GOVERNANCE OF SOCIETAL CYBER AND INFORMATION SECURITY RISKS: HOW LEGAL INFORMATICS CAN HELP FUTURE-LOOKING LAW

Tuomas Pöysti

Dr. Tuomas Pöysti
Chancellor of Justice of the Government of Finland, Title of Docent, Dr. Iuris, Dr. Phil. (h.c.)
E-Mail-Adresse: tuomas.poysti@gov.fi

Keywords: ***legal informatics, cyber and information security, artificial intelligence, methods, post-phenomenology, European Union law, digital network society, digitalisation***

Abstract: *Over decades legal informatics has endeavoured for a deep understanding of the inter-section of law and ICT and of the risks related to digitalisation by variations of systematic multi-disciplinary studies. This quest continues. A systematic inquiry informed by legal informatics contributes to epistemic foundations to socio-legal understanding and governance of the cyber and information security risks. These risks are today shaped by the artificial intelligence (AI) and, the human - machine collaboration digital technologies increasingly enable. I will discuss current risks of digital network society with specific relevance for cyber and information security in an effort to place cyber and information security to a wider societal context and, to identify the needs of law and legislation in the future protection of human autonomy and dignity. The article discusses how the approach in the legal informatics continues to be helpful in constructing well-founded solutions to societal risks related to digitalisation in general and cyber and information security in particular by law and, hence, future proof the law. Mission of the legal informatics continues to develop intellectual foundations of both legislation and the application of the law in practise beyond individual substantive fields of law.*

1. Introduction

Twenty-five years ago in 1997 I wrote a list of the significant risks of information society from data and information security perspective. Risk mapping was part of a legal study on information security carried out at the University of Lapland together with Ahti Saarenpää, Mikko Sarja, Viveca Still and Ruxandra Balboa.[1] Study was commissioned by the Government of Finland, Ministry of Finance to have a broader view to information security and to have an informed discussion on the legislative and regulatory needs on information security. Studying information security and risks related to ICT and data processing was seen then and continues to be seen a task of the legal informatics.[2] I attach myself to the Nordic or Scandinavian tradition of legal infor-

[1] See Saarenpää A. & Pöysti T. (eds.) (1997) Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Valtiovarainministeriö ja Lapin yliopiston oikeusinformatiikan instituutti, Edita, Helsinki 1997. The study was consequential in several terms: many regulatory ideas were taken on board by the Government including information operations and warfare but one and maybe the most significant part: there is not yet a general act on cyber and information security.

[2] See Saarenpää A. & Riekkinen J. (2023) Oikeusinformatiikan perusteet. Lapin yliopisto, Rovaniemi, pp. 8–19 and 198–207. See Pöysti T. (2004) ICT and Legal Principles: Sources and Paradigm of Information Law. Scandinavian Studies in Law, Vol. 47, 559–600 on the information security as a general principle of law and as a meta-level citizen right.

matics launched by Peter Seipel, Jon Bing and Peter Blume and in Finland by Ahti Saarenpää and later his students including myself.[3]

Variations of legal informatics provides disciplined methods and research traditions to analyse interactions between data and information, information and communication technology (ICT) and law.[4] Addressing unknown terrains between law, information and information & communication technology ICT have been the benchmarks of legal informatics in the efforts to find general logical solutions to formalise legal knowledge and reasoning to computable formats, to address risks in for traditional lawyers cumbersome phenomena like predictive modelling, or to analyse and develop automated rule-making or quantitative analyses of legal materials.[5] Legal informatics is a gentle enlightener of practitioners and legislators.[6] Legal informatics acts as a conscience for the deep impacts of the ICT and data processing to law and needs of legal protection in constitutional rule of law.[7]

In this contribution I will revisit the list of risks recognised in our 1997 study on information security and I will inquire about the current socio-technical conception of risks to which cyber and information security is situated in law. On the bases of that I will ask how legal informatics in socio-legal analyses will help future-proofing legislation. While doing this I will also make observations of the journey of thinking from

[3] For a short Nordic definition of legal informatics, see Seipel P. (2005) Archives in the Service of the People. Scandinavian Studies in Law, Vol 48: 371–395, p. 372 and p. 380. For my definitions see Pöysti (2004), op.cit; Pöysti T (2006) Communicational Quality of Law – a Legal Informatics Perspective. In Magnusson Sjöberg C & Wahlgren P (eds) (2006) Festskrift till Peter Seipel, Nordstedts Juridik, Stockholm, pp. 463–493, p. 464–471 and Pöysti T. (2007) Scandinavian Idea of Informational Fairness in Law – Encounters of Scandinavian and European Freedom of Information and Copyright Law. Scandinavian Studies in Law, Vol. 50, 221–248. For the general Finnish understanding see Saarenpää A. – Riekkinen J. (2023) Oikeusinformatiikan perusteet, op.cit. See earlier version Saarenpää A. (2015) Oikeusinformatiikka in Niemi M-L., (ed.) (2015) Oikeus tänään. 3rd, revised edition. Lapin yliopiston oikeustieteellisiä julkaisuja C 63, Lapin yliopisto, Rovaniemi: pp 17–205. On the method of legal informatics see also Saarenpää, A. (2016). Does legal informatics have a method in the new network society? In Ylä-Kotola, M. et al. (eds) (2016). Society trapped in the network: Does it have a future? University of Lapland, pp 51–75. See also Saarenpää, A. (2016). Legal informatics today: The view from the University of Lapland. Lawyers in the media society: the legal challenges of the media society.

[4] Legal informatics consists of different variations of approaches and scientific endeavours from the very beginning of the continental legal informatics (Rechtsinformatik as discipline and Informatik und Recht as discussion forum) and the American tradition of jurimetrics, automation and law and computers and law, see Lukas E. (2021) Niklas Luhmann als Pionier der Informatik. In Pohle J. & Lenk K. (eds), Der Weg in die ‘’Digitalisierung” der Gesellschaft: Was können wir aus der Geschichte der Informatik lernen? Metropolis-Verlag, Marburg, pp 197–226, p. 220–221; Kilian W. (2021) Digitalisierte Informationen im Rahmen einer ITanknüpfungsfähigen Juristischen Methodenlehre. In Pohle J. & Lenk K. (eds), Der Weg in die ‘’Digitalisierung” der Gesellschaft: Was können wir aus der Geschichte der Informatik lernen? Metropolis-Verlag, Marburg, pp 303–314, p. 303–306 Allen L.E. & Engholm C.R. (1978) Normalized Legal Drafting and the Query Method. Journal of Legal Education 29:380–412 and Loevinger L. (1963) Jurimetrics: The Methodology of Legal Inquiry. Law&ContempProbs 28:5–35.

[5] See Pohle J. (2021) Eine juristische Disziplin der Zukunft – An der Schnittstelle von Recht und Infomatik. In Pohle J, Lenk K (eds), Der Weg in die ‘’Digitalisierung” der Gesellschaft: Was können wir aus der Geschichte der Informatik lernen? Metropolis-Verlag, Marburg, pp 263–294, see also Leith P. (2010) The rise and fall of the legal expert system, in European Journal of Law and Technology, Vol 1, Issue 1. See Greenstein S. (2017) Our Humanity Exposed: Predictive Modelling in a Legal Context. Stockholm University, Faculty of Law, Department of Law, Stockholm. This doctoral dissertation studies predictive modelling, which is a significant societal use of various AI techniques from the perspective of the data protection law, in particular the European Union General Data Protection Regulation (EU) 2016/679, (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88), the GDPR, but also from human rights and human autonomy perspective.

[6] A topical example of that in the Nordic legal informatics is the writings of professor Dag Wiese Schartum on digitalization friendly legislation and on the programming and algorithm development as the continuation of the work of legislator, see Wiese Schartum D (2021) Jus og digitalisering. Lov og Rett 60:92–109 and Wiese Schartum D. (2020) From Legal Sources to Programming Code: Automatic Individual Decisions in Public Administration and Computers under the Rule of Law. In: Barfield W. (ed), The Cambridge Handbook of the Law of Algorithms. Cambridge University Press, Cambridge, pp 301–336.

[7] On the function of enlightener of human rights and assisting on their constitutionalization in issues like data protection in German Rechtsinformatik –tradition and older Informatik in general, see Lukas (2021), op.cit. note 1, p. 219–221 and See Fuchs-Kittowski K. (2021) Informatik im Spannungsfeld zwischen formalem Modell und nichtformaler Welt. In Pohle J. & Lenk K. (eds), Der Weg in die “Digitalisierung” der Gesellschaft: Was können wir aus der Geschichte der Informatik lernen? Metropolis-Verlag, Marburg, pp 31–66, p. 56–58.

technical data security to societal cyber and information security currently legislated in law and unfolding in the offing.

