management practises which provide material conditions for easy and efficient access-to-information.

In addition to particular legal requirements concerning good information management and publicity-friendly information and communication infrastructure, the principles of the right to information and freedom of information define some of the essential aspects of good software and other application design and design of information infrastructures in general. The right to information is a particularly important aspect of the user-friendliness of information systems and software. A user should be able to control his software and other applications and, therefore, he shall have easy access to information about the useful functions and side-functions of the application and also concerning the level of security and principal risks of operating the application. Access to such information is also a major element of information security since the hidden functions of software are one of the biggest information security risks. A user's right to information concerning the features and functions of the application is, thus, a criterion of quality of software. The right to information is realised, in particular, through the user interface. In the design of the user interface, the user's right to information is a key factor of user-friendliness.

3 The Right to Information Security

3.1 Evolution of Information Security: Towards a General Principle of Law in Network Society

The evolution of information security highlights very well the technical, economic, social and legal changes related to the gradual but rapid development of network and information societies. Today we are at the edge of new needs for information security in which security governance and security thinking must enter a new phase and respond to current and future challenges of information security. Security is a whole, an overall feature embedded in culture, governance, systems and practises.[52] The perspective and terminology are moving from data security to information and network society, highlighting the

52 OECD Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security. OECD Council Recommendation adopted in the 1037th session of the Council, 25.7.2002, chapter I, Towards a Culture of Security.

needs and realities of network society.[53] Prior to the emergence of the Information Age and network society information security, tacit knowledge was embedded in good professional practises and in several rules and institutions of law. As tacit knowledge, information security was not documented and conceptualised, it was not solely practical skills, thus, it was an example of what in philosophy is called *fronesis*. With information and communication technology and, particularly with the emergence of computers, data security becomes an explicit subject of knowledge, science and technology and management. At the beginning and to some extent currently data and IT security was mainly focused on treatment of individual vulnerabilities in isolated computers. Now security measures increasingly focus on building in information security as part of the information infrastructure and architecture and creating a comprehensive culture and management of security. The expertise of information security becomes and must become increasingly proactive and multi-disciplinary given that security governance must address various issues and problems having an impact on the level of optimality of security culture. Expertise and the science of information security become not only explicit but also increasingly multi-disciplinary.

A constant feature and aim of information security is its tacit and nowadays explicit and reasoned addressing of informational risks. Law is one of the oldest tools of risk management. Information security has long been a tacit institution and principle of law, and a tacit good promoted by legal rules. Information security is among the rationales of many old legal rules, notably in the private and public law rules concerning the requirements of form for various legal transactions, in which the requirement of form served among other things to secure documentation, that is evidence security, of the most important legal transactions. The Criminalisation of forgery has long served the integrity and authenticity of public and private documents. Presumptions are also a very old legal technique to share the burden of informational uncertainty and establish a solution in a situation in which there is no conclusive evidence on an issue. Information security was as such a part of the tacit knowledge of lawyers and a tacit virtue and legal good inherently promoted and protected by law.

The evolution of the stance of law and legal regulation to information security follows the same path as the evolution of science, technique and management of information security. Firstly, information security becomes explicit in the technical domain and the law had to take a position concerning liabilities of information security failures and their significance in legal evaluation of practical situations. At this stage information security had not yet emerged as an explicit rule or principle of law, technical security and legal principles; ultimately, legal certainty and justice still remained separate. The classical conception of the rule of law and the paradigmatic models of public law and private law did not require explicit regulation of information security; it was a technical issue internal to administration or to the duty of care and the

53 Following the line of the OECD Guidelines for the Security of Information Systems and Networks, the Regulation No 460/2004 of the Council of the European Union adopting the European Network and Information Security Agency ENISA uses the terminology of information and network security.

