Trust on Digital Administration and Platforms

Tuomas Pöysti

1 Introduction and Question

1.1 Trust in Information and Administrative Law

Trust of the citizens towards public administration and towards the use of public power belongs to the goals of Scandinavian administrative law. Trust is one of the underlying principles of justification in the system of administrative law and justice.[1] Administrative law seeks to provide legitimacy by fair procedure and to guarantee good administration. Thereby it creates conditions for trust between individuals and other private parties and public administration. In the practise of Finland's Supreme Guardians of Law, the Chancellor of Justice and the Parliamentary Ombudsman, trust has also been used as an additional legal premise and legal element to be taken into consideration in the interpretation of the rules of administrative law against formalistic and reductionist arguments.[2] Administrative law also establishes rules concerning co-operation between public organisations and foundations for trust and collaboration in the authority to authority -relationships.

Trust is a policy objective in the European Union legislation on digital services and information. In the preamble of the European Union General Data Protection Regulation (EU) 679/2016, hereinafter the GDPR, the significance of trust to the development of digital economy across the internal market is recognised. Creation of trust is set as one of the background objectives of the data protection regulation.[3] The Article 29 Working Party bringing together data protection authorities, established under the Personal Data Directive 95/46/EC and which has now become the European Data Protection Board established by the GDPR, has defined trust as a goal of several elements and provisions in the European Union data protection law.[4] The creation of and the enhancement of

1 Administrative Procedure Act (434/2003) section 6 contains the general principles of administrative law. Impartiality and objectivity is one of those principles and its purpose is among other things to maintain trust and legitimacy, *see* Government Proposal to new Administrative Procedure Act, HE 72/2002 vp., p. 41 where trust is seen as an impact of the legality and observance of the good administration. Confidence is referred to in section 28 (7) of the Administrative Procedure Act concerning grounds for disqualification of a public official in the conflict of interest situations. Confidence refers to legitimacy of institutions whereas trust refers to features in person to person relationships. In the legal literature for example the rules on the conflict of interest is seen to represent general quest to maintain trust and legitimacy, *see* Kuusikko, Kirsi, *Esteellisyys hallinnossa*, Helsinki 2018 (ebook), chapters 1.1. and 1.2.

2 *See* for example Deputy Chancellor of Justice decision on case OKV 4/50/2009, 28.4.2011, which concerned the administrative structures of a municipality (local government entity) and whether the organisation of municipal construction and environmental inspection guaranteed objectivity, impartiality and independence of taking care of these functions in the municipality. The context was the purchaser – producer –model which was taken as a basis for the municipal organisation. According to the Deputy Chancellor of Justice the organisation and activities of public authorities shall also appear to be impartial, objective and secure rights of participation and hence establish citizen trust towards authorities.

3 Paragraph 7 of the preamble of the GDPR.

4 Article 29 Working Party: Guidelines on transparency under Regulation 2016/679, 29 November 2017, WP260 rev.01, available "ec.europa.eu/newsroom/article29/item-

user's trust to new digital technologies is a wider policy objective in the European Union programme for digital single markets.[5]

Trust is in a complex relationship with the rule of law and governance based on the Constitution and fundamental rights and freedoms the Constitution protects. In the literature such governance is called the constitional state.[6] Rule of law contributes to trust. Trust is in close relationship with legitimacy. Currently our societies and public administrations are under profound change – a digital revolution. As a result digital platforms and the networks of services and different service providers become one of the main methods of organisation and ways to deliver service in public administrations. In this piece I will address how law contributes to trust and is able to maintain trust in the age of digital administration and platforms. A further question is how processes of law and legality oversight can help to maintain trust in the changing context of law and administration.

1.2 A Constitutional Practitioner's Perspective

This article is written from the angle of the Finland's Chancellor of Justice, who pursuant to section 108 of the Constitution of Finland is an independent constitutional authority and the Supreme Guardian of Law in Finland. Finland has two Supreme Guardians of Law with similar constitutional powers: the Parliamentary Ombudsman and the Chancellor of Justice. In Finland the institution of the Chancellor of Justice has maintained many of the original features of the Chancellor of Justice in Sweden – Finland from years 1713 – 1808, and, is in some aspects different than the institution under similar name in today's Sweden.[7]

The constitutional duty of the Chancellor of Justice is pursuant to section 108 of the Constitution of Finland to supervise the constitutionality and lawfulness

---

detail.cfm?item_id=622227" (page visited 10.5.2018), *see* also Article 29 Working Party: Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679, 4 October 2017, WP 248.rev.01, available at "ec.europa.eu/newsroom/article29/item-detail.cfm?item id=611236" (page visited 2018-05-31).

5 In the European Commission Digital Single Market Strategy trust appears in several meanings. Trust refers to citizen and consumer trust to the rules concerning across the borders transaction and also to the trustworthiness of infrastructure and particular digital technologies. Closely related to that is user trust to digital services and their security and handling of personal data in those services. *See* Communication from the Commission: Digital Single Market Strategy for Europe, COM (2015) 192 final.

6 On the rule of law in society of networks and constitutional state, which is a state governed by Constitution and material application of fundamental rights and freedoms, *see* Saarenpää, Ahti, E-government and good government; an impossible equation in the new network society? Scandinavian Studies in Law (ed. by Peter Wahlgren), Vol. 47, 2004, p. 245-273.

7 *See* Pöysti, Tuomas, *The General Comment* by the Chancellor of Justice in the Annual Report from year 2017 to the Parliament and to the Government, Parliamentary Documents 2018, Valtioneuvoston oikeuskanslerin kertomus toiminnastaan vuodelta 2017, K 4/2018 vp., p. 12-23.

of the official actions of the Government, the Ministries and the President of the Republic. The Chancellor of Justice is by section 111 of the Constitution required to attend all the plenary sessions of the Government as well as presidential sessions at which the President of the Republic makes decisions on proposals presented by the Government. Pursuant to section 108 of the Constitution of Finland the Chancellor of Justice supervises the legality of courts of law, public authorities and persons and bodies assigned to perform public tasks. In addition, the Chancellor of Justice supervises, from a public interest standpoint, advocates, public legal aid attorneys and licensed attorneys. The Chancellor handles complaints and may perform inspections of authorities and institutions falling within the scope of his supervisory activity. The Chancellor of Justice endeavours to ensure that the courts of law, other authorities and other persons or bodies assigned to perform public tasks comply with the law and fulfil their assigned obligations.[8]

According to the section 108 of the Constitution in the performance of his duties, the Chancellor of Justice monitors the implementation of basic rights and liberties and human rights.[9] Pursuant to the Act on the Chancellor of Justice (193/2000) the Chancellor of Justice may also make proposals to develop and change legislation if he/she has in his oversight activities weaknesses and contradictions or if they have been found in court practise or in administrative practise to be subject for non-coherent interpretations or been subject to confusion or questions on their content.

An important duty of the Chancellor of Justice is the constitutional prior control of the draft legislation prepared in and presented by the Government and the prior control of legislation in the connection with the Government.[10] The supreme prior controller of the constitutionality of Parliament's legislative acts in Finland is pursuant to section 74 of the Constitution the Constitutional Law Committee of the Parliament of Finland.

---

8 On the Chancellor of Justice and its work, *see* "www.okv.fi".

9 The Chancellor of Justice is in the connection with the Government but not under Government. Constitutionally the Chancellor of Justice is a guardian of law, which is independent from the Government and the President of the Republic, see., *see* Government Proposal to new Form of Government of Finland (Constitution of Finland), HE 1/1998 vp., p. 119.

10 On this *see* Pöysti 2018, op.cit. Concerning the Parliamentary Ombudsman and with some observations on the Chancellor of Justice, *see* Nieminen, Liisa, Eduskunnan oikeusasiamies "pienen ihmisen" asialla – joustavuutta vai hampaattomuutta näkökulmasta riippuen, Lakimies, Volume 116, 1/2018 p. 143-176. From the earlier literature *see* Lavapuro, Juha, *Uusi perustuslakikontrolli*, Helsinki 2010, p. 5 and 9-16 and 31-32 on the concept of the control of constitutionality and general remarks on the significance of the Chancellor of Justice and Parliamentary Ombudsman in the control of constitutionality and fundamental rights and freedoms, p.42-43; Hidén, Mikael: *Säädösvalvonta Suomessa*, Osa I eduskuntalait, Helsinki 1974. Specifially on oversight of draft legislation by the Chancellor of Justice, *see* Jonkka, Jaakko, *puheenvuoro oikeuskanslerin kertomuksessa vuodelta 2016*, K 13/2017 vp. p. 12-23 (General comment by Chancellor of Justice Jaakko Jonkka in the Chancellor of Justice Activity Report to the Parliament and Government 2016, Parliamentary Reports 13/2017) and Jonkka, Jaakko, *Oikeuskansleri valtioneuvoston valvojana, Juhlajulkaisu* Mikael Hidén, Helsinki 2009, p. 99-118 and Saraviita, Ilkka: Perustuslaki, Helsinki 2011, p. 930.

Prior constitutionality control of draft legislation is also a forum in which the Chancellor of Justice actively promotes the realisation of fundamental rights and freedoms. Legislator has expressed that the Supreme Guardians of Law should not only limit to ex post assessment of legality and compliance with the law but shall be proactive promoters of the realisation of fundamental rights and freedoms and other rights and provide guidance and advice for that purpose.[11]

Hence, this piece represents constitutional practitioner's self-reflections.[12] The questions of trust and its conditions in law are not theoretical but of profound practical and societal significance. The reliability of the ICT systems and their connections to the realisation of rights appears daily in the practise of the Finland's constitutional supreme legality overseers, the Parliamentary Ombudsman and the Chancellor of Justice. In the Chancellor of Justice daily praxis of the constitutional oversight of legislation the quality and content of the legislation in the digital age appears as a very topical challenge.[13]

1.3 Research Question Defined

Scandinavian societies are societies based on high level of trust.[14] The question is, how this can be maintained in the future and what is the role of information law and administrative law in this in the context of digital platforms and service networks built on these platforms. These networks can be called ecosystems.

We live in a digital revolution which has considerable legal implications, both risks and possibilities. The law has guided the relationships between humans and human created organisations. The law will also steer the relationship between humans and intelligent machines and maybe even be a tool to protect humans from the dysfunctions of the machines.[15] This is part of the methodologic remit

11 *See* the Government Proposal to the Parliament for the Act on the Division of Work Between the Parliamentary Ombudsman and Chancellor of Justice, HE 72/1990 vp., chapter 1.1.

12 I have been appointed to and working in the office of the Chancellor of Justice from 1st January 2018 and therefore I am not in an independent relationship to the institution of the Chancellor of Justice. Prior to that I worked in the Government as Under-Secretary of State for Governance Policy and Digitalisation (Ministry of Finance, autumn 2017) and as Under-Secretary of State responsible for Social and Health Services, County and Central Government Reforms (October 2015 – July 2017). This means that some of the legislation and reforms discussed here have been drafted under my managerial leadership and I have had a governmental expert's influence on the matters. These cases are particularly mentioned in the text.

13 The Constitutional Law Committee of the Parliament of Finland criticised the drafting the European Union GDPR and in particular the proposed Data Protection Act which is to give the general complementing rules in Finnish law to GDPR, *see* Constitutional Law Committee Opinion PeVL 14/2018 - HE 9/2018 vp. The criticism concerned the difficult systematics and difficult to read and understand drafting of the data protection legislation.

14 *See* European Social Survey, "www.europeansocialsurvey.org", *see* also OECD: Governments at a Glance, OECD, Paris 2017.

15 Generally, *see* Council of Europe study *Algorithms and Human Rights – Study on the human rights dimension of automated data processing techniques and possible regulatory*

of the legal informatics and information law within the legal informatics tradition to scientifically and from the material rule of law perspective to assess risks related to digital technologies and to the network society in general.[16] It is a further step in the scientific study and methodical focus on information and information processes in a deeper analyse of law.[17] The law will certainly be needed to create conditions for seizing the opportunities the ICT enables .and to provide new rules of the game.

In this piece I will analyse trust as an objective related to legal certainty and contribute to a general understanding of trust in the context of digital administration and digital platforms.

The context of analyses is administrative law and European information law with focus in the inter-relationship between law and the ideal of shared objectives as foundations of empirical trust. The question is then how a combination of administrative law and information law can contribute to trust and, how trust as a normative ideal can be systemically taken into consideration in the changing law of the digital environment.

I will, additionally, give some recommendations how the idea of trust and legitimacy can be included to the reading and interpretation of GDPR and, I will argue that General Data Protection Regulation and Finland's administrative law both see the law as a planning obligation with an aim to provide predictability, management of risks and other elements of legal certainty. In other words the question here is how the law as planning could become a living and binding promise corresponding to the people's desires for justice and participation.