2. Conception of Information Related Risks Underlying Law and Path from Data Security to Cyber and Information Security

The idea of the list of information society risks in our 1997 study was that through a macro-level, societal risk conception, information security could be placed into a wider context for better analyses of the future legislative needs.[8] 'Leitmotiv' of our information society risk list and the whole information security study was strikingly similar to the study carried out 23 years later by the Joint Research Centre of the European Commission: Cyber and information security is an essential societal need.[9] Regulatory theory and its conceptions of risks and the legislative studies concerning Nordic private law were taken as a primary theoretical reference for our 1997 study.[10] Following Helmut Willke we saw the role of legislator and government to provide governance and management of these risks based on law.[11] The quest for holistic approach to information security and beyond was rare at that time. In 2020s holistic approaches to cyber and information security are mainstream of cyber and information security thinking.[12] The list identified 20 risks of an information society. Risk list was a hermeneutic interpretation of the research data consisting of official policy documents and legal sources and legal literature on risks and regulation.[13]

The Organization for Economic Co-operation and Development OECD, which is influential in digitalization and information & digital security policies, issued its first recommendation on the security of information systems already in 1992.[14] Ten years later the OECD updated that recommendation and enlargened its scope of application to cover the security of information networks. Development of the OECD recommendations tells about a considerable widening of the perspective and understanding of the concept; a move from technical protection of some elements of data in an individual information system to a broad, multi-angle principle of digital security as a fundamental element of the quality of infrastructures and services in society.[15] In 2003, the OECD published an extensive assessment of emerging Systemic risks in the 21st century. Report discussed large-scale risks and analysed changes in the quality and spreading of risks and the needs for new perspectives in risk management at the societal and international level.[16] Differentiation between systematic risk and systemic risk are essential in law, policy and management. Systemic risk generally refers to a situation where a vulnerability or disruption extensively spreads in networks and causes serious problems to the functioning of an entire sector or the society as a whole.[17] An individual design or underlying thinking failure or vulnerability

8 Saarenpää & Pöysti (eds) (1997), p. 23–25.

9 See Nai Fovino I. et al. (2020) Cybersecurity, Our Digital Anchor. European Commission Joint Research Centre, Science for Policy Report, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, JRC121051.

10 See Saarenpää & Pöysti (eds) (1997), pp. 5–9. See Ogus A. (1994) Regulation – Legal Forms and Economic Theory. Clarendon Press, Oxford. Hellner J. (1990) Lagstiftning inom förmögenhetsrätten – Praktik, teori och teknik. Juristförlaget, Stockholm, p. 135–155.

11 See Willke H. (1992) Ironie des Staates. Grundlinien einer Staatstheorie polyzentrischer Gesellschaft. Suhrkamp, Frankfurt am Main. Saarenpää & Pöysti (1997), pp. 19–20.

12 See, for example Nai Fovino I. et al (2020), op.cit. and concerning the emerging concept of smart cities Hernandez-Ramos J.L. *et al*. (2021) Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions. In IEEE Security & Privacy, vol. 19, no. 1:. 12–23.

13 Saarenpää & Pöysti (eds) (1997), p. 26–48.

14 OECD, Guidelines for the Security of Information Systems, 1992, https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm (visited 20.12.2022).

15 Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. OECD/LEGAL/0312.

16 See OECD (2003) Emerging Risks in the 21st Century. An Agenda for Action. OECD, Paris.

17 Concept of the systemic risk is mainly developed in the theory and regulation of financial markets and in the Union law systemic risk is defined, for example, in Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing

or programming error or pertinent human skills or attention problems are sources for systematic risks leading to repeated security incidents or other harmful events.[18]

Unknown, complex and turbulent problems may have wide consequences and for which new kinds of governance approaches are needed. These problems have become increasingly visible.[19] Challenge and possibility to cyber and information security follows from an increasing human – machine – confluence and collaboration. Security relies there partly on automatic monitoring. Human – machine interaction can be a significant source of vulnerabilities and security incidents. In that some traditional human controls simply would not work any longer.[20]

OECD changed its information security recommendation into a recommendation on digital security risk management in order to promote social and economic prosperity in 2015. This signals a final turn from a technical issue related to availability, integrity and confidentiality of information systems and data to a wide and inter-connected societal and economic issue. Cyber and information security is a multidimensional issue with individual and organizational micro-levels, administrative branch or subsector of society wide meso-level and whole-of-society macro levels.[21] Later OECD updated recommendation on the protection of critical infrastructures.[22] In 2022 the OECD adopted a package of four recommendations on various aspects of digital security updating or replacing earlier policy instruments and underlining digital security as a strategic whole-of-society and whole-of-government issue. Underlying ideas are the inter-connectedness of digital security and the need to develop trust to and within the digital environment and the embed balanced equilibrium between usability and security by security-by-default to infrastructure and product and services of digital society. Cyber and information security is a fundamental quality element of all infrastructures.[23]

The role of law extends and the law as a system of society reaches beyond the issues of regulation and governance: law is an institutional system representing and realising liberty and justice.[24] The legislator reacts to risks and uncertainties by principles and rules on risk-sharing and by setting specific risk management and compliance requirements as legal duties. The EU General Data Protection Regulation (EU) 2016/679, the GDPR, represents an explicitly risk-centric approach with also some societal precautionary approaches continuing from its predecessor, the EU Personal Data Directive.[25] The Personal Data Directive art. 17 and art. 32 of the GDPR contain a general information security provision. Due to wide definition of personal data in art. 4 (1) of the GDPR – 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who *can* be identified – the GDPR

Directives 2006/48/EC and 2006/49/EC, *OJ* L 176, 27.6.2013, p. 338–436 . In cyber and information security thinking similar questions are mainly but not exclusively dealt under the concept of critical infrastructures and their resilience.

18 See on this Pöysti T (2023) Legislating for Legal Certainty, with a Right ot Human Face, in Automated Public Administration. In Suksi M (ed.) The Rule of Law and Automated Decision-making – Exploring Fundamentals of Algorithmic Governance, Springer 2023 (forthcoming, in print).

19 See Ansell C., Sørensen E. & Torfing J. (2021) The COVID-19 pandemic as a game changer for public administration and leadership? The need for robust governance responses to turbulent problems, Public Management Review, 23:7, 949–960.

20 See Nai Fovino et al. (2020), p. 51; Skopik F. et al. (2022) Blind Spots of Security Monitoring in Enterprise Infrastructures: A Survey. IEEE Security & Privacy. Vol. 20: 18–26; Green B. (2022) The Flaws of Policies Requiring Human Oversight of Government Algorithms. Computer Law & Security Review. Vol. 45, 105681 [Online].

21 See OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, OECD/LEGAL/0415, 2015. See OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris.

22 See OECD, Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456.

23 OECD Recommendation on Digital Security Risk Management, OECD/LEGAL0479; OECD Recommendation on National Digital Security Strategies, OECD/LEGAL/0480, OECD Recommendation on the Digital Security of Products and Services, OECD/LEGAL/0481; and OECD Recommendation on the Treatment of Digital Security Vulnerabilities, OECD/LEGAL/0482.

24 See Hydén H. (2022) Sociology of Law as the Science of Norms. Routledge, London & New York. p. 132–133.

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

is pretty much the law of nearly any data processing or data medium and information management system. The GDPR recognises also network and information security work as a legitimate objective for processing of personal data for secondary purposes. The GDPR is more concrete than its predecessor with examples of possible security techniques such as pseudonymisation and encryption. The GDPR links information security explicitly to the rights and freedoms of data subjects. The technical and organisational security measures in art. 32 of the GDPR are connected to general risk management and risk assessment duties further specified in art. 35 on the data protection impact assessments.[26] The information security in GDPR is an element of data protection by design and default in art.25, protection measures in art. 22 on automatic decision-making and the documentation required for the principle of accountability, which in art. 5 (2) is elevated to one of the general data protection principles. The principle of accountability serves also as legal foundation for an obligation to organise auditable and systematic network and information security work at the data controllers and processors. Art. 25 and 32 of the GDPR lay down foundations for security by design and default in processing of personal data and in ICT systems potentially processing such data. Duties of notification of personal data breaches to supervisory authority and to data subject pursuant to art. 33 and 34 are novelties in the EU-wide legislation in the GDPR compared to Personal Data Directive. Conceptually the information security in art. 32 (1b) of the GDPR includes the recovery from vulnerabilities and the elements of wider resilience.