contractual loyalty of the other contracting party. However, in legal practise the duties of information security were increasingly seen as responsibilities following from the requirement of legality, the obligation to perform contracts as agreed or the particular duty of care requirement in payment transactions. Information society and network society have led to overall juridification of information security with an expansive number of explicit information security rules in positive law. While the dependency on ICT has grown and the situation of individuals and organisations and communities of individuals and organisations have become increasingly centred on the use of ICT, information security has become protected by the constitution. Information security is attached as a necessary precondition to several fundamental rights and freedoms and, as such, the regulation and promotion of information security is an explicit duty of the legislature as part of constitutional obligations to assure efficient application of fundamental rights and freedoms. Legal certainty, justice and technical security start to concur, or, at least, there is an increasing need for such concurrence.[54]

The change from passive and reactive and solely technical security to the conscious construction and evaluation of a comprehensive culture of security which is called upon in the new OECD guidelines of information systems and network security, entails the change of legal regulation, standardisation and best practises on systems design and management, all of which are ofinterest to information law. New information law provides a rule of law perspective and a risk management perspective to the creation of the new culture of security with its various components.

Today information security is among the fundamental principles of information law. Information security is an important meta-right in network society; we have as individuals and as members of a community the right to an adequate level of information security and to an optimal culture of information security and management of information security. Information security also represents a new kind of infrastructure rights following the positive juridification of infrastructures. Individuals and the community as a whole do not only have rights in the form of claims and obligations and protection in direct relationships between other individuals and the government and its agencies, but, also legally-protected expectations as to how their interests are taken into account in organising the management and functioning of private and public entities. Evolution and establishment of information security as a legal principle and meta-level legal right is part of a wider movement towards a law-based definition of good governance as a collective and individual right and the particular expressions of the requirements of good governance such as the principle of sound administration, good information management practise and good information processing practise.

---

54 This is, nevertheless, new thinking in practise, since in many areas the security ideas and fundamental rights appear as adversary, or, even opposite and contradicting goals. On the need for new thinking on the relationship between security theory and practise and fundamental rights, particularly privacy, *see* OECD, Working Party for Information Security and Privacy, Peter Hope-Tindall, Bio-metric based technologies, OECD document DSTI/ICCP/REG(2003)2/FINAL.

3.2 Constitutional and Fundamental Rights Underpinnings of Information Security: Towards a Right to Secure Identity and Integrity

The ICT-based information and communication networks are the common environments in which the meta-level right to information security is realised. The terminology of network security is in this sense justified and, it underlines the change from isolated security issues to a wide and comprehensive, ultimately ethical and cultural, issue of society for which everyone is in his own role and capacity responsible. In the information law context, however, the term information security is sufficient and broader than the term network security, covering also the security issues and interests of non-networked information resources. In information law, reading the principle and meta-right of information security always entails network security when there is a connection or exposure to effects and risks of networks.

Information security as a legal principle provides a comprehensive view and theory of various dimensions of information security and it captures the different layers of information security in the legal order. Information security has constitutional underpinnings; it is a corollary of fundamental rights and freedoms and as such a second-level fundamental right. Information security is also part of information and network ethics in which the principle and meta-right of information security represents a practical application of an ethics of encounter, the meeting of various individuals and communities and their legitimate expectations and the taking of them duly into account without silencing them. Information security is part of the information and network age concept of ethical responsibility. There are an expanding number of general and particular provisions of law explicitly concerning information security. Information security is a genuinely multi-disciplinary issue and virtue, which has the governance and risk management dimension, technical design and management dimension and the general management, responsibility and cultural dimensions. The information security rules contribute and aim to make an impact on all these dimensions and, provide a particular, statutory method to align security thinking and measures with fundamental rights and freedoms and with risk management.[55] Information security rules are part of a wider governmental policy of information security and they support and make an impact on organisational information security policies. Because of these wide functions and objectives of information security rules and of the multi-disciplinary nature of understanding the phenomena of information security, the reading and understanding of information security rules requires knowledge about general theory and doctrine of information security. The principle of information security with its various components and corollary principles, and the wider conceptual and paradigmatic framework of information law provide a context in which those norms become part of a dynamic system and understandable in practise.