My piece is written in the context of the anniversary of the Stockholm Institute of legal informatics (Institutet för Rättsinformatik, IRI). Legal informatics, computers and law or in Peter Seipel's original words Computing law is a discipline of inquiry of intersection of law and information and communication technology.[18] Today also various expressions of law and digitalization are used to describe this research field. This approach has to be separated from a doctrinal study of ICT and digitalisation related legal question in various fields of law such as the copyright law or administrative law. Legal informatics is also a scientific discussion arena about legal change bringing together scientific understanding of digital technologies and the law.[19] Such a

---

implications, Council of Europe, Strasbourg, DGI(2017) 12. "rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5" (page visited 10.5.2018).

16 *See* Saarenpää Ahti, *Does Legal Informatics have a Method in the New Network Society?* Society Trapped in the Network: Does It Have a Future? Rovaniemi 2016, p. 51 -75, in particular p. 55 and 66.

17 Wolfgang Mincke has proposed information to lie at the heart of the methods of legal informatics, *see* Mincke, Wolfgang, *Knowledge, Information and Individuals.* Society Trapped in the Network: Does It Have a Future? Rovaniemi 2016, p. 34-50.

18 *See* Seipel, Peter: *ICT Law – A Kaleidoscope View* in ICT, Legal Issues (ed. by Peter Wahlgren) , Scandinavian Studies in Law, Vol. 56, Stockholm 2010, p. 33 – 56. Computing law was the original name proposed by Seipel to what is known as legal informatics of today, *see* Seipel, Peter, *Computing Law: Perspectives on a New Legal Discipline*, Stockholm 1977.

19 Saarenpää 2016, op. cit., p. 61-66.

discussion is needed more than ever to reply to the regulatory challenges of our time. Also this piece follows the broad approach of legal informatics both by the selection of topic, the quest for deeper understanding of the legal implications of the digital technologies and, also methodically aiming to bring a technological perspective to a study of law and regulation.

1.4 Methodological Perspective: Contextual Realism in Law

In a wider sense this study follows an approach of contextual realism which has close connections to law and society –type of approach or sociology and social sciences informed approach to law. Idea is to seek to ensure societal relevance of law and its fundamental principles. This requires particular sensitivity to a context in which law is applied. Alf Ross has defined legal policy as the art of the realisation of justice embedded in law.[20] Contextual realism means this with the emphasis on the understanding of the specific practical contexts within which law is applied. Law in this perspective is not only an abstract normative system but a dynamic system of applied knowledge with an aim of solving problems in specific concrete situations.

The context sensitivity requires deep understanding also the societal, technological and economic features of the practical concrete solutions and systematised collections of legal solutions. Legal rules and principles are, in the contextual realism tested against empiric finding but also tested in relation to scientific theories in social sciences. Such comparisons enable testing of various legal solutions against scientifically reasoned though on how they might operate in practise. This is a particular need in the drafting of legislation but also in the setting future directions of law by giving precedents or by giving future guidance in the course of activities of Supreme Legality Overseers or constitutional guardians.[21]

In contextual realism law is, hence, not following from a single authority and closed hierarchical system. The law is rather an open system combining international, European union and domestic legal sources with knowledge derived from other disciplines in which the weighting of rights is made on the basis of balancing and argumentation and considering the effects of law to the position of individuals in specific concrete situations. Normatively the contextual realism aims at the efficiency of and the realisation of fundamental rights and freedoms as a balanced system in practise and in practical situations. It rejects any arguments of the prima facie superiority of any specific fundamental right albeit right to live and equality as negative freedoms enjoy wide protection in the system of fundamental rights.

This means, that inter alia the right to protection of personal data shall be balanced and reconciled with other fundamental rights and freedoms and arrangements which would danger the balance and balancing in the system of

20 Ross, Alf, *Om ret og retferdighet,* 2. opl. Copenhagen 1966, p. 417.

21 On the value of empiric research and of theories of social sciences in law, *see* Tyler, Tom R., *Methodology in Legal Research,* Utrecht Law Review, Vol.13(3), 2017, p.130-141.

fundamental rights cannot be accepted – a message strongly sent by the Finnish Parliament Constitutional Law Committee on its opinion on the proposed new Data Protection Act and also concerning the way in which the GDPR shall be interpreted. Additionally significant in that opinion is the resolution of a structural tension between the GDPR and Finland's Constitution in favour of the Constitution in a situation where such interpretation would not put the fundamental rights and rights guaranteed by the GDPR into jeopardy.[22] I would emphasise in the reading of the opinion the careful analyses of the context and realisation of the objectives of the GDPR before giving priority to a constitutional arrangement.[23]

Normatively, some of the objectives of contextual realism are included into the Article 25 of the European Union GDPR in the ideal of the data protection by design and default and to the ways in which the Article 29 Working Party has interpreted in its draft guidance on the data protection impact assessments. Scandinavian legal informatics and Scandinavian information law has aimed at a wider definition of the rights-friendly infrastructure or good information management practise guaranteeing in specific information processing circumstances that the legal rights related to information are also effective in practise and written in to the features of technical environment.[24] This can also be seen as a specific dimension of legal certainty and a specific societal requirement for the relevance of law and its fundamental principles in the changing society. [25]

22 Opinion of the Constitutional Law Committee PeVL 14/2018 vp.

23 I was heard twice as one of the legal experts in the Constitutional Law Committee during the preparation of Opinion PeVL 14/2018 vp. Expert opinions are found at "www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_9+2018_asiantuntijalausunnot.aspx".

24 This has become a subject of fairly vast literature. For significant earlier Nordic contributions to the idea, *see* Schartum Dag Wiese: *Data Protection and Privacy – Legal, Technological and Organizational Aspects*, in ICT, Legal Issues (ed. By Peter Wahlgren), Scandinavian Studies in Law, Vol. 56, p.125 - 147.

25 Pioneer studies in this field in Scandinavia are Magnusson-Sjöberg, Cecilia: *Rättsautomation - särskilt om statsförvaltningens datorisering*, Stockholm 1992; Magnusson-Sjöberg, Cecilia: *Legal management of information systems: incorporating law in e-solutions*, Lund 2005; Schartum, Dag Wiese, *Rettssikkerhet og systemutvikling i offentlig forvaltning*, Oslo 1993; Wahlgren, Peter, *Automation of legal reasoning : a study of artificial intelligence and law*, Stockholm – Deventer 1992; and Kuopus, Jorma, *Hallinnon lainalaisuus ja automatisoitu verohallinto:oikeustieteellinen tutkimus kansalaisen oikeusturvasta teknistyvässä valtionhallinnossa*, Helsinki 1988. These studies bring relatively early and earlier than the later internationally acclaimed work by Lessig, Lawrence, *Code and Other Laws of Cyberspace*, New York 1999, the incorporation of law and realisation of rights from the legal certainty perspective to the systems design and automation. All these studies had a look on legal application systems or development of automated administration. Jorma Kuopus' dissertation, for example, analysed the tax administration, which since then has been one of the lead areas in the use of electronic and digital solutions and nowadays the digital platform approach and the artificial intelligence. Only now in the earlier promise of automation seems to be realising in practise and the theoretic points discussed in early 1990s are again highly relevant albeit technical enviroment is different and legal systems are partly, but only partly, more mature to encounter the intelligent machines.

Technically the challenge of law is how to write law to provide rights by design and default in the current digital platforms and digital administration. Governance and management challenges specifically required by the GDPR but systemically also required by the practise of the Parliamentary Ombudsman and Chancellor of Justice in Finland as a duty derived from the general principle of legality is the management of risks related to fundamental rights and freedoms.[26] From a scientific perspective rights by design and default needs a multi-disciplinary and multi-professional study of the circumstances in which the law is applied and how law can be written into the technical environment following rights by design and default approach.

Theoretically this requires an approach to law as moral, societal and technical planning inspired by Scott J. Shapiros ideas of law as moral planning.[27] Legal work and legal method calls for a systemic and systematic risk management and this increasingly concurs with a general theory and practise of risk management developed in various aspects computing, management and administrative sciences. Contextual realism is scientifically based juridical risk management and application of these methods also in the writing and practise of law.[28]

The multidisciplinary approach to the practise of legislative drafting and law concurs with the ideas of Panu Minkkinen on the law and legal science as a science of law, justice and society reaching beyond the classic boundaries of dogmatic law albeit Minkkinen does not discuss technology and law as a specific example.[29] From a more practical perspective law in this dimension of rights by design and default becomes a project management and planning issue. Quite often the information design and project design may be obstacles to rights by design. Hence the control of the project management will become increasingly part of the realisation of justice itself. To the many good practises in law also the good project management could be included.[30]

---

26 *See* Art. 24 and 25 of the GDPR for a risk-centric approach where the core of data protection and information and cyber security duties is seen as a management of the relationships between the general data protection principles and the risks related to those principles and to fundamental rights and freedoms in general. *See* also the draft guidance by the Article 29 Working Party, *Guidelines on Data Protection Impact Assessments*, wp 248.rev01, op.cit.

27 *See* Shapiro, Scott J, *Legality*, Cambridge 2011; Canale, Damiano & Tuzet, Giovanni, *The planning theory of law : a critical reading*, Dordrecht ; New York, 2013. which is critical collection of essays discussing Shapiro's book Legality. To Shapiro law is institutionalised social planning. Critique raises the fundamental challenge between normativity and empiria and that Shapiro is convincingly passing the quilliotine separating them. Shapiro's law as social planning seems to function in the universe of legal facts, not in the empiria of the societal facts of parliaments, courts and real-life legal arguments. Nevertheless this approach opens up interestingly to the sociology of law and is particularly appealing in the case of GDPR which is written as a masterplan for societal and systems planning.

28 On the legal risk management *see* Wahlgren, Peter, *Juridisk riskanalys: mot en säkrare juridisk metod*, Stockholm 2003.

29 Minkkinen Panu, *Oikeus- ja yhteiskuntatieteellinen tutkimus - suuntaus, tarkastelutapa, menetelmä?* Lakimies, Volume 115, 7-8/2017, p. 908 - 923 (Socio-legal studies, an approach, a perspective a method?).

30 Saarenpää has observed in his analyses of the legal network society the inclination of modern information law and administrative law towards requirement of observance of good practise

2 Setting the Scene: the New Digital Revolution

2.1 Technological Change with Profound Impacts

Law is a mirror of its society and also of the technologies of the time. This is evident in the case of data protection (protection of personal data) albeit there are legitimate and constant claims for technology neutrality of legislation. These claims are more expressions of desires for justice beyond the daily surface of applications which come and go; quest for justice beyond the daily fashions in management and regulation. The desire for technology neutrality but a constant return to always be the mirror of technology and society holds even for administrative law even though it may appear to be more distant and, more neutral to the technologic issues of the day.

Today we live in very exciting times. A silent but certain revolution takes place under our eyes, hidden in our everyday lives. We move to a digital age. The World Economic Forum calls it with good reason the 4th industrial revolution. Digital technologies are increasingly embedded to our everyday environment and life. The question is not any longer of automatization enabled by digital technologies but a fusion of all sorts of technologies enabled by digitalisation and ICT which blurs the boundaries between the physical, digital and biological spheres. The impact to the economy and business, government, work and people is systemic and far-reaching.[31]

The change we witness does not realise trough big political declarations or trough violent political upheavals. But, it may lead to and will lead to such upheavals if change is not led and managed properly. The change happens in the advancement of information and communication technologies (ICT) and in the profound digitalisation of the everyday life which follows as a result of that. The form and functioning mode of digital technology is also under change. We are quickly heading towards an age of distributed, autonomic and intelligent systems in an environment in which networks, networking capability and at least some smart features are embedded in nearly every device.[32] These devices can be connected through internet of things (IoT) applications and are steered trough intelligent assistant computers. Following exponential Moore's law the capacity of data processing has increased and so has the amount of data. Rough estimates of the amount data in 2025 by some market analysts and forecasters is around

---

as a regulatory strategy to address uncertainties but take constitutional rights seriously, *see* Saarenpää 2004, op.cit.

31 Term 4th industrial revolution is particularly used by World Economic Forum, *see* Klaus Schwab: The Fourth Industrial Revolution: what it means, how to respond. Foreign Affairs, December 2015. *See* also the thematic pages of the World Economic Forum on the 4th industrial revolution, "www.weforum.org/agenda/archive/fourth-industrial-revolution" (page visited 11.3.2018).

32 Already this creates a challenge from the data protection perspective, *see* van Dongen, Lisa; Timan, Tjerk. *Your Smart Coffee Machine Knows What You Did Last Summer: A Legal Analysis of the Limitations of Traditional Privacy of the Home under Dutch Law in the Era of Smart Technology*, SCRIPTed: A Journal of Law, Technology and Society vol. 14, no. 2 (December 2017): p. 208-238.

160 zettabytes.[33] The amount of data and also new scientific data has dramatically increased during the recent years. While the estimates are rough and may methodologically be controversial, the finding is that there are huge volumes of data ad these volumes get bigger.