The GDPR is not the only widely applicable cyber and information security provision in the Union legislation. EU Directive on privacy and electronic communications 2002/58/EC includes significant network and communications security provisions.[27] European Commission has proposed to replace directive with Regulation on Privacy and Electronic Communications in order to have a coherent set of legislation with the GDPR but the legislative procedure is delayed and still on-going.[28] The Union legislator has enacted EU-wide cybersecurity legislation by adopting NIS Directive (EU) 2016/1148 and EU Cyber Security Act (EU) 2019/881.[29] Cyber Security Act establishes ENISA as a permanent Union agency and sets a voluntary security certification scheme. NIS Directive explicitly departs from the vital role of the network and information security for societal and economic activities. It emphasises the magnitude and impact of the security incidents and the specific concerns and interests on the security of essential services and infrastructures. NIS Directive is explicit on the systemic risks, inter-connectedness of and dependence on technology across essential sectors. It seeks to enhance good security management practises related to digital systems and information processing.[30]

The European Commission presented a proposal for NIS2 Directive in 2020 in order to include more sectors and harmonise further security requirements and to bring further change of mind-set in legislation and regu-

[26] See art. 32 (1) and para. 76 and 78 of the GDPR. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

[27] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

[28] See COM (2017) 10, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Legislative procedure 2017/0003/COD.

[29] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), OJ L 194, 19.7.2016, p. 1–30. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency on Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.

[30] See also European Union Agency for Cybersecurity ENISA Guidance on Minimum Security Measures for Operators of Essential Services and ENISA NIS Directive Tool.

lation.[31] NIS2 Directive is linked with wider topics of strategic and operational resilience and quality of the infrastructures, which all are part of the security and well-functioning of the markets in the European Union. To these objectives also the European Commission proposal for CER Directive seeks to contribute as part of a wider Security Union Strategy.[32]

Several sectorial Union acts contain significant provisions relevant to cyber and information security directly or indirectly via generic risk management and conformity requirements.[33] Union however lacks a coherent policy and legislation setting horizontal cyber and information security requirements.[34]

Similar lack exists in Finland. The recommendation in our 1997 information security study of the need of a general act of parliament on information security was ignored at the time albeit many elements of the legislating on information security beyond the implementation of that time Personal Data Directive was included to sectorial legislation. Concerning Finland's public sector the Openness in the Government Act (621/1999) originally included section 18 on the good information management practise including inter-operability of information systems and information security and the Finland's Personal Data Act had a general principle and objective of good information processing practise as its parallel covering both public and private law. Provisions in section 18 of the Openness in the Government Act suffered from weak enforcement. The implementation was not sanctioned sufficiently strictly. The provision had the modern feature of connecting information security to a wider principle of good information management practise, which was also open for the development of technology and ethics of data processing.[35] This was a feature fully in line with much later NIS Directive.

Difficulties in the inter-operability of the public sector ICT systems led to the enactment of Act on the Steering of the Public Administration Information Management (634/2011), which deployed systematic enterprise, process, information and systems architecture model. This act proved to be too difficult to apply due to the demanding enterprise architecture method. The act was replaced in 2019 by the Public Information Management Act (906/2019), which also repealed the section 18 of the Openness in the Government Act.[36] Public Information Management Act contains more specific cyber and information security provisions for public authorities and sets general leadership responsibilities for senior executives of government entities. But it lacks the systemic principle of good information management practise. This may become a problem when technology and its application in various context develops.

These imperfections and limits of law as forum of justice and as instrument of good governance policies follow from the scarcity of legal thinking, dissatisfactory regulatory patterns and legislative and legal design models guiding information and information systems management and development. Fragmentation of law, absence of clear systematics, lack of sufficiently wide thinking and perspectives and weaknesses in the application and implementation processes remain constant problems in the law of cyber and information security.[37]

---

31 COM (2020) 823 final. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, legislative procedure 2020/0359 (COD).

32 COM (2020) 829 final, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, legislative procedure 2020/0365 (COD). On the Security Union Strategy, see COM (2020) 605 final.

33 Significant sectorial acts include EU Medical Devices Regulation (Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC), OJ L 117, 5.5.2017, p. 1–175 and Union acts concerning operative risk management in the financial sector (credit institutions and insurance companies), see for example Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) OJ L 335, 17.12.2009, p. 1–155, and the more detailed regulation concerning internal control and risk management covering also operative risk management and information systems.

34 See Nai Fovino et al. (2020) and the European Commission staff impact assessment document SWD(2022) 282.

35 See Saarenpää A. (2004) e-Government and good government; an impossible equation in the new network society, Scandinavian Studies in Law, Vol. 47: 245–273.

36 See on this Government Proposal HE 284/2018, p. 29.

37 On the concept of the scarcity of law, see Pöysti T. Communicational Quality of Law. In Magnusson Sjöberg, C. & Wahlgren, P. (2006) Festskrift till Peter Seipel. Stockholm: Norstedts Juridik, 463–493, p. 475–479.

3. The Revisited List of 20 Digital Network Society Risks

When revisited with the perspectives of current security research, international policy documents and Union legislation related to cyber and information security the 1997 risk list had decently endured the test of time. Nearly all risks identified in some form in the 1997 risk list appear to be highly relevant today albeit in 1997 terminology was not stable and legal categorization of many risks was only at its initial stateges. Today identification of risks is founded on a significant number of scientific research in different disciplines of socio-technological studies and computer science. The European Union and Finland's national legislation has changed and the addressing the risks of digital network society have become more widely explicit in law. However, the piecemeal legislation leads to that a coherent overall picture to risks may vanish in the middle of many details. In 2023 I will synthetize a list of key societal risks in digital network society with particular relevance to cyber and information security to the following 20 points:

1. *Trustworthiness risks* related to technology and socio-technological governance, which maintains general and specific trust in society.[38] Number of specific reported security vulnerabilities in software and ICT is growing.[39] New technologies also create new weaknesses, vulnerabilities and risks.[40] Trustworthiness of technologies is a key objective and concern in the recent European Union legislative initiatives and policies, for example concerning artificial intelligence. Trustworthiness depends on technical, ethical and legal aspects.[41] The resilient functioning of digital technologies and cyber and information security depend on the whole life cycle of the system and the whole path of the information.[42] Security should also then be security by design and default option including resilience by design and default. The vulnerabilities unavoidably do realize and attacks do happen.[43]
2. *Data, information, knowledge and cognitive risks*. These include classic issues of authentication, authenticity, availability, integrity and confidentiality of data and information which have long been in the agenda of information security. Integrity of evidence and the risks of corruption of digital documents and digital evidence are legally relevant specific aspects of that.[44] With the increased fluidity of data the *risks of combining of data,* correctness and use of the inferred information and the security of the metadata and the inferred data shall be added to the issues of legal concern and concern for cyber and information security work. Duties of care and informing data subjects and users about the risks

[38] See de Bruin H. et al. (2002) The use of legal knowledge-based systems in public administration: what can go wrong? In: Bench-Capon TJM et al. (eds), Legal Knowledge and Information systems, IOS Press, pp. 123–132; this is still very topical account on the sources of errors. The new technology opens new possibilities but also creates new security risks and vulnerabilities, see Nai Fovino et al. (2020), p. 51–53 concerning quantum computers and their potential advantages but also they may make the classic cryptography obsolete in communications security.

[39] See Weir C., Migues S. and Williams L. (2022) Exploring the Shift in Security Responsibility. IEEE Security & Privacy, vol. 20, no. 6: 8–17.

[40] See Nai Fovino et al. (2020), p. 66–68.

[41] On the trustworthiness of digital technologies, see European Commission's High Level Expert Group on Ethics Guidelines for Trustworthy AI, which saw rule of law and fundamental and human rights as a point of departure for trustworthy AI. See also Council of Europe in the Ad Hoc Committee on Artificial Intelligence, which drafts a binding legal instrument on Artificial Intelligence. See the European Commission proposal for Artificial Intelligence Act (COM (2021) 206 final, Legislative Procedure 2021/0106/COD). For a comparison, in United States of America, the White House Office of Science and Technology identified five principles that should guide the design, use, and deployment of automated systems in the age of artificial intelligence, the Blueprint for an AI Bill of Rights.

[42] On the life cycle perspective to systems of automatic decision-making and their regulation, see Koulu R. et al. (2019) Algoritmi päätöksentekijänä?: tekoälyn hyödyntämisen mahdollisuudet ja haasteet kansallisessa sääntely-ympäristössä. Helsinki: Valtioneuvoston kanslia. http://urn.fi/URN:ISBN:978-952-287-764-2.