---

55 Many information security rules are good examples of the teleological use of law and regulation, in which law is legislated and consciously used to solve a particular social problem and thereby promote the social effectiveness of a policy.

At the constitutional level, information security is part of a wider right to security and identity guaranteed in Article 5 of the European Convention on Human Rights and in Article 6 of the EU Charter and in Finnish law in Section 7 of the Constitution, which together comprise necessary requirements for the effective protection of human dignity, integrity and personal liberty. The right to security is an individual right related to the liberty and integrity of an individual, which is recognised in Article 3 of the EU Charter. Mental integrity means the security of the person from intrusions, which prevent or endanger an individual's right to use his public or private self-determination, including the rights to collect and use property and seek and use information in public and private communications. Information security is also a necessary condition for the right to identity, which according to the established practise under Article 8 of the European Convention on Human Rights is part of the concept of the right to private life. In the context of ICT-dependent network society, the right to identity, when read together with the right to security and integrity, develops towards a general right to secure identity. Information security transfers from a mere technical and management issue to become a fundamental right and principle of law of a fundamental nature.

Information security also has close underpinnings in other fundamental rights as a necessary condition and element of the efficient assurance of adherence and protection. The right to confidentiality of communication, guaranteed in Article 8 of the European Convention on Human Rights and in Finnish law in Section 10 (2) of the Constitution requires an adequate level of information security in paper-based, analogue and digital communications. The same applies to the right to property when the property is in the form of informational and intangible assets in the network environment. The promotion and safeguarding of the minimum level of information security becomes, in the ICT dependent context of network society, a particular obligation of public powers under the general duty to assure and promote respect for fundamental rights and freedoms. Information security is a technical and managerial necessity and duty but also an obligation at the level of legislative policy, policy drafting and the general guidance of society. As the procedures of society and public participation are increasingly transferred to networks or based on ICT applications, information security becomes a condition of fair trial and participation, and, ultimately, part of the reasoned, legitimate trust in the governance and functioning of the markets.

3.3 Definitions and Underlying Theory of Information Security

There are several technical and, following the juridification of information security, legal definitions of information security. These represent two slightly different schools of thought in terms of emphasis in the security definitions and underlying security theory. The first one emphasises the resistance of ICT systems to different accidental failures and malicious activities and defines the management dimension of information security as the prevention of such threats and the building up of a resisting capacity. Definition and theory is, thus, centred on the concept of threat and ensuing risk analyses. The second approach defines

information security as a state of the world in which security parameters have been reasonably assured. In this approach information security approaches the overall criteria of quality of information systems. The difference between definitions and schools of thought are, in terms of definition, mainly in the emphasis, but symbolically and in management practise the difference is significant. The first one leads to a negative concept of security and to a more narrow approach to security culture as the prevention of certain negations of normality. The legislative model for this kind of approach is centred on the criminal law measures protecting information security as a legal and social virtue and good. The latter one is difficult to distinguish from the general criteria of quality and good conduct, but provides a theoretical framework for integration of security features with the principles of efficiency and wider respect and implementation of fundamental rights and freedoms. The legislative model for this approach is the principles of good data processing practise and associated information security obligations in the laws concerning processing of personal data.

There is a fairly common understanding that the fundamental parameters defining information security are availability, integrity and confidentiality of information and the ICT system. In the communications and network context authenticity is defined as an additional parameter, sometimes together with non-repudiation. Information security is always also a function of legitimate, that is, reasonable and objectively founded trust in certain qualities of information and the functioning of ICT systems and networks. Auditability becomes then also a parameter of information security, and connects information security to other fundamental principles of information law, such as the right to information. There is an evolution noticeable in the thinking of information security and in the definition of it in official policy documents. Confidentiality was initially defined as the first criterion of information security.[56] Early thinking on information security centred on technical access controls for which information security is often also confused with data protection in the sense of technical protection of data. The over-emphasis of the early information security practise on confidentiality has been for a fairly long time a subject for critique.[57] Following criticisms and the development of practises and security needs in network contexts, increasing attention has been paid to integrity and authenticity dimensions and to availability and usability. Following the European Commission communication on the European approach to information and