Data is everywhere and it is processed while data protection law still speaks about data minimisation principle in Art. 5 subpara 1c. We live in the age of massive big data. Machine learning and other forms of artificial intelligence (AI) and thereby powerful intelligent systems are coming around. The AI requires data, both big data and smart data, to learn to function better and to deliver problem-solving and entertainment it is entrusted for. The intelligent machine will increasingly be able to read in data without typing or recording it intentionally. Voice recognition is increasingly a powerful technology and with it the intelligent, AI based personal assistants enter into our daily lives.

But there is more to come. Through functional magnetic imaging techniques measuring brain activities and combining that data to the deep neural networks we can come pretty close to replication of the human brain functions.[34] Also through face recognition and image processing it is possible, with powerful algorithms and enough data, come pretty close to mind-reading. The intelligent computing is close also to arrive at a certain point and level of cognition of its own. The list of potentially disruptive technologies is amazing, some may sound lunatic but many will be reality.[35] Also some science fiction scenarios – based on the existing and known scientific knowledge – on brain emulations etc. can be a reality.[36]

This means that we move quickly from PCs and central computers to distributed, autonomic and intelligent systems. However, on the same time cloud computing and other concentrated and shared resources bring a new type of centralisation to computing. Why do I speak about PC in this context? Because the PC is de facto of the underlying assumptions of some of the laws still in place, for example Finland's Act on the Electronic Services and Communications in the Public Sector (13/2003), which is based on the assumption of personal computers and e-mails. Despite policy agenda saying

---

33 *See* IDC's Data Age 2025, IDC White Paper 2017. "www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf" (page visited 15.3.2018).

34 For a generalist introduction *see* Shilo Rea's webarticle *Beyond Bananas: CMU Scientists Harness "Mind Reading" Technology to Decode Complex Thoughts*. Carnegie Mellon University. Dietrich College of Humanities and Social Sciences, "www.cmu.edu/dietrich/news/news-stories/2017/june/brain-decoding-complex-thoughts. html" (page visited 12.3.2018). For a scientific report on the research, *see* Jing Wang, Vladimir L Cherkassky and Marcel Adam Just: Predicting the Brain Activation Pattern Associated with Propositional Content of a Sentence: Modeling Neural Representations of Events and States. Human Brain Mapping. Vol 38 (2017), p. 4865-4881, also available at "www.ccbi.cmu.edu/reprints/Wang_Just_HBM-2017_Journal-preprint. pdf".

35 For an overview chart of disruptive technologies, *see* the table compiled at the Imperial College, London at "www.imperialtechforesight.com/future-visions/87/vision/table-of-disruptive-technologies.html" (page visited 12.3.2018).

36 Hanson, Robin, *The Age of ERM, Work, Love and Life when Robots Rule the Earth*, Oxford 2016. The book is fascinating in its realism: scenarios are developed by simply applying what is scientifically known today.

other things, some public administration services are still unusable with mobile devices and require a PC. This concerns for some of the employment services, for example. This issue is currently pending at the Chancellor of Justice.

One of the most significant changes is that smart individual and distributed systems can be connected to centralised computing resources and power trough platforms. Digital platforms also connect individuals whether private individuals or businesses. Digital platforms also enable flow of multiple data to feed AI and complementing centralised could computing and vast raw data from multiple sources with small smart mobile applications helping in a variety of everyday situations and in the conduct of business and administrative matters. We have entered into the era of digital platforms.[37]

2.2 Digital Platforms

Digital platforms together with internet including internet of the things and other networks together with cloud computing enable also networks of various solutions and services (ecosystems) emerge and function – the ecosystems are built upon platforms and data the services within the frame of a platform. Platforms bring together the most powerful processing of big data brought together with distributed autonomic and intelligent systems. This provides unpresented mobility and use of data with unpresented economies of scale and economies of scope. Blockchain technologies provide opportunities for decentralised databases and trust on their content against changes and, also, technique for smart contracting.

The AI requires data, both big data and smart data, to learn to function better and to deliver problem-solving and entertainment it is entrusted for. The human-machine partnership and the intelligent machine as an enhancement of the human capacities and capabilities, simply as a continuation of human mind and body, will create a very powerful duo or network. Already this has considerable legal implications, both risks and possibilities.

Public and private organisations are ways in which technology, production factors such as labour and capital and information are combined in the production processes. In particular organisation is a method to organise information processing and manage informational asymmetries. Digital revolution will change organisations and this has, and should have, a profound impact on the various layers of law.

The new model of organisation is platform to which a network of actors and services is attached. This dynamic network is the ecosystem. The fundamental model of administrative organisation – and also of business organisation – will be the platform and ecosystem. The change from the Weberian bureaucracy is significant. But on the same time many fundamental principles remain the same.

37 For a Finnish general perspective to megatrends in technology, *see* Elina Kiiski Kataja: *Megatrendit* 2016, Tulevaisuus tapahtuu nyt, Sitra 2016 and the Finnish Government foresight assessments on global change factors, *Valtioneuvoston yhteiset muutostekijät*, *Valtioneuvoston kanslia*, Helsinki 2017 and Government's National Foresight Network website “www.foresight.fi” (page visited 12.3.2018).

The art and wisdom of legal and juridical leadership is to be able distinguish which issues are genuinely changing and in which there is only a search for up-to-date interpretations.

This change and fluid mixture of the old and the new, are now the foundations for the application and development of information law and administrative law. The European Union GDPR recognises the role of platforms and contains rules to realise data protection in the platform environment. Art. 26 of the GDPR addresses joint controllers of personal data. With the rules on the joint controllership the GDPR aims to address the fairly difficult relations in the platforms. At the policy front the European Commission endeavours to build in a fair and innovation friendly platform economy as part of the European Union Digital Single Market. [38]

2.3 Public Sector Reforms based on Digital Platforms in Finland

Finland is implementing a digital ecosystem and platform based approach to the reform of public administration and production of public services. Finland has during the electoral period 2015 - 2019 in accordance with the programme and strategy of Prime Minister Juha Sipilä's government pursued a historically large and ambitious administrative reform agenda. It includes (a) comprehensive social and health services reform together with a regional administration reform (County Reform);[39] (b) reform of transport services and road and railway services towards digital mobility as a service concept; (c) digitalisation of all public services and d) promotion of the use of AI in society and in public administration. Concerning the use of AI the government is preparing a report to the Parliament on AI and data policy. The benefits of AI will namely realise only if AI is attached to a platform where it can be used across sectorial boundaries and where there is vast amounts of data to be analysed. Albeit AI can also function in small applications much of the potential of AI require thus attachment to a digital platform and availability of a variety of data for analyses.[40]

In addition to these initiatives the Government works to realise a common spatial data platform and foster it to develop to an ecosystem as one of the programmes under the Government's digitalisation agenda. The Government has presented in May 2018 a Report to the Parliament on Spatial Data Policy. Spatial data is defined and the legal foundations for such policy initiatives are in

38 Commission Communication on Online Platforms, COM (2016) 288. Commission Communication on the Mid-Term Review of the Digital Single Market Strategy. A Connected Digital Single Market for All, COM (2017) 228 final.

39 The Author of this article was between October 2015 – 2017 Government's Project Lead for this reform.

40 *See* on the preparation of the Report on data policy Ministry of Finance specific website for the drafting of the report, "vm.fi/tietopoliittinen-selonteko?p_p_id=56_INSTANCE_ hzZR Jcm3o8tR&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=2&_56_INSTANCE_hzZRJcm3o8tR_languageId=sv_SE" (page visited 11.5.2018).

the European Union INSPIRE Directive 2007/2/EC and on the national Act on Spatial Information Infrastructure (421/2009). The Government aims to have the most competitive and most secure spatial data ecosystem which would enable different kind of knowledge management, bio-economy and mobility as a service –solutions and services. To realise this vision the Government report to Parliament seeks to establish a concrete action plan on the quality and real-time machine readable access to spatial data. Action plan will require also legislative changes. [41]

The Parliament has passed a new Act on the Transport services (320/2017) in several stages. Government Proposals for a comprehensive reform of the regional administration and social and health services and for the increased freedom of choice in social and health is pending at the time of this writing at the Parliament.[42] Government has also made a proposal for an Act on the Secure Secondary Use of Social and Health Data, which would create a secure environment for data-analytics and anonymized and pseudonymised use of the social and health data.[43] The government proposal is at the time of writing this article pending in the Parliament where the Social and Health Affairs Committee is finalises its Committee Report on the proposal. The Constitutional Law Committee has given its opinion on the proposal for the Act on Secure Secondary Use of Social and Health Data and required some amendments in order to ensure constitutionality and conformity with the GDPR.[44]

The National Service Gateway "suomi.fi" is in the operational service. It is based on the Act on the Common Support Services for e-Govermenment (571/2016), the the so called National Service Gateway Act. Government is also drafting a new Information Management Act which would bring together currently separate Act on Electronic Services and Communication in the Public Sector, Act on the Common Support Services for e-Government (National Service Gateway Act), Archives Act (831/1994) and provisions on the good information management of the Openness in the Government Act (621/1999). The idea is to have legislation following the model of life cycle of information. Idea also is to concentrate provisions on the information management and data, information and digital services architecture on the same Act of general application in the public sector. A working party has presented an outline for the contents of the Act and Ministry of Finance has commissioned a working party to prepare a draft government proposal.[45] In legal literature the need to assess and compile

41 On the Report on the Spatial Data Policy, *see* Government Report VNS 2/2018 vp., and the Ministry of Agriculture and Forestry web-site "mmm.fi/paikkatietoselonteko" (page visited 14.5.2018).

42 *See* Government Proposals 15/2017 vp., and 16/2018 vp.

43 Government Proposal HE 159/2017 vp.

44 *See* Constitutional Law Committee Opinion PeVL 1/2018 vp. Particularly the possibility to deliver social and health services data without anonymization and without data subject consent to be used in private research and development activities was considered to be in contradiction with the fundamental right to protection of personal data and not in accordance with the GDPR Art.9 rules on the processing of data belonging to special categories.

45 *See* the Ministry of Finance press statement and the decision to establish a working party for law drafting, 11.1.2018 at "vm.fi/artikkeli/-/asset_publisher/tiedonhallintalain-valmistelu-

currently rather fragmented provisions on the information management is well recognised.[46]

The legislative framework calls upon a reform of the Act on the Electronic Processing of Patient and Client Data in Social and Health Services, on which a proposal is expected, also to align current rules with GDPR. On the same time there is a need also the consider revision of Patient Act (785/1992) and Social Services Client Act (812/200) in order to fully and substantially align Finnish legislation with the GDPR in social and health services and to provide foundations for comprehensive integration of social and health services with each other. The digital platform and service ecosystem would additionally need the revised Biobank Act (688/2012) and a new Genome Act which would address the specific questions of biobanks and biologic samples from humans and carrying out genomic research and use of genome data. Social and health services reform, proposed Act on the Secure Secondary Use of the Social and Health Data, revision of the Biobank Act and the project on Genome Act relate also to the growth strategy in health sector where health and also social services sector is seen as a potential source of economic growth and new business opportunities through the possibilities of performing research and development with data analytics on social and health services data and on genome data and biobanks data.

Hence, several public services and administrative law reforms have taken, at least in principle, the model of platforms and ecosystems built on them as a fundamental organisational model. Legislation is then developed around the concept of platforms. The new Act on the Transport Services defines roads, railways and water routes as a platform for public and private operators to provide mobility services. The new act is a move from classic regulation of roads, railways and the services provided therein including taxi, bus and other public transport services to see the whole transport network as an infrastructure enabling digitally steered and also digital services and mobility as a services combining several methods of transports. To enable this, the transport service providers are required by law to provide essential data real time via open interfaces as machine readable open data trough application programme interfaces.[47]

Similarly the platform and service ecosystem model is one of the lead ideas of the Finland's comprehensive social and health services reform. The reform is based on the ideas of the gathering the commissioning and organisation of social

---

jatkuu-hallitusohjelman-tavoitteiden-mukaisesti" and the Ministry of Finance Working Party report on the development orientations of the legislation concerning public sector information management, Valtiovarainministeriö, Tiedonhallinnan lainsäädännön kehittämislinjaukset, Valtiovarainministeriö 37/2017, available at "vm.fi/documents/10623/306884/37_2017_Tiedonhallinnan+lains%C3%A4%C3%A4d%C3%A4nn%C3%B6n+kehitt%C3%A4mislijaukset.pdf/c1f679f5-a26b-4308-9162-c395b3f5d093/37_2017_Tiedonhallinnan+lains%C3%A4%C3%A4d%C3%A4nn%C3%B6n+kehitt%C3%A4mislijaukset.pdf.pdf" (page visited 13.5.2018).

46 *See* Voutilainen, Tomi, & Oikarinen, Tommi, Teknisten *käyttöyhteyksien sääntely*, Oikeus, Vol. 45, 2/2016, p. 260 - 268, in particular p. 267.

47 *See* part III chapter 2 of the Act on Transport Services.

and health services to autonomic counties (regions); the integration of primary, secondary and tertiary care with other health services vertically and also horizontally with social service; increased user's freedom of choice and use of market mechanism in the production of social and health services; revision of the financing of the organisation of social and health services and digitalisation of social and health services and promotion of health and welfare.