[43] Nai Fovino et al. (2020), p. 59 and Skopik F. et al. (2022), op. cit.

[44] On legal informatics account of the electronic evidence in criminal trials in Finland, see the doctoral dissertation by Juhana Riekkinen in legal informatics and procedural law concerning electronic evidence in Lapland University, Riekkinen, J. (2019) Sähköiset todisteet rikosprosessissa: Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen, AlmaTalent Helsinki.

involved extends to metadata and inferred data.[45] In Finland, the Constitutional law Committee has particularly emphasised the risks posed by large data repositories and, in particular, of the special categories of personal data referred to in the GDPR.[46] Societal level of cyber and information security nowadays increasingly extends to cognitive issues and fighting misinformation and governs cognitive risks.[47] Cognitive security in security and ICT technical term refers to the use of artificial intelligence techniques modelling human thought processes, that is, to cognitive computing techniques, used to detect security vulnerabilities.[48]

3. *Risks of communication, authenticity and interaction in digital communications* which include a wide array of technical network and information security risks but, additionally several aspects related to the planning, design and maintenance of the information and communication systems.[49] These also include technical risks of network and communication security including authenticity and identification of the parties of communication and the risks to the communication related services and service infrastructure. Domain name servers, and routers and the application programme interfaces (APIs) in general have constantly proven to be weak points and call upon better embedded security at the level of architectures, protocols, software, authentication policies and configurations.[50] Deep fake techniques create also a significant risk to authenticity and should lead to question the value of image as evidence and foundation for cognition in media and society.[51] In the future increased computing power in networks and particularly provided by quantum computers may even shake the foundations of cryptography in communications security.[52]
4. *Legal risks*. Legal risk often refers to non-compliance with the requirements and the legal consequences under contracts or under legal regulation that apply to failure to comply with legal requirements such as art. 25 and 32 of the GDPR or the conformity requirements in Medical Devices Regulation or Product Safety Directive or in other acts setting conformity requirements or in contractual requirements.[53] Legal risk management has become a vital part of corporate governance and compliance in regulated sectors

[45] See Gouert C. and Tsoutsos N. G. (2022) Dirty Metadata: Understanding A Threat to Online Privacy. *IEEE Security & Privacy*, vol. 20, no. 6:. 27–34.

[46] See Constitutional Law Committee Opinions PeVL 4/2021 vp and PeVL 71/2018.

[47] See European Agency for Cybersecurity ENISA (2022), ENISA Threat Landscape 2022, European Union Agency for Cybersecurity (ENISA), p.82–87 on the risk of misinformation, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[48] Andrade, R. O. & Yoo, S. G. (2019) Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of information security and applications*. [Online] 48102352–. Hurlburt, G. (2022) Thinking and Feeling Cognitive Security? *IT professional*. [Online] 24 (5), 77–80.

[49] On the impact of the user-interface to the success or failure of the digital interaction see Deputy Chancellor of Justice Decision OKV/1418/10/2020.

[50] See Bradshaw, S. & DeNardis, L. (2018) The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom. New media & society. [Online] 20 (1), 332–350; Khormali, A. et al. (2021) Domain name system security and privacy: A contemporary survey. Computer networks. [Online] 185107699– in which the authors provide a synthetized DNS threat landscape; Li, Z. et al. (2021). A clogging resistant secure authentication scheme for fog computing services. Computer Networks, 185, 107731–. See also Pöysti T. (2019) The IIoT and Design for Contextually Relevant Data Protection. In Ballardini, R. M. et al. (2019) Regulating Industrial Internet Through IPR, Data Protection and Competition Law. Alpen aan den Rijn, The Netherlands: Wolters Kluwer: 183–206.

[51] See van der Sloot B. & Wagensveld Y. (2022) Deepfakes: Regulatory Challenges for the Synthetic Society. Computer Law & Security Review, Vol. 46, 105716.

[52] See Nai Fovino et al. (2020), op.cit., p. 52; Moody D. and Robinson A. (2022) Cryptographic Standards in the Post-Quantum Era. *IEEE Security & Privacy*, vol. 20, no. 6: 66–72; Mailloux L.O., Lewis II C. D., Riggs C. and Grimaila M. R. (2016) Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. IT Professional, vol. 18, no. 5: 42–47.

[53] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002, p. 4–17. Legal risks related to cyber and information security can relate to liabilities for the non-compliance with security requirements or contractual responsibilities such as the information security clauses in model IT agreements. See, for example in Finland chapter 8 in the general conditions of contract in the IT2015 –sopimusehdot, collection of standard IT-contract clauses.

where producers and service providers shall ensure compliance with a significant number of different types of laws and standards further detailing the regulatory requirements.[54] It is not rare that the standards developed for different legitimate purposes conflict with each other: for example standards on environmental and social responsibility may require transparency on aspects where transparency may be problematic from the cyber and information security point of view.

5. *Risks in logistics, value chains and supply chains* which are increasingly a general concern for European Union legislator and for businesses in general and which are also dependent on digital platforms, communication and steering systems. Supply chains can be used also on intentional attacks on the resources of final customer.[55] Long value chains also create new vulnerabilities and also possibilities for abuse and make it difficult to assess security of a software code consisting of several layers of code coming from different software developers.[56]
6. Series of *financial technology* and *financial system risks* where *payment method and payment system risks*, including risks related to payment transactions, account systems and card payment and, also, *currency risks*, to which have been added the *risks associated with cryptocurrencies* including criminality and odd activities with them. Payment security has proven to be one of the eventual weak links in the overall digital security and cyber and information security in particular. Digital finances and financial technologies and the general dependence on the payment systems even in the many basic services of economic and societal interest have increased the societal interest on cyber and information security in the financial sector in general and on payments systems in particular, and of the resilience of the payment system. Vulnerabilities and disruption of service in the financial infrastructure may cause severe perturbations in many critical societal functions. The Finnish Parliament's Economic Committee interestingly called upon a constant dialogue with stakeholders to maintain up-to-date threat awareness when issuing a report for the Plenary on the proposal for an Act of Parliament in which the government was named to maintain an alternative resilience payment system should the payments systems fail.[57]
7. *Credit risks and risks of over-indebtedness*; Digital society is very much a credit and credit worthiness society. Credit risks are managed through credit information services and positive credit registers, among other things, but the tools of which create also new risks and vulnerabilities, credit data risks, in the form of concentration of personal data. Particular requirements for the correctness and security of credit data and credit data information systems follow from the value and significance of such data for participation to economy and society.[58]

---

[54] See Winkle T. (2022) Product Development Within Artificial Intelligence, Ethics and Legal Risk: Exemplary for Safe Autonomous Vehicles. Wiesbaden: Springer Fachmedien Wiesbaden GmbH. See also Misćenić E. and Raccah A. (2016) Legal Risks in EU Law: Interdisciplinary Studies on Legal Risk Management and Better Regulation in Europe. Cham: Springer International Publishing AG, Online. See as well Crootof R. (2019) Cyborg Justice and the Risk of Technological-Legal Lock-In. Columbia law review 119.7: 233–251.

[55] See ENISA Threat Landscape (2022), p.88–94 on supply chain attacks.

[56] A timely example of this is the loading of privacy intrusive pictures taken by robot vacuum cleaners under user testing to a social media platform, see Guo E. (2022) A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook? MIT Technology Review, 19.12.2022, A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook? | MIT Technology Review.

[57] This is shown also in the Finnish Acts on the Supply Security of Financial Services and thereto related Legislation, see Acts and Government Proposal Hallituksen esitys eduskunnalle laiksi eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla ja siihen liittyviksi laeiksi HE 104/2022 vp, https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_104+2022.aspx; Report of the Economic Committee of the Parliament TaVM 18/2022 vp, which also underlined the network and communications security as an essential condition for the continuity of service in the financial system.