---

56 Influential early definitions of the criteria of information security are, among others, Parker, Donn P., *Fighting Computer Crime*, Charles Schribner's Sons, New York, 1983. The contents of Donn P. Parker's definition of information security is discussed and developed in further detail in the information security report of the Institute of Law and Informatics of the University of Lapland, *see*, Saarenpää, Ahti & Pöysti, Tuomas (eds.) & Sarja Mikko, Still, Viveca and Balboa-Alcoreza, Ruxandra, *Tietoturvallisuus ja laki*, *näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä*, Valtiovarainministeriö, hallinnon kehittämisosasto ja Lapin yliopiston oikeusinformatiikan instituutti, Helsinki 1997, p. 54-74.

57 On this criticism to which Scandinavian legal informatics made significant contributions, *see, e.g.*, Nordic Council of Ministers, *Information Security in the Nordic Countries*, Nordiske Seminar- og Arbejdsrapporter 1993:616, to which the Norwegian Research Center for Computers and Law contributed.

network security, European policy documents and legal rules have defined availability as the first criterion of information security, thereby underlying the availability, usability and user's perspective as fundaments of security culture and management.[58]

The European Parliament and Council Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency, called ENISA for short, (hereinafter the ENISARegulation) defines network and information security as ''*the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems*''.[59] Availability means here the availability of data and the operationality of services.[60] Authenticity means according to the ENISA Regulation confirmation of the asserted authenticity of entities or users.[61] Data integrity means that the data, which has been sent, received or stored, are complete and unchanged.[62] Data confidentiality means according to the ENISA Regulation the protection of communications or stored data against interception and reading by un-authorised persons.[63] Definitions in the ENISA Regulation seek to give a brief understanding of what network and information security and its main elements are for the practical purposes of defining the tasks and powers of the European Network and Information Security Agency. Information security is defined there as a function of risks, threats and losses where threats are presented either as accidents or malicious and or unlawful activities. The definition is fairly narrow even though it is informative. It is part of the security tradition in which the security measures aim to counter defined threats and risks, that is, by sanctioning with norms and security standards and other measures abnormalities and exceptions regarded by definitions to represent harmful issues. This approach of negation and focus on abnormality has the weakness of casting a shadow over the positive facets of information security. Information security has an important positive function among the foundations and promoters of the smooth running and continuity of operations and, ultimately the informational foundations of democracy and use of fundamental rights and freedoms, including the right to integrity and a secure identity.[64]

---

58 *See* COM (2001) 298 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Network and Information Security: Proposal for A European Policy Approach.*

59 European Parliament and Council Regulation (EC) No 460/2004 on the establishment of the European Network and Information Security Agency, ENISA, definition in Article 4 (c).

60 Definition in Article 4 (d) of the ENISA Regulation.

61 Definition in Article 4 (e) of the ENISA Regulation.

62 Definition in Article 4 (f) of the ENISA Regulation.

63 Definition in Article 4 (g) of the ENISA Regulation.

64 The traditional definition of information security through threats and vulnerabilities has been criticised by Timo Kuronen in his excellent short study on the role of informational resources and information stores to democracy, *see* Kuronen, op.cit.

In a more positive definition, information security is understood as an optimal state of the world in which the whole is constituted from the realisation of the fundamental parameters of information security. Information security is never perfect in a practical world, and, it may be argued that perfect information security is even an impossible fiction in theory after all things contributing to it are taken into consideration and security is not suppressing other important interests, virtues and values. Imperfection and a certain scarcity are natural features of information security. Nevertheless, the definition of information security as an optimal state of affairs provides a normative ideal, which is just as important as the definition of objective criteria against which the level of security is measured. The challenge is to manage the imperfection and arrive at the optimal balance between security and the costs of security measures in which there is a reasonable level of security at reasonable costs and burdens.