According to the Goverment Proposal the new counties will have directly elected councils as supreme decision-making bodies and they will be responsible for 26 compulsory and 5 additional tasks defined in legislation including social and health services, emergency and rescue services, regional development and various regional administrative services and employment services. There will be 18 counties in Finland to which tasks from around 400 different administrative organisations will be gathered. Each county will be defined as controller of social and health data concerning inhabitants in its territory and counties will additionally be controllers of client data on other services they are responsible. However, certain exceptions to this main principle may appear. [48]

At the time of writing this article the fate of the regional and social and health services reform is still open. The Parliament waits the Opinion of the Constitutional Law Committee on the proposed Act on the Freedom of Choice in Social and Health Care.[49] The increased freedom of choice has proven to be very controversial and it also entails very difficult constitutional considerations. Constitutional Law Committee rejected the earlier Government proposal for freedom of choice by considering it unconstitutional because of the risks and impacts the Act would have had on the equality in access to social and health services and the obligatory privatisation the proposal entailed. The Constitutional Law Committee in particular rejected the proposed transfer of the production of services, where the individuals' freedom of choice would have been the main principle, to limited liability corporations, to be against the constitutional provision of each person's right to sufficient social and health services as provider further by an Act of Parliament.[50] Politically and particularly among current local government sector the establishment of Counties is also somewhat controversial but this controversy is rather political than constitutional.

---

48 *See* Government Proposal HE 15/2017 vp. For comprehensive documentation and up to date information on the social and health services reform and regional government reform, *see* "alueuudistus.fi" (page visited 12.5.2018).

49 HE 16/2018 vp.

50 Constitutional Law Committee Opinion PeVL 26/2017 vp. on Government Proposal HE 47/2017 vp. The author of this article does not have an independent relationship to that proposal nor to proposal HE 15/2017 vp. on the establishment of Counties and reform of the organisation of the social and health care since I have been as the Government's Project Lead on the county reform and social and health services reform, Under-Secretary of State for Governance Policy and as the rapporteur for the Government on the proposal HE 47/2017 vp. The Constitutional Law Committee did not concur with neither my nor with the Government's overall assessment on the constitutionality of the proposal. My assessment was that there were risk but they were sufficiently mitigated and that Constitutional Law Committee could have taken the proposed interpretation of Constitution.

The main organisational and policy principles in the reform of social and health services are 1) transfer of organisation and commissioning of social and health services from municipalities, local government entities, to 18 new counties which would have a directly elected council as the supreme decision-making body, 2) comprehensive integration of social and health services so that the same organisation, county would be responsible for organisation of both primary, secondary and tertiary care and social and health care with each other; 3) curbing cost increases with almost 1,5 percentage points to GDP, that is 3 billion euros between 2019- 2029 compared to the basic scenario of cost development forecasted in 2015, and, improving equality in access to care and services and 5) full digitalisation of both health and welfare promotion, preventive services and the social and health services.

The comprehensive integration of care and services requires full integration of patient and client data with health and social services histories. The costs savings depend to a major extend on the success of the profound digitalization of the way in which the whole service system functions. An independent international panel of experts collected by the WHO affiliated European Observatory on Health Policy has found that the reform has, in the light of international experience, right elements but caution and sufficient transition time and a careful approach is required in the enlargement of freedom of choice and digitalisation needs wise and determined leadership.[51] Nevertheless of the outcome this reform package is an interesting legal and governance case study from diverse aspects. In addition the digitalisation and digital platform approach is not dependent on the controversial freedom of choice or county reform part albeit also they would facilitate the passage towards that.

2.4 The Architecture of Public Digital Platforms in Finland

The overall architecture of the public digital platform consists of the core data, data exchange layer provided by the national service gateway and application and functional solutions layer in which substantive services are provided and processing of substantive data takes place. The goal is also to open the application layer to private sector partners either as developers and providers of additional added value services or to be service providers in the provision of public services. Core data is complemented by information from the statutory basic registers.

Basic registers are national registers and data repositories and statistics compiling significant and comprehensive data for the functioning of the entire society, Basic registers have statutory duties and foundations and which often have according to law public trust. Basic registers have reliability, multiple use and specific data protection and information security arrangements. Basic

51 Couffinhal, Agnes, Cylus, Jonathan, Elovainio, Riku, Figueras, Josep, Jeurissen, Patrick, McKee, Martin, Smith, Peter, Thomson, Sarah and Winblad, Ulrika, *International expert panel pre- review of health and social care reform in Finland*, Ministry of Social Affairs and Health Reports and Memorandums 2016:66, Helsinki 2016 "/urn.fi/URN:ISBN:978-952-00-3848-9" (page visited 12.5.2018).

registers include population register, national data base for enterprises, foundations and associations, real estate register and register on buildings. [52]

Public trust means that data and information in them is considered reliable and valid unless it is specifically proven not to be correct. Such basic registers maintain also legal certainty and security and, if basic registers are well protected and carefully maintained, provide better protection for personal data and information security compared to a situation where many public authorities would collect and reproduce personal data for example on the population and addresses. Foundations for public trust is maintained in a way that inclusion of data to basic registers is an official act of public authority and legislation contains specific rectification methods and procedures in case of erroneous data.

It is a long time data and information policy in Finland to reduce collection of data and organise multiple use of data collected to the basic registers. This idea of collecting information only once is still today one of core digitalisation policy principles established by the Finnish Government.[53]

Finland has national patient and social services client data registers and archives (Kanta) which will be developed further to provide a functional platform for new social and health services organisation and a centralised database and active archive for health and social services patient/client data.

Government has presented to the Parliament a Bill for an Act on the Secure Secondary Use of Social and Health Services Data. The Bill is based on the ideas developed in a joint venture with Finnish Future and Innovation Fund Sitra. The Act would create conditions for the secure secondary use and the anonymised and pseudonymised secondary use of social health data for research and development purposes.[54]

Private information sources and MyData type of solutions can be attached to the platform and ecosystem additionally. The Idea is to create an ecosystem of both private and public services build on a publicly owned platform and common core data. Legislative framework will be complemented by revised Act on the Electronic Processing of Client Data in Social and Health Care Services, revision of the Act on Biobanks and the new Act on Genetic Data.

Core data on patients and clients in health and social care and services and other services is to be provided by the Counties as data controllers pursuant to GDPR and complementary national legislation. Counties will be data controllers even in the case private sector service providers would be responsible for the production of care. National Social Security Institution Kela is responsible for the maintenance some data archives and depositories and of the maintenance of some ICT systems to be used in the social and health care system. Pursuant to Article 6 (1) c and e subparagraphs on the legal basis for processing to comply with legal obligations of the data controller and for processing which is

52 *See* Korhonen, Rauno, *Perusrekisterit ja henkilötietojen suoja*, Rovaniemi 2003, p. 9- 13 and 224-293.

53 The principles of digitalisation of the Government, adopted by the Government of Finland, are available at the Ministry of Finance web-site at "vm.fi/digitalisoinnin-periaatteet" (page visited 12.5.2018).

54 *See* Government Proposal to Parliament HE 159/2017.

necessary for the performance of a task in a public interest require that in these cases the legal grounds for processing of personal data shall be given in a specific Union or Member State Act. This is an area in which the GDPR may be complemented by national rules. These national rules shall, however, stay within the limits given by the GDPR.

The Constitutional Law Committee of the Finnish Parliament has considered that these specific acts should be limited to minimum and a general act, the proposed Data Protection Act, should in most cases be sufficient general Act of Parliament to provide the complementing national rules. In these two situations referred to in Art. 6 c (processing necessary for the compliance with the data controller's legal duty) and 6 e (processing necessary for performing a task in the public interest) the requirement of the founding data processing for a specific Act of Union law or Member State law is to protect the consent as a genuine exercise of individual autonomy and informational self-determination. Consent may not be used in situation where the parties are in a considerable unbalance with each other.

In the case of health care and social services the situation at the appointment is not of an equal character since the patient is quite often seeking help to acute problems and can be on a dependent position to the medical or social service provider. That is one of the reasons for which the Parliament's Constitutional Law Committee did not accept medical appointment as a situation where consent for the use of samples and data for development and innovation purposes under the Act on Secure Secondary Use of Social and Health Data may be given. [55] The GDPR is in this regard rather clear and classic on the roles of private and public sector; consent and contractual relations are for the private law situations and acts of administrative law shall regulate grounds for processing necessary for the purposes of public interest and public functions. This has good potential for social conditions for trust; either there shall be consent of equal partners or the processing rests on democratically legitimate legislation and trust emerges from the proper and inclusive legislative procedure.

The GDPR here is, however, a bit problematic in relation to digital platforms provided by the public sector. The whole idea of the platforms is to be able to provide additional services on request. The legal bases and the possibility of the individuals voluntarily opt for a government service and to a use of government platform remains vague. The GDPR here, as the Union law in general, does not follow an organisational approach but a functional one and it is the functional nature of the data processing which is decisive on the choice of the legal foundations for processing. The objective of GDPR by this is to require adequate and objective protection measures and to objectively ensure the necessity of processing for those particular legal obligations of the data controller and, for specific public interest obligations. Member State law can complement Union legislation concerning voluntary services in the public administration platforms. The basic foundations shall be given by the democratically legitimate legislative authority, the rules of the game are not for individual administrative agencies or developers to decide.

55 Opinion PeVL 1/2018 vp.

Common core data is, hence, provided by the national social and health care data registers and databases and national archive. This is called the Kanta -platform (this is also called Kanta –archives) which technically consists of different data repositories such as electronic prescription, medication database, archive of patient data and also the archive of social services client data, information management service and My Health Information, the user's own data file service (Omakanta) which compiles each user's own patient data with some of MyData -features.[56] Legislative foundations for the Kanta services are the Act on the Electronic Processing of Client Data in Social and Health Care (159/2007) and decrees passed on the basis of these acts. The system functions as an active repository of all client and prescription data in health and social care.

The Act on the Electronic Processing of Client Data in Social and Health Care is under review and a draft for a new Act has been under public consultation procedure. The revision will create foundations for the inclusion of social services client data to the Kanta services and facilitate the use of data.[57] In the future the data can be analysed across the sectors of the social and health services and clients can also add their own data and data from application user has authorised to collect and provide data to OmaKanta (My Health) Information service which is part of the Kanta system of solutions. In addition the data on the biobanks in accordance with the Act on Biobanks can be connected to the analyses of data in the national repositories.

Personalised medicine is a strong development direction in social and health care. Essential part of the current and future personalised medicine is use of genome data and therapies based on genomic technologies. Personalised medicine can be a methodical approach to seek after more cost-effective health care.

. Risk analyses based on the genomic data can also be a powerful tool to advance health and prevent diseases. Finnish Ministry of Social Affairs and Health pursues a systematic strategy for utilisation of genome data in the health services and also in the business ecosystem around health.[58]

Following the National Genome Strategy preparation for an Act on Genome Data and establishment of a National Genome Centre to support utilisation of genome data and to provide for a national genome data repository is under way.[59]

---

56 For a general presentation of the system *see* Kanta www-site, "www.kanta.fi/en/kanta-palvelut" (page visited 17.3.2018) in which also the privacy statements of the Kanta services are available.

57 On the law drafting process and the replies to the public consultation *see* the thematic page of the project on the Government Proposal for an Act on the Electronic Processing of Client Data in Social and Health Care Services, "stm.fi/hanke?tunnus=STM022:00/2017" (in Finnish).

58 *See* Finnish Ministry of Social Affairs and Health: National Genome Strategy of 2015 and the thematic pages of the Ministry for improving health through the use of genome data, "stm.fi/en/genomicdata" (page visited 17.3.2018).

59 *See* the evaluation memorandum of the working party established by the Ministry of Social Affairs and Health on National Genome Centre, which has also assessed the need of and provided an outline for the content of the Act on Genome Data, Ministry of Social Affairs and Health 22.12.2017, "stm.fi/documents/1271139/6033514/Genomikeskustyöryhmän

Genome data belongs to the special categories of personal data according to the Article 9 of the GDPR even though not all genome data has particular value or sensitivity and not of all data can individual be identified. Due to the designation of genome data to be one the special categories of data defined in Art. 9 of the GDPR, the use of genome data requires specific protection measures to safeguard fundamental rights. There are plenty of genuine risks related to privacy and integrity of human beings related to use of genome data albeit there are also enormous opportunities. The use of genome data and genome technologies are thus a very important subject for regulation from the fundamental rights perspective.[60] In the Finnish national law-drafting the issues on national freedom of manoeuvre with regards to the Article 9 of the GDPR has proven to be one of the most challenging and difficult topics.[61]

Vision in the Finnish Government social and health services ecosystem is to be able to connect nation-wide genome database with other national registers and databases. Goal is also to provide this data pool in a secure, anonymised and pseudonymised form for research and development purposes and for the steering of health and welfare promotion and social and health services.