[58] On the errors of the credit risk data and significance of the information system design to the accuracy of credit risk data Finland's Data Protection Authority, the Data Protection Ombudsman Decisions 10.1.2022 on erroneous delivery and registrations on payment failures where poor information system design in the Finnish Court system together the practises of the Credit data register companies led to consider disputing a claim in Court as a payment failure in the credit registers, 834/532/18, 4356/532/19 and 8211/161/19. Same issue was at an earlier stage investigated by the Parliamentary Ombudsman in 2017 and the Data Protection Ombudsman

8. *Data protection risks and other information-rights risks* which are threats against data protection rights and other information- and information processing dependent rights. The GDPR seeks to control the risks related to the possibilities to combine data and data protection issues concern today both inferred data and metadata.[59] Risks related to the digital identity and operating profiles of legal persons, that is data protection beyond the current boundaries of EU data protection law, belong also to this category of information-rights risks.[60] Question is also of confidence to the sources of applications (and data) distributed under trustworthy names and marketplaces such as the shops and stores of Tech Giants trough which also malware has been spreading. Abuse of names and operating profiles in getting attention and in scams is a wide phenomena.
9. *Technology risks associated with the thinking, design and maintenance of the overall architecture and operating architecture, system architecture and the information system environment*. This category of risks does not concern trustworthiness in general but the realization and maintenance in specific situations.[61] Thinking errors or limits of design constantly appear as the root causes of many legal problems.[62] Weak governance and mal-aligned incentives for the security in the development of technology and software and the trade-offs between efficiency and security are often root causes for these risks.[63] Considerable trade-offs exists between ease of use and security. All too often the choice is for lower costs and ease of use at the costs of security. European Union law and Member States law has been weak to provide theses incentives as shown in the legal informatics studies of the software development.[64] European Union searches for the rectification of at least some of these problems by proposing new European Parliament and Council Regulation on horizontal cybersecurity requirements for products with digital

concurrent with the findings of the Parliamentary Ombudsman, see Parliamentary Ombudsman Decision EOAK/945/2016 who also requested Ministry of Justice to take remedial action concerning Court information systems. On the positive credit register in Finland, see Act on Positive Credit Data Register 739/2022 and the Government Proposal HE 22/2022 vp, and the constitutionality review of the draft law in Parliament in the Constitutional Law Committee Opinion PeVL 28/2022 vp, see para. 4 and 5 on the specific risks related to credit data and para 6 of the considerable significance of such data.

59 This follows already from the very definition of personal data in art. 4 (1) of the GDPR according to which 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly... and the application when the question is of identifiable persons is confirmed also in the preamble para. 26 of the GDPR. This provision and the definition of personal data in the Personal Data Directive have given rise to wide application of concept of personal data in the jurisprudence of the European Court of Justice, see, for example case *Peter Nowak*, Case C-434/16, [2017] (ECLI:EU:C:2017:994) and concerning the narrower concept of health data, which falls nowadays under the specific groups of data requiring particular, more intensive protection, case *Bodil Lindqvist,* Case C-101/01, [2003] ECR I-12971 (ECLI:EU:C:2003:596), at para. 49 and 50 and case *Breyer*, Case C-582/14 [2016] (ECLI:EU:C:2016:779) at para. 46 where the court excluded references which are practically impossible from falling under the concept of identifiable under Personal Data Directive and case Vyriausioji tarnybinés etikos komisija, Case C-184/20, [2022] (ECLI:EU:C:2022:601). See also Wachter S. and Mittelstadt B. (2019) A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. Columbia Business Law Review No 2: 494–620.

60 On the concept and idea of data protection to legal persons beyond data protection laws see a pioneer work Bygrave L. (2002) Data Protection Law. Approaching Its Rationale, Logic and Limits. Kluwer Law International, The Hague, p. 173–298.

61 See, for example Skopik F. et al. (2022), op.cit.

62 See in Finland's supreme legality oversight Chancellor of Justice Decision OKV/2674/10/2020 concerning terms of use and information to be given to the users on the AI-powered OmaOlo –health care services platform; Decision of the Deputy Chancellor of Justice OKV/1418/10/2020 on the web-services provided by Public Economic and Employment Offices and the misunderstandings the interface design could lead to; Deputy Chancellor of Justice Decision OKV/1179/10/2020 on weak designs and their consequences for the accessibility and secure communication by clients of social security with disabilities or issues with functionalities in screens and key boards. Time-barring connection de facto prevented slow utilisers to benefit from digital communication. See also Chancellor of Justice Decision OKV/338/1/2018 on the technology neutral services where the Chancellor hold that technology neutral web services which function also in mobile devices would enhance equality in line with the Constitution and the Deputy Chancellor of Justice Decision OKV/1418/10/2020 where design of the user-interface and the underlying ICT system made the communication prone to misunderstandings and thereby good administration was not realized. On the usability of the services of digital public administration in Finland and on the Chancellor of Justice case law on the usability among guaranteed features of good administration and other fundamental rights, see Koulu R., Sankari S. and Sormunen S. (2022) Digitalisoituva julkishallinto: käytettävyys kuuluu kaikille. Edilex 2022/36 [Online], p. 4–5, 14 and 22.

63 See Nai Fovino et al. (2020), op.cit., p. 24–26.

64 See Råman J. (2006) Regulating secure software development: analysing the potential regulatory solutions for the lack of security in software. Rovaniemi: University of Lapland.

elements. The proposed regulation seeks to strengthen cyber resilience by introducing horizontal cyber security requirements for products with digital elements, particularly with software and hardware vulnerabilities and to force manufacturers to provide better information on the cyber security.[65]

10. *Platform and ecosystem risks and the related (11) risks of the abuse of private and public power* contained in digital platforms and the service network created around them and the application risks of an individual information system or application. Competition in the digital economy is increasingly between ecosystems organised around platforms. This creates an ecosystem risk for individual businesses and other actors. All services attached to a platform and its ecosystem are technologically and operationally dependent on that platform. Hence, security vulnerabilities multiply. Economic and government actors as well as consumers and citizens may be locked into an ecosystem. Platforms use considerable power and modify legally relevant power positions.[66] This creates new inconsistencies with law by adding the platform service provider between the classic partners of producer/seller – consumer/user and, consequently risks of confusion, uncertainty and abuse of power emerge. New question of the basis of allocation of duties of care, for example in the provision of cyber and information security unfold.[67] Competition law and data protection law and broader information law come and need to come closer together as coherent preventive and reactive systems of remedies for abuse of power and disproportionate positions of power.[68] European Union has started to address power inequalities and the risks of abuse of market power by the new Digital Services Act (EU) 2022/2065 and Digital Market Act and the Data Act (EU) 2022/1925 seek to address some of the new informational power asymmetries in platforms and ecosystems based on platforms.[69]

12. *Risks of abusive or suppressive bio-politics via personalised mass-influencing*. Datafication with Big-Data and SmartData analytics and platforms enable also personalised and massive influencing to large parts of population by both private and public actors.[70] These changes in the possibilities provided by the technology blur also the borders between private and public and personal and mass communications. The bio-politics described by Michel Foucault in his famous series of lectures in the College of France has become a reality with un-precended possibilities and risks for abuse of power. Abusive bio-politics is not necessarily evil dictatorship. It can also be well-intentioned but imposed policies and restrictions of competition seeking short term consumer benefit or general happiness but supressing autonomic,

65 See COM(2022) 454, legislative procedure 2022/0272/COD, see also commission impact assessment in document SWD(2022) 282.

66 On the research in legal informatics on the abuses of the dominant position of big platform companies in a data protection perspective, see Wiatrowski, A. (2021). Abuses of dominant ICT companies in the area of data protection. Lapin yliopisto. See also Hintz, A. et al (2018). Digital citizenship in a datafied society. Polity Press, chapter 1, pp. 20–41, where the authors argue that in a digital society digital platforms and omnipresent digital technologies at everyday life mediate legal rights and political views: privacy and surveillance and risks related to information security have a also considerable significance to citizenship. Author concludes that agency and power is vested to those who can process data and that code of the ICT systems processing data is outside the scope of influence for many and dis-empowers many. Trustworthy infrastructure becomes a basic element of digital citizenship as citizen-consumers and political citizens.

67 See, for example Päläs J. (2022) Oikeusasema jakamistalouden hyödykesopimussuhteissa – Tutkimus vallasta, subjektiuksista sekä oikeuden ja sosiaalisen etääntymisestä. Acta electronica Universitatis Lapponiensis 340. Lapin yliopisto, Rovaniemi, p. 61–78 and p. 89–96 on cyber security related duties of care and protection of the weaker party in the power relations of sharing economy based on digital platforms.

68 See Kuenzler A. (2022) What competition law can do for data privacy (and vice versa). Computer Law & Security Review, Volume 47, 2022, 105757. See also Pöysti T. (2018) Kohti digitaalisen ajan hallinto-oikeutta, Lakimies 7–8/2018: 868–903, 896–903 on the role of legal informatics, administrative law and also competition law in the control of power residing in data structures, code and infrastructures.

69 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, p. 1–102. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L 265, 12.10.2022, p. 1–66.