The definition of the criteria of information security shall also include the protection of legal rights and legitimate legal interests related to information, information processing and communication. Information law aims at a general and particular, situational understanding of information security and its constituent parameters which incorporates into the security concept itself the fundamental values of a material rule of law. The OECD has defined nine principles of information systems and network security. The integration of the rule of law with the concept, culture and management of security is not explicitly provided for in the titles of the OECD information security principles, and, thus, on the surface the principles tend to continue along the line in which legal principles and security were seen as distinct factors. However, one of the security principles is the principle of democracy. It requires the compatibility of security measures with the requirements of democracy. The explanation of this principle connects clearly information security to fundamental legal values and principles such as the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, and the appropriate protection of personal information, openness and transparency.[65] In addition, the principle of ethics further strengthens the demand for integration rights and fundamental legal principles to the information security concept and culture.[66] The information security concept, security management and the resulting security culture support and promote the principles of good constitutional governance which is a wider aim of the evolution of the rule of law.

Information security can, in the doctrine of information law, be understood as a state of affairs in which the availability, integrity, authenticity and confidentiality of information, information processing and communication is sufficiently and reasonably assured taking into consideration the risks related to information and its processing and communication in various circumstances and duly taking into account the legal rights related to information, information processing and communication. In the strictly legal and ethical sense,

---

65 *See* the OECD Guidelines for the Security of Information Systems and Networks, op.cit., principle 5, democracy.

66 *See* the OECD Guidelines for the Security of Information Systems and Networks, op.cit., principle 4, ethics.

information security refers to obligations and responsibilities related to the assurance of availability, integrity, authenticity and confidentiality. A sufficient and reasonable level of security means tolerance against failures and malicious activities and the continuity of operations and the safeguarding of legitimate interests both in normal and exceptional situations. The level of information security shall be auditable, which means that it should be possible to verify by objective means what the level of security is. Information security shall, thus, not be based on mere trust but on reason. Auditability connects information security to another fundamental principle of information law, the right to information. Each user has the right to information concerning the functions of the ICT system and network, and a secure system should not be allowed to perform functions without the possibility of the user to observe the processes of the system. A user also has a right to be duly informed about the functions of the system and the general level of security.

Availability means the technical, administrative and even legal accessibility of information and communication and the technical usability of information, information processing and communication for defined purposes. Usability opens the availability towards wider criteria of good quality information processing and information management in which there are efficient tools for information processing and management. Availability requires in the Information Age, in which the systems are complex and there is a general overflow of information, the availability of sufficiently good meta-data and meta-information about the information and search and identification tools and tools of structuring. The continuity, inter-operability and availability of program updates and support for media formats are also an important element of availability. Availability means that information and information processing shall be usable at the requested time. The response time of the system falls within general criteria of usability but the basic level of response is also an element of information security. In the legal dimension, availability means that the rights to information and communication are duly taken into account, and, that information and communication and the systems of processing are available as required by the legal rules and principles.

Integrity means the technical and logical correctness of data, completeness of information and that information has not been altered in an unduly and uncontrollable way. Integrity means also that information is up-to-date and that the different versions of data are controllable and not confused in an uncontrollable manner. Integrity requires, thus, the controllability of information processing and functions of ICT systems.

Authenticity is a feature close to integrity. Authenticity means reliable identification of the source or the unaltered nature of data. Non-repudiation, which means legally reliable proof of actions in an ICT system and ensures that a significant action cannot be denied of its existence, is also closely related to authenticity. Authenticity and its corollary non-repudiation aim often at securing evidence and documentation (evidence security) in the legally relevant transactions. Authenticity is also an important security feature in governmental information systems granting access to official information. For example, authenticity is a key quality factor and criterion for reliability in storing and disseminating legal information.