Counties would not only be responsible of social and health services but a range of 30 different services ranging from the rescue and emergency services to regional development and employment and enterprise advisory and promotion services with unemployed persons support to maintenance of environmental health, agricultural administration and regional planning and water areas protection and maintenance. This means that all legal residents of Finland will be clients of the counties and through various roles also enterprises will at least indirectly be customers of counties. In particular the ability to combine employment and social services and health services data would serve well those persons who are in a unfavourable labour market position.

Recently, for example, a wide Government commissioned working party on rehabilitation proposed that rehabilitation should be defined as a customer-need based and targeted process in which the person in need of rehabilitation advances his functional and performance abilities and work abilities and his working and living environment with the help of professionals. [62] The rehabilitation as a process requires joint functioning model across various service providers and organisations, fluid transfer of data in the process and joint and at least interoperable information systems concerning client data and patient data. A common client plan on the measures to be taken in the rehabilitation process is

---

+arviomuistio+22+12+2017.pdf/21cfeec9-f634-4f6c-b2a98262914e3c03/Genomikeskusty öryhmän+arviomuistio+22+12+2017.pdf.pdf" (page visited 17.3.2018).

60 *See* the opinion of the Chancellor of Justice on the regulation of genome data, 24.1.2018 Drnno OKV/78/20/2017 "www.okv.fi/media/filer_public/0f/97/0f97eb9e-5463-4bd0-89f7-aba9f887be6b/okv_78_20_2017.pdf".

61 *See* the Ministry of Justice commissioned Working Party on the implementation of the GDPR in Finland, EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö, oikeusministeriön mietintöjä ja lausuntoja 35/2017, Helsinki 2017, p. 21., available at "urn.fi/URN:ISBN:978-952-259-612-3".

62 Ministry of Social Affairs and Health, Rehabilitation Committee , p. 36

an important tool to achieve targeted and systematically planned entirety of measures.[63] The free flow of data and interoperability of data across systems needs to be ensured. This requires definition and legal regulation of the information and data structures required in the rehabilitation process, otherwise various actors will not achieve in the sufficient amount of coordination.[64]

Rehabilitation is here simply one example of the services in which counties and their ability to combine structure data across various organisations will be crucial to the attainment of the societal objectives of the welfare state and social protection policies and to the effective realisation of fundamental rights and other legal rights of the individuals. Such solutions would, for example, in particular help many of the long term unemployed persons, since among them there is high probability for disabilities preventing full participation to labour markets.

The quality of the information infrastructure and the user-centredness is seen in the legal literature as guiding second order principles of law on public sector information management.[65] On the other hand such information processes and enabling platforms need careful legal regulation and special protection measures by law and technical and organisational means since this also means fluid movement and combination of data belonging to the special categories of data pursuant to Art. 9 of the GDPR. The GDPR gives a rather liberal environment for the use of the data for health care and social protection so the vision of transportable data widely available in social and health services can be realised within the GDPR.

The processing of special categories of personal data poses, however, also very specific risks to privacy, private life and eventually to other fundamental rights and freedoms albeit it is concurrently very much needed for the effectiveness of fundamental rights. Specific protection measures by law are thus required to make this kind of information architecture secure and rights-friendly. In addition regulation and law is required to maintain citizen and user trust to the infrastructure and to the information processing in it and to the activities of the authorities and service providers in the ecosystem.

The issue between trust and the new methods of care and collaboration regularly also appears in the practise. Recently some specific issues have been raised in the practise of the Chancellor of Justice concerning exchange of information and multi-professional meetings for the persons living under the threat of serious domestic violence. In the case question was the legality of non-regulated practises of information exchanges and drafting of a joint risk assessment and security plan for victims of domestic violence. Consent of the data subject may have its limits to provide for foundations for exchanges of sensitive personal data. Extensive non-regulated exchanges of information may also lead to lack of trust towards official action and unnecessary suspicion

63 Rehabilitiation Committee, p. 40-42.

64 Rehabilitiation Committee, p. 70-77.

65 *See* Voutilainen, Tomi, ICT-oikeus sähköisessä hallinnossa - ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely, Helsinki 2009, in particular p. 133 - 154.

concerning the nature of official action and service. [66] The case shows how the responsibility for the management of information and even power organise around informational positions and how these can become unclear and somehow disappear in the well-intentioned multi-stakeholder information flows and collaboration. The same happens in a wider scale in the platform and multiple service producer and multi-stakeholder environment.

2.5 The National Data Exchange Layer and the New Dimensions of Service Principle in Administrative Law

The National Data Exchange Layer in Finland (the interaction layer) in the social and health care architecture is provided by the MyHealth (OmaKanta) and the "suomi.fi" National Service Gateway. The data exchange layer in Finland's national service gateway architecture is technically based on the X-Road data transfer protocol utilising structured XML –schemas. X-Road was originally developed and is widely used in Estonia.[67]

The Kanta social and health services platform has its own interaction layers for professional users, for citizens MyHealth -service OmaKanta uses national service gateway data exchange layers, The idea in the National Service Gateway and in the Act underlying it is to create a common framework for public administration to provide a digital access to public services and to provide a secure view to the user on his administrative files and issues.[68] The proposed freedom of choice in the social and health care would also be realised through the National Service Gateway and thereto attached OmaKanta (MyHealth) services.[69]

The purpose is to overcome the problem of fragmented public authorities and form a genuine platform of the public sector. This would also overcome the challenge recognised in Sweden that relatively independent agencies do not sufficiently provide common digital solutions.[70]

Beyond the data exchange layer are functional data bases and solutions of different services and service providers (service layers). The data from the basic registers and in the case of social and health care and other occasions where the

66 The case described in the text concerns multi-professional collaboration in which social services and police together with other collaboration partners conduct common risk assessment for persons who are victims for serious domestic violence. *See* the decision of the Deputy Chancellor of Justice 8.3.2018, OKV/175/1/2017.

67 The X-road protocol is available at "github.com/vrk-kpa/X-Road/blob/develop/doc/Protocols/pr-mess_x-road_message_protocol.md" (Page visited 11.5.2018).

68 On the National Gateway Programme *see* the Finnish Ministry of Finance website "www.vm.fi/palveluarkkitehtuuri" and "esuomi.fi/palveluntarjoajat/palveluvayla" with subpages for a more technical description of the gateway and services attached to the interaction layer (Pages visited 11.5.2018).

69 *See* Government Proposal HE 16/2018 vp.

70 *See* on the Swedish situation *Utredningen om effektiv styrning av nationella digitala tjänster*, SOU 2017:23 and the committee directive Rättsliga förutsättningar för en digitalt samverkande förvaltning, dir. 2016:98.

law authorises that, the core data is available for authorised authorities and service providers. Core data system will provide archiving system.

Attached to the service layer are applications from third parties providing additional services in the platform. These applications and service providers would be able to produce data to the core and can use, with limitations from competition law perspective specified in the National Service Gateway Act, which limits the use in the private sector the public sector identification solutions. Users may authenticate data transfers to these additional service providers from the data core.

The proposed law on the Secure Secondary Use of Social and Health Data requires establishment of a secure user environment in which anonymised and pseudonymised data can be analysed and used also for research and development purposes.[71] The availability of external service providers beyond the public administration is vital for the attractiveness of the platform to users; ordinary citizens deal with public administration fairly rarely and therefore the usability calls upon to have additional private services attached to the system.

Functional application layer is also an important arena of creation of new data and value to the users. However this also creates application interfaces which must be sufficiently transparent with regards to the reliability of the service provider, use and processing of personal data and information and cyber-security. Provisions of the GDPR establish basis but in contracts and practical rules of the game the transparency, reliability and security of the applications and solutions shall be sufficiently secured.

Nordic administrative law recognises service principle as one of the fundamental general principles of administrative law.[72] Service principle refers also to the advice given to the service users and members of the public and includes a structural and an organisation culture dimension whereby the administration shall be oriented towards the users. The service principle is dynamic; it develops constantly in practise. It defines widely also work ethics and functioning mode of public administration and connects to the objectives of quality of administrative action, adherence to the principles of good administration and citizen-focus and participation in the functioning and decision-making of the public administration.[73]

The user-friendliness and the quality of the inter-faces and how informative they are can be considered to be parts of the service principle in the digital environment and here service principles concurs with the GDPR rules on the clear and intelligible information and clarity of the substance, extend and consequences of consent. Contemporary way to realise service principle is the informative and easy-to-use presence in the on-line world and, in particular digital platforms trough which users can widely reach public administration and obtain information on which authority is dealing with a particular matter.

71 HE 159/2017 vp.

72 *See* Administrative Procedure Act (434/2003), section 7.

73 *See* also Mäenpää, Olli, *Hallinto-oikeus*, Talentum Focus Electronic book, Helsinki 2013 (regularly updated), chapter III.6.

Availability and accessibility of digital services and the easiness of their use are also dimensions of the service principle in the public administration.[74]

In the practise of the Parliamentary Ombudsman and Chancellor of Justice a more specific criteria of matters which shall be duly consider in the organisation of administrative services have been developed. According to this established practise administrative services including the digital administration shall be designed on the basis for needs for the realisation of equality, principles of good administration and the linguistic rights of the citizens.[75]

Currently the general legislation in Finland does not absolutely require public authorities to provide for electronic communication and digital services but this is dependent on the technical and organisational preparedness of each authority and its resources. The Chancellor of Justice has already 12 years ago considered, however, that the service principle and taking into consideration the customer needs favour the provision of digital communication channels and contact addresses and that technologic development and development of authentication, digital signatures, technical data protection measures and information security arrangement create needs to reconsider even legislation concerning digital contact and digital initiation of matters.[76]

The digitalisation of administrative procedures with customer-centric focus is a modern way to realise the general service principle in public administration and design and realisation of digital services is law-informed legal planning exercise where realisation of rights and good administration is written into the structures and technical and organisational functioning mode of the administration.

A specific dimension of the service principle is also the universal public information and data services provided by public administration. This means sharing resources on open data and advising on the availability of open data which are founded partly on the European Union Directive on the Re-use of Public Sector Information 2003/98/EC, amended by Directive 2013/37/EU (the PSI Directive). Finland's Openness in the Government Act requires also production of information on request in a general level.

The social and health care reform and the regional administration reform aim to broaden the structural dimension of the service principle and customer-focus as leading functional mode of public administration. On the same time the idea is to create a fairly uniform digital platform from the public administration and divide this platform to 3 levels with distinctive general role and duties: 1) local government with general local tasks and as a democratically legitimate and generally competent entity and public law community; 2) counties who are charged with regional development and administration services, organisation of social and health care and welfare services and enterprise promotion and

74 *See* Government Proposal for an Act on Offering of Digital Services, HE 60/2018 vp., p. 7-8.

75 *See* for example Deputy Parliamentary Ombudsman decisions AOAS 1624/4/12 22.2.2013, AOA 2954/4/12 28.5.2013, AOA 4653/4/14 31.12.2015 and Parliamentary Ombudsman Decision EOA 4770/4/15 8.6.2016.

76 Chancellor of Justice decision 170/1/05 13.2.2006.

employment services 3) central government responsible for the supervision and assurance of the fundamental rights and freedoms and public security provision. Central government entities in this organisation would have always nation-wide territorial powers. Administration and the common digital platform it provides is seen as an enablener and facilitator, the principles of dialogue and inter-action being the desired virtues and functioning mode of the public administration.[77]

Service principle and customer-focus and customer and human-centric approach are also aspects of open government as structural principle and ethical virtue of public administration. Open government and service principle concur in their demands to organise access to government services and access information on those services in a way which truly facilitates customer's life. Openness in this respect extends much beyond the access to public documents to active engagement, participation, co-learning and sharing of timely and reliable data.[78] Digitalisation together with the service principle is not only digital processes; it is learning and developing in wide and fair societal participation new ways in which the public administration can inform citizens and stakeholder and works together with them in order to deliver in society.

Further guidance on the future development is given in the principles of digitalisation adopted by the Government. The principles of digitalisation are a policy-orientation document approved by the Government. It is, hence, not a source of law and certain caution shall be exercised in the use of such principles in legal discourses. Supreme Administrative Court has in its opinion on the new steering model of digitalisation projects pointed out to the division of powers and that judiciary is, therefore, not bound by management development principles of the executive branch of the government and certain caution also need to be exercised before such principles are written into the legislation.[79] The digitalisation principles nevertheless express the direction to which digital public administration is developed and objectives used as will of the legislator (voluntas of the legislator) when new laws realising such principles are adapted.

Among 9 principles guiding the future digital administration and digital government are elimination of all unnecessary transactions, collection of data and information only once and allowing multiple use of the government collected data and finally opening up interaction and data exchange layers and use of open application programme interfaces. Additional principles include construction of easy-to-use but secure services, quickly realisable benefits for citizens and other clients, guaranteeing ability to serve also in exceptional

77 *See* Government Proposal HE 15/2017 vp., and the Opinion of the Administrative Committee of the Parliament, HaVL 3/2018. General information and all the drafts and other preparatory documents on the regional government reform (county reform) and social and health reform is available from "alueuudistus.fi".