70 See Greenstein (2017), op.cit, p. 75–78 on features of Big Data and p. 93 Smart Data from a legal perspective.

well-informed decision making with real possibilities of a choice.[71] Cyber and information security are elements, which maintain psychological, cognitive and even physical integrity and dignity for individuals to make informed choices and keep choices relevant, not only a tick-a-box -formality.[72]

13. *Democracy risks*. Informational rights are at the heart of liberal democracy and constitutional state based on democracy and rule of law, the freedom of expression and, right to informational selfdetermination and privacy, are the necessary conditions for democracy. In digital society democracy and citizenship are realised on and is dependent of the quality of digital infrastructures.[73] Information and communication technologies including artificial intelligence can in many sense enhance access to information and exchange of information. Concurrently with promises social media and ICT based communications have enhanced communicational phenomena weakening or threatening democracy.[74] Safeguarding good citizenship and sensible, pluralistic public discourses in the current digitalized speech and media context with automated and personalized content curation are concerns for international organizations and legislators. Here digital security in general and cyber and information security in particular together with human-rights-friendly infrastructures and access to content and good content assessment skills are essential elements in democracy in the digital age.[75] Serious defects in cyber and information security may establish also a chilling effect on free speech and access to information.
14. *Risks of digital exclusion*. Digital society offers empowerment and tools for human agency but also gaps and obstacles to public and private participation. These replicate existing inequalities but depend also on multi-faceted issues of access to use of digital infrastructure and tools to use digital procedures as well as of skills and even physical conditions.[76] Accessibility issues together with the cyber and information security become preconditions for equal rights and participation to which both European and national legislators and constitutional guardians have paid attention to by the EU accessibility directive (EU) 2016/2102 and by national laws and calls on to work with solving structural forms of digital exclusion and enhance inclusion in digital world.[77] EU accessibility legislation covers mainly

---

71 See Foucault M. (2004) Sécurité, territoire, population. Cours au Collége de France, 1977–1978. Gallimard; and Fleury C. (2015) Les Irremplacables. Gallimard, p. 190–193 and 224–225.

72 On consent inflation and security issues related to IoT and Quantified Self see Pöysti T (2006), op.cit..

73 See Paliwala, A. (2013) Netizenship, security and freedom. International review of law, computers & technology. [Online] 27 (1–2), 104–123. See, generally for the general challenge of digital technology to democracy, see Ceccarini, L. (2021) The Digital Citizen(ship): Politics and Democracy in the Networked Society. [Online]. Cheltenham: Edward Elgar Publishing Limited.

74 See Reiss M. (ed) (2020), Citizenship in a Networked Age, Templeton World Charity Foundation, London, p. 86–97; One of those phenomena is personalization of communication and, for example, the avoidance of news in the online content feeded by algorithmic curation, see Reiss M. (2022) Dissecting Non-Use of Online News – Systematic Evidence from Combining Tracking and Automated Text Classification, Digital Journalism, DOI:10.1080/21670811.2022.2105243.

75 See, for example, Haas J. (2020) Freedom of the Media and Artificial Intelligence. Office of the Represetative of the Freedom of the Media, Organization for Security and Co-operation in Europe OSCE, Office of the Representative on Freedom of the Media Organization for Security and Cooperation in Europe (OSCE), Vienna. See Organization for Security and Cooperation in Europe OSCE, Representative of the Freedom of Media (2020) COMPILATION REPORT, PUBLIC CONSULTATION ON THE IMPACT OF AI ON FREE SPEECH, https://www.osce.org/files/f/documents/f/c/485648.pdf and Bukovaska B. (2020) Spotlight on Artificial Intelligence and Freedom of Expression. Office of the Representative on Freedom of the Media Organization for Security and Co-operation in Europe (OSCE), Vienna 2020.

76 For an interesting sociological analyses of the structures of digital divide using Max Weber's classical theory of social stratification, see Ragnedda, M. (2017) The Third Digital Divide: A Weberian Approach to Digital Inequalities (1st ed.). Routledge, in particular chapter 2 and chapter 5.

77 For Finland see Act on the Provision of Digital Services (306/2019) implementing the accessibility directive and Constitutional Law Committee Reports PeVM 11/2021 vp, para. 8–10 and PeVM 16/2020 vp, p. 3. See the prior constitutionality review opinion of the Chancellor of Justice OKV/1027/21/2020 concerning Quality Guidelines for good aging and improving services for elderly where the Chancellor called upon ensuring user participation and taking into account user perspectives and securing possibilities for the elderly to use digital tools safely and securely. See also the Decision of the Deputy Chancellor of Justice concerning the possibilities of the disabled persons to use digital communication with and digital services of the Finnish Social Institution OKV/1179/2020. These aspects and cyber and information security should also be taken into account in the general enhancement of digitalization. Data protection impact assessments pursuant the GDPR are intended to be an active tool of ensuring adherence to fundamental rights and

public sector. Accessibility issues are often considered separate from the cyber and information security issues. This is a problem. For example, elderly persons are vulnerable and targeted in computer crimes. Accessibility shall also be guaranteed in balance with cyber and information security of the applications. Security thinking and accessibility issues are part of a wider and yet to be solved paradox between usability and security.

15. *Control risks for public authorities* were on the original risk list of 1997. Control risks for public authorities related in the original risk list to the capacity for the public authorities to exercise legitimate control and oversight for example concerning double-use technologies or taxation in platforms. Double use technology legislation covers increasingly everyday items due to the embedded nature of the advanced digital technology, which can have also military use.[78] Specific cyber and information security control risk is the abuse of cyber surveillance technology for non-authorised military purposes and for spying.[79] Cyber and information security is today essentially a public good depending also on the situation awareness and activities of the government and its agencies to detect and prevent risks and of the strategic leadership and planning required in the NIS Directive and recommended in the 2022 OECD digital security guidelines. This requires also up-to-date legal framework for cyber and information security awareness and co-operation within the government and between government entities and the society at large.[80]
16. Today *human control risks* concern securing human autonomy and agency including informed decision-making and assessment in a virtual-physical environment where humans live together with and as part of a technological system consisting of ubiquitous digital technologies with certain degree of autonomy.[81] Human control or user control can in this context be rather seen as realization of the principles of accountability and responsibility in the whole life cycle of automatic systems.[82] Some human control arrangements create risks and blindspots themselves. Human control can be a fallacy giving a false sense of security. In complex systems environment human controls are not sufficient for effective security and oversight.[83] Humans are one of the most vulnerable parts in the cyber and information security.[84] The eventual use of

freedoms including digital equality and right to security, see Opinion of the Chancellor of Justice on the Final Report of the Working Group of the Government's Programme for the Enhancement of Digitalization, OKV/2791/21/2022.

78 Saarenpää & Pöysti (eds) (1997), p. 41.

79 See Kim, H. (2021) Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue. *The International and Comparative Law Quarterly*, *70*(2): 379–415 where also the growing regulatory and strategic competition between U.S., China and EU is observed to have a considerable impact on the arrangements on dual use products.

80 Finland is about to legislate on this issue, see Government Proposal for Amendments of the Act on Digital Communication Services, Act on the Processing of Personal Data in the Defence Forces section 29 and Act on the Processing of Personal Data at the Police Services section 22, HE 243/2022 vp. Finnish government also carries out a wider project assessing the conditions and possibilities for the Government and its agencies to ensure cyber security and cyber defence, see Government of Finland project PLM003:00/2022 – VN/2434/2022, https://valtioneuvosto.fi/hanke?tunnus=PLM003:00/2022. Project is based on the Government Decision on the Cyber Security Development Programme 10.6.2021, see Kyberturvallisuuden kehittämisohjelma, Liikenne- ja viestintäministeriön julkaisuja 2021:7, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163219/LVM_2021_7.pdf. Overview and the materials of the Finnish Government Cyber Security Development Programme in English, see https://www.lvm.fi/en/-/cyber-security-development-programme-higher-level-of-cyber-security-brings-growth-and-jobs-1376758.

81 Under human control or user control is one of the key ethical principles according to principles of Trusworthy artificial intelligence by the European Commission's High Level Expert Group on Ethics Guidelines for Trustworthy AI and in the Council of Europe Commission for the Efficiency of Justice European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment (Council of Europe 2019). See also Pöysti T (2018) op.cit., where I in p. 895–899 develop ideas on the protection of human autonomy and constitutional humanism as one of ultimate objectives of digital administrative law.

82 Maintaining human control is generally one of the core principles recognised in the scientific contributions to responsible artificial intelligence albeit this should be rather read as conformity with the principles of accountability and responsibility, which does not requirethat everything should be based on the preprogrammed rules, see Dignum V. (2019) Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way. [Online]. Springer International Publishing AG, pp.3–6, 20–22 and 47–62.