Confidentiality in the technical sense of the term means that information, communication and information processing (ICT system) remain only at the disposal of those who have due authorisation and that processing is done only for the purposes for which processing is authorised. In the legal sense, confidentiality means the protection of the various exclusive rights to information and information processing and the safeguarding of the confidentiality of communications. The rules on access, secrecy, confidentiality and purposes of legitimate processing define thus the sphere in which the information system may be accessed and which operations each user may perform within his profile and role.

Information security is also an ethical requirement, a part of individual and community information and network ethics. The OECD guidelines on ICT systems and network security define ethics and responsibility as fundamental principles of information security.[67] Law is in mutual interaction with morality and ethics, and, law incorporates and institutionalises particularly through its principles the requirements of morality and community and individual ethics. Information law is, within the institutional support and acceptance given by positive law, a body of essential requirements of information and network ethics. Information security as an ethical requirement and principle means that all participants in ICT use, design and management take duly into account the legitimate interest of others and act in a responsible manner.[68] The OECD principles seem to aim at achieving a meta-ethical encountering of the legitimate interests of different participants. Information security is a practical ethics of encountering, which aims to ensure that the rights and legitimate interests of other humans are duly taken into account, without suppression and narrowing of the perspective and without proper consideration of the other, in all activities related to the information and communication system design, management, use and governance of ICT, information processing and communication. To such ethics of encountering belongs also the responsibility of everyone for his actions and inactions, according to everyone's individual capacities, powers and roles.[69] Information security is a practical ethics of encountering, which aims, in particular, to overcome the situational or intentional scarcities of perspective and attention. These lacks of perspective and attention lead to scarcities of law and justice in the governance, design, management and use of information systems. Scarcity of law and justice means here obstacles to proper and efficient implementation of the requirements of law and good ethics of information, and consequently obstacles to achieving and limitations of informational justice.

---

67 OECD Guidelines, op.cit., principle 2, responsibility and principle 4, ethics.

68 OECD Guidelines, op.cit., principle 2, responsibility, principle 3, response and principle 4, ethics.

69 The concept of ethics of encountering and its connection to the ideas of responsibility are taken from the philosophy of Emmanuel Lévinas, *see, e.g.*, Lévinas, Emmanuel, *Autrement qu'être ou au-dela de l'essence*, initial publication the Hague 1978, edition cited Le Livre de Poche – Essays 2001, Dordrecht 2001, passim. and particularly p. 15-16, 22-25 and 214-219.

3.4 Systematics of Principal Information Security Provisions in European Legislation

The number of general and particular, specific provisions of information security seem to be constantly rising as network and information society develops. The same applies to contracts concerning information security. The strategic importance of information security and information as such requires that there are contractual arrangements for the definition and maintenance of the adequate level of information security. The capacity to give good advice on information security contracting or contractual provisions concerning various aspects of information security and management of information security risks belongs today to the basic skills of a good business lawyer. This is, however, a skill to which traditional law school curricula do not necessarily prepare one very well. Enacted rules of law concerning information security establish either general or particular obligations of information security and thereby implement the principle of information security in the legal order, or, they provide risk management and governance tools for the management of information security and particular security risks.

Information security related provisions in the legal order could be systematised in different ways. If information law is seen following the approach taken by Professor Timo Konstari as a body of rules and principles concerning information and information processing in positive law, there are significant information security related provisions in general information law, public and private information law and in the various sectors of law such as labour law, criminal law, consumer law and administrative law. The classical, static, systematic dividing of the legal system into the different fields of law may, however, prevent us from seeing the common features and background factors, policies and aims of information security related norms and they may remain strange for lawyers and information management professionals who do not necessarily find them and keep calling for more precise laws of information security. Information law as a complementary and dynamic systematics of law, which opens information processing and communication, information and communication economics and ethics-related perspectives to the legal order, can provide a systematic perspective of making sense and dynamically applying and developing the security-related legal rules either as foundations of action and responsibility or as tools of risk and security management.