78 *See* OECD, Council Recommendation on Open government, C(2017)140 - C/M(2017)22, 14 December 2017, available at "www.oecd.org/gov/Recommendation-Open-Government-Approved-Council-141217.pdf".

79 Supreme Administrative Court Opinion 7.5.2018 Drno H 267/18, available at "www.kho.fi/material/attachments/kho/aineistoa/lausuntoja/RSSzqHZHT/H26718.pdf". (page visited 12. 5.2018).

situations and under emergencies and utilisation of the already existing services and solutions. [80]

3 Trust in a Socio-legal and Technological Perspective to Law

European legislator and the European Commission in its policy documents determine trust as one of the objectives of the European Union GDPR and legislative acts in the context of Digital Single Markets. Trust is in a complex relationship with the principles of rule of law and constitutional governance based on fundamental rights and freedoms. The rule of law contributes to trust but, rule of law also requires that trust is based on explicit and legitimate criteria. In the longer term trust requires verifiable conditions, not simple faith. Law is a promise and for long term trust the law should be a reasonably binding promise, not only text in books with little lively presence in action.

Trust is a socio-legal issue. Trust in the context of the regulation of digital information, digital administration and digital platforms has at least 4 different dimensions with various sub-dimensions: (1) trust as a empiric and theoretical social phenomena and subject to sociological research, (2) trust as a normative goal and concept in law and in ethics and morality and in political theory, (3) trust as an institutional-technical phenomena like trusted third parties and (4) trust as technological concept in technologies of trust and trustworthiness of infrastructure. All these dimensions contribute to the understanding of regulation and law.

Trust is often treated as a sociological issue and studied from the angle of sociology and law. Trust has a close connection with legitimacy and legal certainty. As a legislative policy objective trust may be vague and even misleading. For legitimacy and legal certainty trust cannot be only a sociological or technical issue and we need a legal, rule of law understanding of trust. But for the law to be realistic and have an empirically identifiable impact on behaviour, sociologic and psychologic analyses and understanding of trust are informative.

In the context of digital single markets trust mainly appears as trustworthiness of infrastructure and platform and trustworthiness of applications and solutions available in them. In the Union policy documents this seems, at least indirectly refer to the realisation of rights and legal principles in the digital environment. That is also the way in which several articles of the GDPR are written, for example Article 25 on the data protection by design and default where the whole concept is defined as planning for the realisation of rights and as legal risk management against risks related to the realisation of rights. The same applies for the rules on the data protection impact assessments in Art. 35, and for the rules in the general information security provision in Art. 32 of the GDPR. Trust

80 These principles of digitalisation of the government, adopted by the Government of Finland, are availble at the Ministry of Finance web-site at "vm.fi/digitalisoinnin-periaatteet" (page visited 12.5.2018). Further guidance is avaible at the suomidigi –public administration development forum maintained by the Finnish Population Centre Väestörekisterikeskus, which is under process of becoming a general digitalisation agency, *see* "suomidigi.fi/" (page visited 12.5.2018).

in this sense was also strongly present in the preparatory works related to GDPR.[81]

Trust appears to be a narrative of justification of the actions by the European legislator, much less a foundation for judgements used by the European Court of Justice. Trust in a normative sense of being trustworthy and respectful for the realisation of rights is also an ideal and objective established by the European legislation, in particularly the GDPR.

Trust, in order not to be only of simple rethorics, shall be supported by efficiency of rights, balancing of rights, effective rights of participation and self-determination, transparency and accountability. European Union law in general strives after the practical efficiency of rights.[82] Thereby efficient supervision and oversight and efficient access to justice are essential elements of legitimacy and legal certainty (legal security) in European law. Efficient supervision is seen specifically in the data protection law as well. Oversight by independent data protection authorities is defined in Art. 8 (3) of the European Union Charter on fundamental rights as an essential element of the Union right to protection of personal data. In GDPR oversight by independent data protection authorities is an important element of the implementation of the more unified European concept of data protection.

Digital working environment requires new elements and new ways of realisation of transparency, accountability and supervision of public administration and digital platforms. The General Data Protection Regulation strengthens the role of the data protection authorities but, also, in practise there is also a need for an up-to-date role for the Supreme Legality Guardians (in Finland the Parliamentary Ombudsman and the Chancellor of Justice) to safeguard the rule of law under rapid legal and technical developments. And the law shall provide up to date foundations for accountability, transparency and efficiency of rights in the new context which call upon to revise some general acts on public administration and clarify the rules of the game for public platforms.

The digital revolution and the complex environment of the digital platforms with thousands of applications, vast amounts of data and AI inside the systems will increasingly also move the issues of trust and trustworthiness to the technical domain. Technical arrangements become increasingly decisive for the practical effectiveness of rights. Human mind is also often quite limited and hence assistance by AI powered computer is very much needed for the reliability assessments and transparency on trustworthiness in the digital environment. The old idea of the Nordic legal informatics on legal certainty in automated judicial and administrative decision-making and AI powered decision-support and decision-making and of the Openness in the Government Act of Finland concerning writing legal rights also to the architecture, processes and functioning of the systems is newly topical on a vast scale. This is exactly also the challenge in the online dispute resolution mechanisms such as the ICANN

81 See, for example Commission proposal, COM (2012) 11 final.

82 See, generally Walkila, Sonya, *Horizontal effect of fundamental rights in EU law*, Groningen 2016.

resolution system, which generally speaking, look pretty promising in terms of their costs and benefits, accessibility and expediency in speed.[83]

Trust is to certain extend measurable. It also has societal and even economic value. Trust is discussed in sociology and also in institutional economics. Economic history and informal and formal institutions, which create trust, explain considerably economic success of countries. Functioning of the rule of law and also trust to rule of law seems to play a very significant role.[84]

Digitalisation with platforms and ecosystems create new arenas where governance by law or by scarcity of law will be established. This means that the historical process of building up reliable governance by law and thereby also a system which is best to promote generalised trust and reduce transaction costs in economics and, increase trade, or some system with less trust and more costs will emerge in a speedy way.

Economic analyses tell us that both formal institutions like law and informal institutions such as social norms facilitate economic exchanges. Trade and commerce seems to increase when rights, particularly property rights are respected and rules of the game can be anticipated and they are intelligible. [85] These findings also support the narrative in the European Union Digital Single Market Strategy and in the preparatory works for the GDPR.[86]

In the sociological perspective trust refers, firstly, to generalised trust where persons unknown to each other. Secondly, it refers to particular trust between persons knowing each other like members of a family, friends or groups of kins. Trust may also be strategic. Then parties have a specific, shared interest to a deal or arrangement between each other. Trust can also be extended to institutions; question is about confidence towards institutions in general and towards a particular institution – abstract system like normative institutions can here be equalled with organizations. The distinction between the confidence towards abstract systems and organisations and trust between human beings is in many sociologic theories following foundational work done by Max Weber vital for deeper understanding of the structures of society and their relations to behaviour and functioning of individuals. [87] In instrumental trust people trust others and

---

83 On this challenge in the online dispute resolution mechanisms *see* Koulu, Riikka, *Dispute resolution and technology: revisiting the justification of conflict management*, Helsinki 2016, p. 31.

84 A powerful argument on that is Acemoglu, Daron, & Robinson, James A., Why nations fail : the origins of power, prosperity and poverty, London 2013. A systematic mapping of the value of rule of law and attempt to measure rule of law is World Bank's World Development Report, *Governance and the Law*, World Bank 2017, available at "www.worldbank.org/en/publication/wdr2017" (page visited 12.5.2018).

85 Yu Shu, Beugelsdijk Sjoerd, de Haan Jakob, *Trade, Trust and Rule of Law*. European Journal of Political Economy, Vol 37 (2015), p. 102 -115.

86 Concerning GDPR *see* COM (2012) 11 final.

87 *See* Kouvo, Antti, *Luottamuksen lähteet, vertaileva tutkimus yleistettyä luottamusta synnyttävistä mekanismeista*, Annales Universitatis Turkuensis C 381, Turku 2014, p. 16-21. For a more technical discussion on the measurement of trust, *see* OECD (2017), *OECD Guidelines on Measuring Trust*, OECD Publishing, Paris, "dx.doi.org/10.1787/9789264278219-en".

make also themselves vulnerable when they anticipate or assess from the past known behaviour of the others that they will behave as anticipated. [88]

Confidence comes very close to legitimacy. Legitimacy has been shown to predict observance with the rules.[89] Rule of law produces generalised trust and that also facilitates commerce and builds favourable conditions for investment and growth.

Legitimacy is a familiar concept in constitutional and political theory. In the European Social Survey the generalised trust is measured. It is seen as a condition for legitimacy of the coercive nature of the legal order and criminal justice in particular.[90] European Social Survey measures thus confidence in hard law. It has been argued that the whole language of law is violence and that legal system is organised coercive power.[91]

This legitimacy and criminological orientation is increasingly interesting administrative law in the context of digital platforms. The GDPR relies heavily on rather hard administrative sanctions and nature of data protection law has moved towards administrative law of a very classic state. The GDPR uses the approach of the effective, dissuasive and proportionate sanctions and the assumed deterrence following a doctrine originally developed by the European Court of Justice on other contexts.[92]

Trust following the measurement in European Social Survey is belief that authorities can be relied upon to act competently and in ways that are procedurally fair and provides equal justice and protection across society. Trust as confidence to authority is hence, a measure of belief in procedural fairness and respect of equality and relative competence of official action. Legitimacy is seen as a constitutional property of a legal institution; it is the right to govern and recognition of that by those who are governed. Ultimately legitimacy is either normative situation following from justificatory principles or subjective state of mind of the governed and extrapolation of those conceptions at the level of society.[93]

---

88 Tyler Tom R., *Why people cooperate : the role of social motivations*, Princeton 2011, chapter two.

89 Tyler 2011, chapter two.

90 Jackson, Jonathan, Hough, Mike, Bradford, Ben, Pooler Tia, Hohl, Katrin and Kuha, Jouni, *Trust in Justice: Topline Results from Round 5 of the European Social Survey*, ESS Topline Results Series, Issue 1, 2011, available at www.europeansocialsurvey.org/docs/findings/ESS5_toplines_issue_1_trust_in_justice.pdf. (page visited 12.5.2018).

91 Koulu 2016, op.cit. on the online dispute resolution.

92 This approach is coherent in theory but may be subjected also to serious criticisms from psychologic point of view, *see* Tyler, Tom R. and Mentovich, Avital, *Punishing Collective Entities*, Journal of Law and Policy, Vol. 19, 2010-2011, p. 203 -230.

93 On the legitimacy and compliance with the law *see* Tom R. Tyler, Tom R., & Jackson, Jonathan, *Popular Legitimacy and the Exercise of Legal Authority: Motivating Compliance, Cooperation, and Engagement*, Psychology, Public, Policy, and Law, Vol.20, 2014, p. 78-443. Here important observations on the difference between justifiability of power and consent and adherence to power are made.

Psychologic and social models of trust and, why an institution of coercive nature is trusted, are in this context, interesting for a deeper understanding of trust components. Tom R. Tyler's psychologic model of procedural fairness and trust, which is founded on empiric observations, is here quite interesting. According to Tyler's empiric findings trust follows from various factors among which the perceived procedural fairness and treatment of persons is quite decisive. [94] In the organisational contexts also shared values, attitudes, objectives and shared identities are decisive for cooperation. Social motivations and hence, engagement and participation of the people and their communities have a major impact on the observance of law and generally on cooperation and trust. This is also supported by empiric findings in various contexts. [95]

Social motivation and psychologic models of trust come pretty close to corpus of knowledge in administrative law domain on fair procedures, participation and engagement and good administration. In the digital realm and processing of personal data the consent and transparency as they are developed in the GDPR and interpreted in the guidance given by the Article 29 Working Party seeks to do also exactly that.[96]

A challenge of trust in digital platforms is that law's realm extends beyond human interaction and covers also the current and increased future interactions between intelligent machine and humans. Fundamental principles of justice and law do still prevail but the implementation environment is complex. User laziness, and the mere desire to get access to services and resources in an environment where consent for processing of personal data and user's own data and content has become a currency against which services is rendered. That is namely exactly what many social media platforms do as their fundamental business model. The default mode may rather be an excessive processing of data from the European Union's data protection law perspective. Particularly the relevance of the data minimisation principle can be questioned, and also whether that principle is still valid in the current context of big data.

The effective transparency and testing of the trustworthiness of AI powered solutions in the network and whether the teaching data for the algorithms has been sufficiently diverse to avoid weaknesses and biases are hard and even impossible to realise in manual human observations. We, thus, need a reliable intelligent machine to test also transparency of our processes in the digital environment. The digital platforms are multi-actor environments and the challenge of accountability and transparency is even bigger. The GDPR may in

94 Tyler, Tom R., *Procedural Justice, Legitimacy, and the Effective Rule of Law*, Crime & Justice, Vol.30, 2003, p. 283-359.