83 See Green (2022) op. cit.

84 See Hebert C. (2022) Trust Me, I'm a Liar.*IEEE Security & Privacy*, vol. 20, no. 6: 79–82, where the author analyses of the use of deception in the defence against cyber attacks.

artificial intelligence tools to cyber criminality is an increasing thread which is likely to realize and calling for additional sophistication in the security thinking and tools.[85] Cyber and information security arrangements and the law on cyber and information security ultimately protects human autonomy, which is one of the most fundamental principles and values in law.

17. *Risks of cybercrime and other crime taking* advantage of technological environment and constantly developing technological tools. Cybercrime has received considerable attention by international organizations and European and national legislators. The Council of Europe Convention on Cybercrime (ETS No. 185, Budapest Convention) and the European Union Directive 2013/40/EU on the attacks against information systems are principal European level legislative instruments.[86] The Council of Europe Convention on Cybercrime was the first international treaty on crime committed in the digital network environment and providing criminal law and procedure protection for network security.[87] Cybercrime continues to be an increasing threat where benefits of attacks seem to be greater than costs and risks to attackers.[88] Cybercrime is estimated by the European Commission's Joint Research Centre to cause annual costs of 5,5 trillion euros and an increasing trend of cyber attacks is observed since 2015.[89] Prevention of cyber crime depends on the effective realization of GDPR and security by design and default protecting not only systems but the rights of the users and stakeholders.[90]
18. *Risks of hybrid influencing and cyber warfare*.[91] In the current security situation in Europe hybrid influencing and use of cyber means are topical issues.[92] Hybrid influencing and cyber warfare are significant national security and European Union security concerns.[93] These concerns have in Finland led to definition of serious hybrid influencing as as a new category of national emergencies in the Emergency Powers Act, which is enacted as a permanent but limited exception to Constitution.[94]

---

85 For topical threats related to AI and cyber crime see for example F-Alert. Monthly threat updates from F-Secure. December 2022, p.3, https://www.f-secure.com/content/dam/f-secure/en/consumer/documents/F-Alert_December.pdf (accessed 4.1.2023).

86 Directive 2013/40/EU of the European Parliament and of the Council of 12 August of 2013 o the attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14.

87 See Council of Europe Convention on Cybercrime, ETS No 185 and the explanatory memorandum, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

88 See Hebert (2022) op.cit. According to ENISA 2022 analyses ransomware, malware and social engineering were the top 3 cyber and information security threats and denial of services attacks number 5 threat and cybercrime has an important share in the remaining top 8 security threats, ENISA Threat Landscape 2022, op.cit. The complexity of security work in a networked ICT environment and the level of detail, which is required for effective cyber and information security strategies require use of automated controls and detections as part of the security architecture, see van Oorschot P.C: (2022) Security as an Artificial Science, System Administration, and Tools. IEEE Security & Privacy, vol. 20, no.: 74–78, Nov.-Dec. 2022 Ge B. and Xu J. (2020) Analysis of Computer Network Security Technology and Preventive Measures under the Information Environment. 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE): 1978–1981.

89 Nai Fovino I. et al (2020) Cybersecurity, op.cit. p. 7–8.

90 For Finnish law and constitutional requirements and potential of the GDPR see the prior constitutionality review opinion of the Chancellor of Justice concerning reform of the Acts related to personal identification number in Finland, OKV/69/21/2022 and the prior constitutionality review opinion of the Chancellor of Justice concerning Government Proposal for amending Act on Population Data Register and Act on Certification services provided by Digital and Population Data Services Agency (victims of the identity theft), OKV/2884/21/2020.

91 There is a growing legal literature concerning cyber war and cyber and information engagements and operations and how they are seen under international law, see for example Hodkinson S. L. (2018) Crossing the Line: The Law of War and Cyber Engagement – Applying the Existing Body of Law to this New National Security Threat. International Lawyer, [s. l.], Vol. 51, n. 3: 613–628; Schmitt, M. N. (2013) Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press and International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019. (2020). International Review of the Red Cross (2005), 102(913), 481–492.

92 Government Proposal for Acts amending Emergency Powers Act and section 79 of Conscription Act HE 63/2022 vp.

93 Nai Fovino et al (2020), op.cit, p. 61–63.

94 See Act on the (706/2022) on the Amendment of the Emergency Powers Act (15522/2011), Government Proposal for Acts amending Emergency Powers Act and section 79 of Conscription Act HE 63/2022 vp, Report of the Parliament's Defence Committee PuVM 2/2022 vp and the Opinion of the Constitutional Law Committee of the Parliament PeVL 29/2022 vp on the constitutionality of the

19. *Risks in cooperation and creation of epistemic awareness and shared understanding between and beyond different professions*. Risk for effective governance for cyber and information security and for the realization of rights in the digital environment is the lack of cooperation beyond narrow perspectives of individual disciplines and their subfields and the various obstacles and misunderstandings in the multi-disciplinary and multi-perspective collaboration and situational awareness. Finding a common language and methods for multi-disciplinary work is not of the smallest problems.
20. *Risks of legal regulation and the scarcity of legal thinking, legislation and application of justice*. Law is a stabilizing force in society. Law may be at odds with the future since the law in statutes, precedents and established practises repeats solutions developed to past conflicts and problems. All too often the law as legislated and practiced suffers from narrow thinking, a scarcity of justice in terms of thinking and quality argumentation or scarcities in terms of tools and legislative and regulatory models. These scarcities makes the law to be imperfect or to fail, or unreasonably costly, to realize the fundamental ratio of law: protection of humans and predictable provision of legal certainty. While certain in-determination is an inherent and unavoidable nature of law and justice – and hence factors making full automation of judicial decision-making extremely difficult – features in positive law and scarcity in legal thinking and argumentation may accelerate this weakness of law beyond reasonable limits.[95] In a policy perspective failures and caveats of legal regulation in the attainment of the objectives of the legislation are valid and legitimate reasons to revise acts. Law may also have transformative goals towards the future to change thinking and action paradigms. Not rarely will the law also encounter shortcomings in this transformative mission. This is explicitly cited to be behind the Commission proposal for NIS2 –Directive: to overcome limitations in the current NIS Directive.[96] The lack of universal cyber and information security requirements and the fragmented, piecemeal approach to it in the various acts and policies of the Union is recognised to contribute to these weaknesses and failures of Union law.[97]

4. Legal Informatics in the Future Proofing of Law

Studies on the impacts and risks of technologies and data processing practises can and even shall be taken into account in the interpretation of the data protection principles and other legislative provisions as well as in the de lege ferenda consideration of new legislation.[98] The identification and categorization of wider societal risks

Government Proposal. On the concept of hybrid operations and hybrid warfare, see Niglia, A. (2016) Critical infrastructure protection against hybrid warfare security related challenges, Amsterdam, Netherlands: IOS Press in which the issue of information and cyber systems and protection of ICT infrastructure is well highlighted. On the Russian activities and doctrine of hybrid influence and warfare in its foreign policy, see Renz, B. & Smith, H. (2016) Russia and Hybrid warfare – going beyond the label. Aleksanteri Papers, no. 1/2016, Kikimora Publications, http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf in which the authors also take up the ambiguity of the concept of hybrid warfare, the same point was later made by the Constitutional Law Committee when assessing preciseness and comprehensibility of the amendments to Emergency Powers Act.

95 For the indeterminacy of law – Unbestimmtheit des Rechts, see Habermas J. (1992) Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Suhrkamp, Frankfurt am Main, pp. 243–258. On the possibilities for automation of legal decision-making, see Ashley, K.D. (2019) Automatically Extracting Meaning From Legal Texts: Opportunities and Challenges. Ga. St. U. L. Rev. 35(4):1117–1151 and Praekken H & Sartor G (2015) Law and Logic: a Review from an Argumentation Perspective. Artificial Intelligence 227:214–245.

96 See Commission proposal for NIS2 – Directive, COM(2020) 823 final, chapter 1 and 3, according to which the proposal seeks to continue the paradigm shift launched by the NIS Directive. See also Commission staff working document, impact assessment report accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, SWD/2020/345 final.

97 See European Commission staff impact assessment document SWD(2022) 282 accompanying Commission proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, pp. 11–13.