The statutory foundation of information security is general information law, particularly in informational privacy legislation. Article 17 of the EC Personal Data Directive establishes a general obligation of information security and incorporates some of the general principles of information security to the legal order. In Article 17 a general duty of technical and organisational security measures is imposed on the registrar of personal data. Since processing of personal data has a very wide definition and covers all processing of personal data by automated means, this obligation approaches a general duty of information security. Information security measures shall provide an appropriate level of security related to the nature of data and the risks involved. Security is a reasonable and proportionate function of the related risks and requires systematic risk awareness and management. Security measures and

management shall take into account the state of the art within technology, which means that there is an obligation to follow technical developments and relate risk assessment and awareness and implemented security measures to reasonable levels compared to the technologies and methods available. The costs of the measures can be taken into account. These provisions, together with the requirement of a relation between the risks and the nature of data and the extent of security measures, define the criteria for application of a general principle of proportionality in the field of information security measures.

Another important general provision of information security is Article 4 of the EC Directive 2002/58/EC on Privacy and Electronic Communications, which establishes information security as a general principle and duty in the field of electronic communications law. General principles of security are essentially the same in this Directive as those defined in the Personal Data Directive. In addition, in Article 4, co-operation with the provider of a public communications network is required, following the nature of the provision of electronic communication services in a network environment, in which the level of security depends on the action and measures of all participants and users. The providers of publicly available communication services have also a general duty of informing their subscribers about particular security risks. This duty incorporates the principle of the right to know the general level and status of security and controllability of the security level as a legal right in electronic communications. The Directive is implemented in Finland by the new Electronic Communications Privacy Act (516/2004). The provisions give to service providers and to so-called community subscribers, such as organisations providing e-mail accounts, some particular powers in relation to information security. The law authorises under some particular requirements, for example, filtering the messages and removal of messages containing a malicious code. Those measures shall be necessary, proportionate to the level of risk and threat and they may not compromise confidentiality, which means that only technical filtering is allowed but not active, human interference or the opening of messages. These provisions provide long-awaited clarifications of the powers of system operators in the face of virus epidemic and denial-of-service attacks.

In criminal law, information security is nowadays generally accepted as a protected legal good (virtue) and several information security related crime definitions and criminal sanctions aim to sanction intentional malicious activities. The Council of Europe's Cybercrime Convention means a European harmonisation of provisions concerning information security and co-operation in the investigation of information security crimes.[70] The Cybercrime Convention is, at the international level, a significant step forward in the institutionalisation of information and network security as a value protected by criminal law. The Convention contributes also to the building of good information ethics by clearly signalling which kind of actions are crimes and are to be condemned. However, the particular challenge in information security related crime is the low rate of detection and the limited ability of law enforcement and prosecutorial authorities to effectively realise criminal liability.

---

70 Council of Europe, Convention on Cybercrime (2001), CETS No 185.

Finnish public information law also contains general provisions on information security. Information security and the protection of its various fundamental components have been defined as a general duty of public authorities in Section 18 of the Openness Act concerning public information management. Section 18 requires also some particular plans for the assurance of information security. Information security is explicitly also incorporated as a general principle in the Act on Electronic Communications with Public Authorities (13/2003). These acts represent a general, international trend in which the e-government acts and/or the freedom of information acts and privacy legislation evolve towards general acts of information security.

4 Conclusion

This short review of the principal meta-rights of the right to information and freedom of information and information security is illustrative of the general development of information law. It already justifies certain wider conclusions. The main result is that there are coherent and systematic tendencies towards a paradigm of information law. The emergence and evolution of information law is a key part of the legal change leading to a reinforced, material rule of law and to more efficient markets in the age of information networks.