95 Tyler 2011.

96 *See* Art. 7 of the GDPR on the conditions for consent and Article 12 on transparent information and modalities for exercise of data subject rights. Article 29 Working Party, Guidelines on Consent under Regulation 2016/679 (wp259rev.01), 16.4.2018, available at "ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051" (page visited 13.5.2018) and Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), available at "ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227".

this regard to be in the right direction but is not sufficient at all to create conditions for socially motivated and reasoned trust.

The Nordic legal informatics concept of rights-friendly infrastructure or good information management practise as it is called in the Finnish Openness in the Government Act or good publicity infrastructure as it is called in the Swedish law and legal literature following rules in the 4th chapter of the Act on Openness and Secrecy (SFS 2009:400) is an open and dynamic general obligation to ensure good governance and also to involve technical means to the service of realisation of rights and transparency. This has also been dynamically interpreted by the Supreme Guardians of Law, the Parliamentary Ombudsman and the Chancellor of Justice. In this practise the good information management practise has been connected with the ideas of rights to participation and service principle in administrative law.[97] Also, an active monitoring of the life cycle of matters and following up matters trough case management systems is part of the official duties under the principles of good administration.[98] Law and control for the legality and good administration extends to the control of the good project management in law and by law.[99]

The Supreme Guardians of Law and other legality overseers also need new partnerships and the administration itself needs to develop or obtain trusted technologies for testing of trustworthiness of algorithms and AI solutions to be used in public administration and also in the digital ecosystem developed on the basis of public platforms. The legal foundations in general level and in the form of legal principles are there, the challenge is more to put the spirit of law into action in new circumstances.

Specific acts however, need to be clarified and more detailed guidance on how to apply the service principle, hearing and participation and equality and good information management and rights-by-design infrastructure in the constantly changing digital environment. This is also vital for the conditions of trust as fairness of the outcomes and also as procedural fairness and engagement with shared values and objectives. The procedures with the Supreme Guardians

97 See, for example, Deputy Chancellor of Justice decision OKV/208/1/2011, 26.11.2013 on complaint which concerned the change of name of a municipal road and the legal implications of that decision.

98 *See* Deputy Chancellor of Justice decision OKV/344/1/2011, 06.09.2013.

99 The Deputy Chancellor of Justice decision OKV/344/1/2011 touched the issue of the legal requirements on project management in projects financed by public authorities. The Deputy Parliamentary Ombudsman assessed widely the ICT development project management in his own initiative report on the implementation of new police case and resources management system VITJA, *see* the Deputy Parliamentary Ombudsman decision Dnro 4765/2/13, 13.3.2015. That decisions lines some general good principles on the running of ICT development projects with particular legal relevance. The project management is decisive for the outcomes of the digitalisation and also a shared problem in many countries. The Dutch Parliament parliamentary inquiry on the ICT project management is very illustrative and contains also good general advice on how to succeed in public ICT projects, *see* Tweede Kamer der Staten-Generaal, Parlementair onderzoek naar ICT-projecten bij de overhead, Vergadejaar 2014-2015, Doc 33 326, Nr 5 (in Dutch only), available at "www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf" (page visited 13.4.2018).

of Law can be considered as a specific consultation and engagement procedure which is available to everybody and also thereby a mechanism of trust.

4 The Legal Governance Principles of the Digital Administration and Digital Platforms

Fairness of the procedure extends also to the design of data and information processing in digital platforms. Platform is also a community and network of services and actors. To keep it functioning requires clear rules of the game and participation which means that they cannot be built on fully individual and different, fully personalised contents and certainly not only on contracting and decision of individual authorities.

The risk in platforms is that the platform organisation stipulates one-sidedly the rules to be followed in the platform. That is very often the case with big commercial social media platforms. The GDPR limits the role of consent as legal foundations for processing of personal data for purposes of the data controller's legal obligations and public interest the consent is further limited in the public sector digital platforms. The article 6 subparagraph c and e require more detailed regulation by Union or Member State law. To build conditions for trust these acts cannot simply be technical formalities nor result from negotiated rule making with interest groups but from genuine and fair and open participatory processes. Here the oversight by Supreme Guardians of Law concerning the legislative procedures and their openness is an important safeguard for trust. In Finland there is an inherent tendency to regard the previous constitutional requirements on the legislation concerning processing of personal data mainly as technicalities in a way that when the technical form of sufficiently precise law was reached then there was satisfaction but no authentic flavour for realisation of rights. But in constitutional governance based on the idea of the material effectiveness of fundamental rights and freedoms also the legislative process and the substantive spirit of law should serve democratic participation and balance of rights.

The consultation process and impact assessments on these public sector acts are then vital for the conditions of fairness. The following of the guidelines for consultation in legislative drafting and impact assessment are important. The GDPR and the Article 29 Working Group draft guidelines on the data protection impact assessment pursuant to Art. 35 of the GDPR see that the data protection impact assessment can partly be made as part of the legislative procedure leading to specific acts referred to in GDPR. Data protection impact assessments are, in general, a way in which also stakeholders and platform users can and even should be consulted on the rules of the platform and activities which happen in the platform and service network build on it. [100]

100 This is also stated in the Article 29 Working Party draft data protection impact assessment guidelines where consultation is defined as part of the procedure in the preparation of impact assessments.

For the maximum creation of favourable conditions of trust the consultation process, impact assessment and the way which different actors in the digital platform perform should facilitate a well-founded positive perception of trustworthiness of the platform and the actors associated with it.[101] General data protection culture, which refers to the general patterns and activities and the way in which rights are taken into consideration in the planning and design of the data processing, architecture, standards and contracts and the information systems, impacts on the trustworthiness and fairness of the activities in digital platforms.

The independent data protection authorities play from the data protection perspective a key role in the oversight of the fairness of design and functioning of digital platforms. However, also the Supreme Legality Overseers have both general and specific role in the promotion and assurance of trustworthiness. Specific role is the legality oversight of the data protection authorities[102] and the oversight of the constitutionality of legislative proposals and legislative procedure. Given the enhanced role of the Member State law and its specific acts on the realisation and balancing of rights in the public sector digital platforms the oversight of legislation and legislative procedures contribute significantly to the trustworthiness and rights of participation.

The Supreme Legality Overseers with general competence have also a role far beyond these specific tasks and instances. General legality oversight enhances generally the realisation of fundamental rights in digital platforms and proper balancing of rights. It is not only an ex post judgement on the legality of an individual act but systematic and systemic promotion of the realisation of fundamental rights and freedoms; it takes places at the dimension of concrete cases and individuals by seeking settlement and resolution of instances of deficient realisation of rights and the on the systemic level by analysing and influencing structural weaknesses having a negative impact on the realisation of rights.

The digital environment is partly a new arena for law and finding balanced solutions for problems general principles of law should be applied and also developed further. Traditionally the supreme legality overseers have made a major contribution to the development and application of the general principles of administrative law in Finland.[103] Supreme legality overseers have also led the

101 On the building of trust *see* Alarcon, G.M., Lyons, J.B., Christensen, J.C. et al.: *The Effect of Propensity to Trust and Perceptions of Trustworthiness on Trust Behaviours in Dyads*, Behavior Research Methods 2007, "doi.org/10.3758/s13428-017-0959-6".

102 *See* Finnish Parliament Constitutional Law Committee Opinion on the proposed Data Protection Act of Finland for a comprehensive analyses of the Parliamentary Ombudsman and Chancellor of Justice as supervisors of data protection authorities and as enforcers of data protection related rights, PeVL 14/2018 vp.

103 For a longer term perspective *see* Konstari, Timo, *Harkintavallan väärinkäytöstä: tutkimus tarkoitussidonnaisuudesta hallintoviranomaisten harkintavallan rajoitusperiaatteena*, Helsinki 1979 on the origins and adoption of the abuse of power / detournément du pouvoir –doctrine in Finland, in which both courts and Supreme Legality Overseers played a significant role. For a critical account from a legalistic perspective in which the Supreme

way how fundamental constitutional principles and general principles of administrative law have been applied in the context of new situations following the use of information and communication technologies.

For example the interpretation of service principle in administrative law in the context of digitalisation has benefited from decisions of the Chancellor of Justice. Parliamentary Ombudsman has assessed also the general project management in ICT projects and the impact of that to the fluidity of procedures and citizens' rights as well as of the impact of the information management practises on individual rights. This aspect will in the future be even more important than today given the law's task and nature as planning and design for legal certainty.

Task of the Supreme Legality Overseers and the courts is the balancing of various rights – the law of the digital platforms and administration is not only about data protection. Parliamentary Ombudsman and Chancellor of Justice have both right of initiative in the case of contradictions or, when there are lacunaes in legislation. This may also be an important tool to ensure good legislative and regulatory environment.

On-line platforms are an essential part of the digital society and administration. Trustworthiness of the platforms and trust in more general terms requires appropriate, transparent and clear legal rules in the platforms. In the European Commission proposals concerning online business environments and in the Member State legislative practise and in contractual arrangements certain principles concerning construction of the digital platforms and ecosystems on them are emerging. In the Finnish national legislation approach in legal acts appears sporadic, fragmented and technical whereas clearer guidance is found in management documents concerning the principles of ecosystems and platforms. Guidance for development is also provided by the principles of ICT law recognised in legal literature.[104] European Union is in the process to set up some principles in the Union law for online business platforms and review the consumer law concerning the relationship between consumers, platforms and individual application and service providers.[105] With these legislative and policy initiatives the European Union is seeking both predictable and trusted legal environment and promote trust via transparency and trustworthiness of the online platforms and inter-mediation services.

Digital platforms represent a new kind of partnership between public and private sectors. Since the European Union has only limited powers in the area of public administration and following entrusting considerable tasks of legislation

---

Legality Overseers are criticized to have entered into the domain of legislative powers, Tähti, Aarre, *Periaatteet Suomen hallinto-oikeudessa*, Helsinki 1995.

104 *See*, for example Voutilainen 2009, op.cit. where second-order (meta) principles of quality and user-centredness and the principles of availability, accessibility, information security, inter-operability, auditability and transparency are discussed, *see* Voutilainen 2009, op.cit., p. 180 - 239.

105 *See* COM (2018) 218 final and on the consumers European Commission's so called New Deal for Consumers package and the proposed amendments of the Union consumer directives as a result of that, COM (2018) 185 final.

in the realisation of the protection of personal data to the Member States the law of the digital platforms in the European Union is a flux of European Union and Member States law and also a flux of pieces of general information law, private law and public law.

The GDPR only creates a new kind of relationship and additional dialogue between Union law and Member States legal system. Construction of predictable, intelligible and coherent law in concrete surroundings and situations requires dialogue between legal systems and also across different kinds of governance systems.

The construction of digital platforms for public administration and establishment of the ecosystem (network) of the various actors related it requires as coordinated as possible concerning of various technical, administrative, service-design and service approach, economic and legal perspectives supported by good ethical thinking and action and good management. Also legislative work, application of law and development of contracts and the whole ecosystem architecture from the legal point of view calls upon a set of principles to see the essential aspects and construct a coherent and intelligible system in an environment with complex features. That is why public administration's digital platforms and ecosystem should be guided by clear legal principles.

Out of the recent legislative proposals in the European Union and new legislation in Finland and the preparatory materials for the Finnish legislative pieces together with the general principles of administrative and information law, including the fairly rich but difficult to grasp regulation in the European Union General Data Protection Regulation some core principles can be constructed. These principles also have the potential to stand for procedural fairness and at least support trustworthiness of the environment and infrastructure and also support fair outcomes and balancing of the positions of various parties. These principles have a certain potential to contribute to various elements of trust among individuals. In addition, on the bases of legal principles certain normative ideals of trust and justice based on juridical legal discource can be developed.

A general observation is that often the legal and juridical discourses produce the clearest discourses on good administration and good governance. The legal discourses often have also the clearest and most equal participation rules compared to various ethical or management and development discourses. This is not to say about the superiority of but to remind of certain core value what the law can bring into the good information management and trust in the digital administration.[106]

First of these emerging principles of the law of digital platforms is the rights by design and default and the active duty of care in the design, management and governance of the platform of individual rights and also of collective rights. The underlying provision is Art. 25 of the GDPR concerning the privacy by design and default. The goal of the provision is that an effective data protection which is written into the architecture, and design of the information and communication

106 On the discourses of good governance and good administration, *see* Koivisto, Ida, *Hyvän hallinnon muunnelmat, julkisoikeudellinen tutkimus*, Helsinki 2011.

processes and data structures and into the systems themselves. That article is the flagship of the law as planning approach. That to be truly effective requires also social motivation and acceptance by the software industries, service providers and users and all of them together. One can wonder whether the current forums of engagement and participation are sufficient to that extend. The challenge is big for the data protection authorities. The public administration as a financially significant purchaser and standard setter has a specific societal responsibility in the realisation of this.