98 See, for example Wrigley S (2021) Bots and AI-related Technologies, Legitimate Interest, and Fair Processing Under the General Data Protection Regulation. Helsingin yliopisto, Helsinki 2021 (doctoral dissertation accepted in the Faculty of law, University of Helsinki), where the author explicitly connects data protection impact assessments to the weighting whether processing of personal data on the basis of legitimate interest under art. 6(1)(f), as interpreted by the principle of fairness per art. 5(1)(a) of the European

with particular relevance to cyber and information security serves the future proofing of law and setting legal requirements on cyber and information security to a relevant context where it is easier to see the ratio of law and eventual needs for revised legislation. Performing socio-legal and sociotechnical studies, which provide scientific basis for coherent, balanced, understandable and up-to-date legislation is among tasks of legal informatics. Legal informatics has particular value in the provision of coherent theories and scientifically robust views beyond specific fields of law. Legal informatics contributes to the general theory and conception of security, risks in ICT and human-technology relations. Its task is also to develop common languages and tools to multidisciplinary research and collaboration between practitioners overcoming the scarcities of justice and understanding between professions and their epistemic communities. These tools include concepts, models, design patterns and contributions to security libraries. Risk analyses are a very small contribution in this mission. Name of the discipline and paradigm may be different than legal informatics and the research methods evolve over time but these fundamental questions needs robustly founded answers.[99]

This scientific mission touches profound questions of the role and limits of law. The old security paradox is that technology is used to overcome security challenges but this increases the complexity of the systems and creates new security vulnerabilities. Technology to assist humans can then exceed the human capacity of oversight: a guard's problem where the guard looses insight into the activity to be guarded unfolds.[100] Security paradox and the guard's problem represent a general feature of living in the digital society. Mystification of digital technologies either as utopia or dystopia shall be avoided.[101] Particularly in artificial intelligence context critical capacity to review both the process of reasoning and outputs of the automatic systems will be needed when artificial intelligence solutions can produce texts and analyses seemingly decent or good but not always with quality. Human history and progress of humanity is about learning to use tools and built collaborations. There is a partnership between human agent and partly autonomous, ''intelligent'' systems to augment human problem-solving power. But the very same capacities will also be used for deception, fraud, harm and war, that is all the evils we know and creative mind is able to innovate. We live and work together with hybrid systems and architecture in human – machine collaboration, as actors of a socio-technical system.[102]

Interactions with the technical systems are not one-directional.[103] Good architecture of security is hybrid including both humans and technical solutions. Security solutions and strategies need to be kept constantly up to date.[104] The blind spots of cyber and information security and the needs of legal certainty and justice call upon to reconsider repair and remedies. Maintenance is as important as creation of completely new systems

Union General Data Protection Regulation (EU) 2016/679. Finland's primary prior reviewer of the constitutionality of proposed acts of Parliament pursuant to section 74 of the Constitution of Finland, the Constitutional Law Committee, has consistently emphasized the risk centric approach according to which rights and freedoms of the individuals shall be guaranteed against risks, which also shall be identified as part of the law drafting, and in which the Acts of Parliament shall include explicit provisions taking into account the identified risks, see, for example Constitutional Committee Opinion PeVL 1/2018 vp, p. 3–5 and p. 7–8 in which also functionally information security and risks to information security were recognised, however, without using the term of information security; PeVL 14/2018 vp, p. 5.

99 See Pohle (2021), op.cit., pp. 286–287, where he sees the systematic and disciplined common interface and communication between legal science and information and computer sciences and the disciplined and methodic study on the informationalization of society and its structures among the enduring legacies of previous generations' work in legal informatics.

100 See Fuchs-Kittowski K. (2021) op cit, p. 50.

101 On the danger of mystification, see Brödner P. (2021) "Machines that think" – die KI-Illusion und ihre Wurzeln. In Pohle J. & Lenk K. (eds), Der Weg in die "Digitalisierung" der Gesellschaft: Was können wir aus der Geschichte der Informatik lernen? Metropolis-Verlag, Marburg, pp 67–82, p.67–73 where the author brings AI-promises to historical context starting from Alan Touring and remits of modelling and of the need to understand also the limits of modelling as core activity of computer science and software development including design of algorithms in p. 73–77.

102 See Akata Z. et al. (2020) A Research Agenda for Hybrid Intelligence: Augmenting Human Intellect With Collaborative, Adaptive, Responsible, and Explainable Artificial Intelligence. IEEE Computer 28: 281–326. See also Cheruvu R. (2022) Unconventional Concerns for Human-Centered Artificial Intelligence, Computer, vol.55, no.7, 46–55.

103 Schneiderman B. (2020) Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy, International Journal of Human–Computer Interaction, 36:6, 495–504.

104 See Skopik F. et al. (2022), op. cit, see Hernandez-Ramos J. L. *et al*. (2021), op.cit.

and solutions. Care and duties of care need to be at the heart of user-centricness and security. Reconfiguration of the human – machine –relations is needed.[105] Information and communication technology is not only a tool but a mediator of experience and actor influencing on human behaviour and transcending meanings in socio-technical systems.[106] New kind of moral and legal crumble zones emerge and raise the issue on the human autonomy, one of the very foundations of respect for humanity and human autonomy.[107] Legal regulation and remedies concern riginal design, maintenance and repair in the human – machine interaction and confluence in the hybrid architectures with hybrid intelligence. The remit of law extends beyond mere human to human – relations to cover human – computer-relations. Legal informatics cares for the general scientific foundations of this extended realm of law and conceptualises the languages of its legislation.

5. Conclusions

The value of legal informatics has been, is and will in the future be in building shared understanding between computer science, information systems management and science and other data sciences and with socio-technological studies related to law in systematic ways.

Legal informatics aims for and fosters cross-disciplinary understanding of the legal dimensions of current and future phenomena in law's intersection with digitalisation, like legislation on cyber and information security. It also develops and maintains tools and conditions for professional understanding between various disciplines working with digitalization. Such an understanding and putting that to a societal context is one of the paradigmatic challenges of cyber and information security and its legal governance. The general scientific mission of legal informatics and the societal need for it have remained the same during the last 25 years albeit science has advanced tremendously during that time. Technical solutions and contents of law have changed. The concept of data security referring to technical arrangements for the protection of integrity, confidentiality and accessibility and usability of data has become cyber and information security with multiple societal perspectives to digital security and ultimately protection of human autonomy in a world were information and communication technology is embedded nearly everywhere. The role of law is to lay foundations and hold accountable for the creation of a culture of security by design and default and the for the everyday maintenance ad repair this requires. Law also provides remedies for failures in this culture of good security by design and default and in maintenance. Legal informatics is needed to contribute to the understanding of the possibilities and challenges in this design, maintenance and to understand what are the effective remedies and relevant issues in this highly technical but still societal context. Legal informatis is also needed to provide a common community of knowledge between legal profession, sociology and economics and the various branches of data, information systems management and computer sciences.

---

[105] See on a general, philosophical level Jakson S. (2o14) Rethinking Repair. In Gillespie T., Boczkwoski P. & Foot K. (eds) (2014) Media Technologies: Essays on Communication, Materiality, and Society. MIT Press, Cambridge, MA: pp. 221–239, p. 222, 226 and 230–232.

[106] See Rosenberger R. (2020) On variational cross-examination: a method for postphenomenological multistability. AI & Society. https://doi.org/10.1007/s00146-020-01050-7 and generally Rosenberger, R. (2013) The importance of generalized bodily habits for a future world of ubiquitous computing. AI & Society 28, 289–296. See Jackson (2014), p. 222. See also Verbeek P.P. (2011) Moralizing technology: understanding and designing the morality of things. The University of Chicago Press, Chicago, p. 153. See Hauser S., et al. (2018) An annotated portfolio on doing postphenomenology through research products. In: DIS'18, June 9–13, 2018, Hong Kong. ACM, pp. 459–471, p. 460 where postphenomenology is seen as useful in the human – computer – interaction – research (HCI). HCI has taken the mission to situate users to the centre of analyses and of ICT systems development from a multi-disciplinary perspective, see Stephanidis C. et. al. (2019) *Seven HCI Grand Challenges*, International Journal of Human-Computer Interaction, 35:14, 1229–1269, https://doi.org/10.1080/10447318.2019.1619259; Cheruvu 2022; Hochheiser H & Lazar J (2007) *HCI and Societal Issues: A Framework for Engagement*. International Journal of Human[#x02013]Computer Interaction, 23:3, 339–374. HCI is a way of thinking, and, a research and development approach acting to ensure that information systems are at the service of humanity. One of the strategic cyber and information security challenges is to bring security design and HCI together and by law create incentives and duties of care and accountability principles and rules for that.

[107] See Elish M. (2019) Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. Engaging Science, Technology and Society 5:40–60.