Network society, which is based on the extensive use and dependence of ICT, information and communication, and, in which information and communication are commodities with strategic value, legal certainty and implementation of fundamental rights and freedoms face some particular, technology–related challenges. ICT and biotechnologies develop rapidly and contribute to profound changes in society. Only change and the desire for justice seem to be constant. The speed and profoundness of change require inevitably new approaches to law and regulation. Concurrently, complexity increases, which is due to the nature of the regulatory objects themselves. Law changes quickly and becomes complex. The rule of law and fundamental principles of law should also be part of the information and communication culture, information and communication policy, information management and the technical systems and infrastructure design and management. The infrastructure and its configurations, the qualities of hardware and the software code, are among the most potent methods of guidance in network society, since they define what is possible and feasible. ICT also shapes individual and community understanding of reality and, increasingly provides for the metaphors used for communication and understanding.

Change does not only concern technology, business, administration and technical aspects of regulation; change concerns the whole encountering of ourselves with others in an environment increasingly shaped by rapid changes of technology. Network society needs a paradigm of law to help both the professionals of law, ICT and management and the general public to make sense of the law and provide guidance and understanding, stability and certainty, in times of rapid changes and technical complexities. Contemporary understanding of information law and its paradigm aims to provide such a theoretical and practical perspective to law and governance.

Difficulty and complexity of legislation concerning information and communication and the application of law in that field arises from the ubiquitous nature of information and communication. Information is everywhere and there are hardly any areas in which there would not be an information perspective. Information and ICT themselves are not the decisive issues in the paradigm of information law. The paradigm of information law is centred on its fundamental principles concerning information processing, information and communication markets and communication. Information law is the fundamental-rights-and-freedoms connected order of informational and communicational freedoms and rights, and the order of responsibility, which is part of all freedoms and rights. The paradigm of information law aims to mediate between the essential values and contents of the fundamental rights and freedoms and other principles of good constitutional governance, and concretise them in the context of network society, information processing and markets and communication. The focus on the regulation of infrastructures and information and information security management, ultimately the security and information culture, is a way to provide better effectiveness to rights than in the traditional regulatory doctrines. Information law and its general principles overcome the traditional static boundaries of doctrines and provide a helpful approach to situations of convergence in which old concepts and distinctions do not work.

Implementation and promotion of fundamental rights is a specific duty of the legislature. Principles of information law guide policy foundations as legal policy objectives and principles of justification (*Rechtsgrundsatz*). In the application of law they provide a systemic perspective connecting individual, particular provisions to wider policy considerations and considerations of informational justice and information ethics. Openness to information ethics is a particular feature; information law provides a paradigmatic forum in which law and ethics converge, aiming to mutually control and enrich each other in a democratic and open dialogue. Information law itself and discussion about its general principles and their application represent, thus, a practical ethics of encountering.

An encountering of other humans and their perspectives and issues is not limited to an encounter between policy and law, justice and rules of written law, and ethics and law. Information law principles and information law in general aim at awareness-raising, informing the technical and managerial professionals of ICT and the general public about legal issues and principles of significance. The information law paradigm aims to facilitate multi-disciplinary co-operation in theory and practise between different professionals, ultimately aiming at the true encountering of different professional perspectives. By so doing the paradigm of information law aims to bring the fundamental values of democracy and integrity of humans to professional and technical cultures of various professions and organisations. The paradigm of information law is strict in requiring good scientific foundations, but, simultaneously, it is more open than the traditional doctrine of sources of law and the paradigmatic concept about the boundaries of legal science. For example, information processing standards, meta-data standards and security standards are of interest and even a source of information and law in the paradigm of information law. The reason for that opening is the simple observation that the rule of law must be written into the

code, standards, hardware and systems configurations of the infrastructure of network society, otherwise there is a constant scarcity of justice and lack of efficiency of law even though there might be plenty of legal rules.

The ICT and network society continues to develop, and so the development of information law is only at its beginning. The emergence and evolution of information law is a key part of the legal change leading to a reinforced, material rule of law and to more efficient markets in the age of information networks. Given the significance of the informational and communicational dimensions of our life and given the profoundness of change the principles and paradigms of information law merit much further consideration.