The data protection by design and default aims to incorporate risk management to architecture and systems design and beyond that, have a legally and rights informed foundation for that risk management. Idea is to assess and consider risks related to the data protection principles and more generally to the fundamental rights and freedoms of individuals in the light of the likelihood and consequences of those risks and on the basis of that then carefully plan technically feasible and reasonable measures to counter and mitigate risks.[107] The principle of proportionality guides the implementation of risk related measures. Data protection is not an absolute right. This is reminded in the para. 4 of the preamble of the GDPR, and, by the Constitutional Law Committee in Finland in a wider fundamental rights perspective.[108] Therefore, in the context of digital platforms and administration it is better to speak in broader terms about rights by design and default. This is part of good administration, which is a fundamental right according to section 21 of the Constitution of Finland and Art. 41 of the European Union Charter on Fundamental Rights.

A specific way to realise engagement and participation in digital administration and platforms is MyData. It refers to solutions in which individuals are given tools to control and manage their personal data in accordance with data protection principles.[109] MyData can also give the technical and organisational means to help to realise the right to data portability,

107 *See* Article 29 Working Party Guidance on Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, 17.10.2017 available at "ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236". These guidelines open the risk management thinking behind GDPR beyond the mere instrument of data protection impact assessment and therefore they are also useful for consideration of data protection by design and default.

108 *See* PeVL 14/2018 vp.

109 On MyData *see* Kallasvuo, Karoliina, *Omadata ja oikeus siirtää tiedot tietojärjestelmästä toiseen*, Edilex, Helsinki 2017, and Knuutila Aleksi, Kokkonen, Vesa, Sundquist, Heikki, Kuittinen, Ossi & Thure, Salla, *MyData muutosvoimana: Julkishallinnon henkilötiedon ihmiskeskeisen hyödyntämisen mallit ja vaikutukset*, Valtioneuvosto – Helsinki 2017, which is a research report commissioned by the Finnish Government on the MyData and change force it may bring with it.The Ministry of Transport and Communication commissioned and published a white paper on the potential of MyData and on possible ways to implement it, *see MyData – A Nordic Model for human-centered personal data management and processing*, Ministry of Transport and Communication, Helsinki 2015, available at "urn.fi/URN:ISBN:978-952-243-455-5". The MyData approach will be written in to the new Act on the Electronic Processing of Patient and Client Data in Social and Health Care and it is partially in the OmaKanta (MyHealth) – service.

which is a new data protection rights in Art. 20 of the GDPR. Similar solutions are in the other sectorial legislation in the process of becoming a general principle of Union law.

The right to data portability is entirely about user empowerment. [110] So should also be the MyData tools to realise that and better control of personal data. MyData in other respects relates to a personalised version of the service principle in administrative law of digital administration. In the light of the normative models of trust related to the concept of right informational self-determination, which is one of the essences of the European union data protection law, and the empiric findings on the social models of trust, MyData has significant potential. Finnish Government has plans to use MyData on several public administration digitalisation projects.[111]

Empowerment and Mydata as public sector solutions came also to an eventual new role of the Government. The Government may also provide digital platforms with serious consideration for data protection: the government protects your data. Given the risk of misuse for governmental powers of the collected data this idea may sound strange. But this is in line with the ideas of Nordic welfare state where public sector is significant carrier of risks related to human life. This is also present in the Finland's concept of social and health care platform in which the core data will always be kept under the control of public authorities in order to prevent a capture of it by private market power.

Competition law and constitutional and administrative law may be in an uneasy relationship with each other when market based solutions are used in the production of public services.[112] The same concerns the use of government collected and held data for development and innovation purposes.[113] But on the rights of participation the objectives of competition law and concurrence neutrality and public law perspective to equality concur. The rights of participation and access to the ecosystem shall be on equal foundation in the role as a citizen/service user or service provider attached to the platform and ecosystem. This means in particular that the rules to provide services and conditions of it shall be open and equal. In addition, the pricing of the data and use of the government held infrastructures shall take place on equal grounds.

The fairness of the rules of participation requires also that the roles of the various participants are clear. Openness of the participation following transparent rules and their consistent application is also significant for the competition neutrality and overall fairness of the platform and ecosystem built on it. Trust towards the platform and ecosystem are pretty dependent on the rigorous application of these principles and on the visibility of these principles

110 On the right to data portability in GDPR *see* the Article 29 Working Party Guidelines on the right to "data portability" (wp242rev.01), 27.10.2017, available at "ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233".

111 Knuutila et. al. 2017.

112 *See* Finnish Parliament Constitutional Law Committee on the reform of social and health services PeVL 26/2017 vp.

113 *See* the Constitutional Law Committee on the draft Act on the Secondary Use of Social and Health Services Data, PeVL 1/2018 vp.

in the rules of the game of the platform and ecosystem around it. This also creates trust and confidence both by citizen-users but also of business participants to the platform.

Open data is a core feature for digital platforms and digital service ecosystems. Open data means machine readable access to data and, as an underlying assumption, structuring data and metadata in a way which supports automated realisation of protection of personal data and other rights to data and information, safeguarding of secrecy when justified by the freedom of information legislation. In addition data and metadata structures shall pursuant to section 18 of the Openness in the Government Act support realisation of access to data and information and realise good information management practise required by Openness in the Government Act.

The GDPR adds some new elements and detailed requirements on the wider concept of good information management practise, in particular concerning the organisational and technical measures to protect data and to balance freedom of information with data protection related rights. In the European Union law a significant foundation for the open data is the Directive on the Reuse of Public Sector Information 2003/98/EC which requires and sets general principles of pricing concerning access to data. The European Commission has presented a proposal for revised and recasted PSI Directive.[114] The revised directive would require the use of open application programming interfaces (APIs) in giving machine readable and real time access to data. The APIs are often in practise decisive how a digital ecosystem attached to a platform can function. Additionally a general principle of interoperability and implementation of the interoperability as the overarching and leading principle will define the conditions for access and usability of data and the digital participation.[115]

Trust in the digital environment finally is dependent on the reasonable and transparent level of information and cyber-security. The GDPR strengthens the role of information and cyber security in provisions in the Art. 32 of the GDPR and by introducing the system of data breach notifications. Also the whole concept of accountability in the GDPR is to show that sufficient protection and sufficient, up-to-date and state-of-the arts related to risks security measures are put in place. The notification regime includes notifications to data protection authorities and to users.

A difficult balancing is needed in the user notifications but the whole system has the potential to establish a good security related dialogue.[116] If so also in

114 *See* COM (2018) 324 final.

115 The European Union Interoperability Framework is a European definition and working tool for the realisation of interoperability. It has proven to be useful in the coordination and governance of interoperability work in digital administration but the decisive work and application is done at Member States administrations. *See* European Commission Communication COM (2017) 134 on the European Interoperability Framework, and the Commission web-site for interoperability "ec.europa.eu/isa2/eif_en" (page visited 13.5.2018).

116 *See* Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, wp250rev.01, 13.2.2018 available at "/ec.europa.eu/newsroom/

practise it has the potential to contribute to the trust. If not, it may become a difficult to apply legal formality with little empiric effects on trust and security of processing. The information and cyber security is part of the wider good information management obligations as defined in section 18 of the Finnish Openness in the Government Act and part of the duties of care of public authorities and civil servants as interpreted in the regular practise of Parliamentary Ombudsman and Chancellor of Justice. To arrive at good results the information and cyber security regulation and governance shall not limit itself only to addressing the incidents and surface level phenomena. Fundamental issue is how to write security into the software products and the systems architecture itself and here Europe is only at the beginning of a painful and long journey.[117]

5 Conclusions

Digital platforms and service networks build on platforms is one of the new ways of organisation. It is a new functioning mode of public administration in the digital environment. They are a distinctive on-line environment where the law functions and is expected to deliver its societal role. Digital platforms and the dynamic network of services and partnerships with different public and private sector organisations, the digital ecosystem, are a major organisational form to organise societal action and collaboration and to deliver on the tasks of public administration and governance.

Digital platforms in the public administration are a way in which the service principle of administrative law can effectively be realised in the online environment.

Digital platforms and networks built on the existing principles of law and legislation but effectiveness of fundamental rights and freedoms in this on-line environment calls upon further definition of the content of these principles. The governance of these platforms and related on-line services need also clear systematic principles around which regulation and also application of law can be constructed. These principles combine principles of information law with principles of administrative law and perspectives from the competition law. The European Union GDPR is at the centre of the law concerning digital platforms but data protection is not an absolute right and it has to be interpreted and weighted with other fundamental rights and freedoms. In a nutshell protection of personal data is always a part of and shall be a balanced part of a wider system of fundamental rights and freedoms. This is also among the core messages of the

---

article29/item-detail.cfm?item_id=612052", in which the potential of the security dialogue is emphasised.

117 The findings in the doctoral thesis by Jari Råman seem still today be up to date albeit in the liability regimes and regulation much progress has been made since then, *see* Råman, Jari, *Regulating secure software development : analysing the potential regulatory solutions for the lack of security in software*, Rovaniemi 2006. A lesson is that without involvement of the software creators and without significant skills in the software area information and cyber security will be limited.

recent Finnish Parliament's Constitutional Law Committee Opinion on the draft Data Protection Act complementing the EU GDPR in Finland.[118]

Trust is among classic normative ideals and objectives of administrative law. Trust is also increasingly an objective in the European Union legislation and policy documents on digital single markets and digital administration. It is also in the stated objectives of the GDPR albeit the European Court of Justice has not used it explicitly in its judgements. However, the way in which the Union data protection law has been interpreted by the Court has sought to safeguard elements of trust. Trust, hence, is a general legal policy goal and closely related to the normative goal and concept of legitimacy. It should also guide the application of law and development of law in the interplay between information law, administrative law and competition law which is typical in the case of digital platforms. Trust is also a social condition for the platforms to deliver and be successful.

The concept of trust is not, however, very well spelled out in the legal sources and it is only sporadically developed in legal and juridical discource beyond legal sociology or classic administrative law. Trust often appears mainly as a magic word to justify new regulation, not as a well structured and reasoned argument to substantially informing development and application of law. Trust mainly appears in the field of digitalisation and law as trustworthiness with two distinctive meanings: technical trustworthiness of the infrastructure and the correspondence of the on-line environment with some normative principles of trustworthiness. In the European Union which is based on the ideal of rule of law, these normative criteria are found in Union legislation and standards endorsed by the Union legislation. Albeit these are important dimensions of trust is this concept still relatively narrow and not sufficiently open for scientific appraisal and development.

Trust is a wide psychologic, cognitive, social and societal phenomena study of which is enriched by psychology, cognitive sciences and sociology. Legal and legal policy discourse of trust should take these wider perspectives seriously and then trust questions come close to the analyses of the conditions of legitimacy. Law of the digital platforms benefits from the sociological studies on the foundations of obedience to law and trust in the use of public power. In these empiric models procedural fairness and how human individuals are encountered are among fundamental pillars of trust. Considerations for procedural fairness are at the centre of administrative law and these considerations are widely valid in the new online environment as well. These perspectives are also useful in the application of the GDPR with regards to how the requirement of consent and how the provision of legal foundations for processing of personal data by specific Union or Member State acts are provided.

Trust depends also on the fairness of the outcomes and on the public and each individual perception of the adherence to the principles considered to be fair. Trust to law requires law to be relevant in terms of effectiveness and efficiency of its provisions and that the content of the law, as it is applied, corresponds to public values and beliefs of right, wrong and fair. The realisation of justice and

118 *See* PeVL 14/2018 vp.

fairness in the modern rule of law based on democracy rests on the effective and efficient application of fundamental rights and freedoms and internationally accepted human rights. To ensure such relevance and effectiveness the development of law and application of law needs contextual realism.

Contextual realism is today's version of what Alf Ross described as the content of the science of legal policy: the knowledge and art of the realisation of idea of justice in law. Contextual realism departs from the requirement of the empiric relevance of law and its rules and principles in each distinctive working environment. Contextual realism means that legal principles and rules are applied in a concrete context and with a deep multi-disciplinary understanding of the societal, economic, technical and governance features of each particular context. Coherence and understanding intelligibility of law is constructed with argumentation combining legal, societal and technical aspects in each such situation.

Contextual realism also means that fundamental rights are balanced with each other in each concrete environment and situation. Individual fundamental rights are always applied as part of a dynamic system of the fundamental rights and freedoms. This is also the message from the preamble of the GDPR and from the Finnish Parliament Constitutional Law Committee on the proposed Finnish Data Protection Act complementing the GDPR in Finnish law.[119] Dynamic systematics and general doctrines of law also concur with literature in Nordic legal informatics about the specific method of legal informatics compared to conventional doctrinal study of law.

Contextual realism calls upon a multi-disciplinary study and understanding of law and therefore the discourses of law-making and application of law as well as the scientific study of law and digitalisation are necessarily open to the perspectives of other disciplines. Legal informatics and the information law emerging from the legal informatics tradition and ICT law have for a long time represented such a study and now this approach in the context of digital platforms merges with administrative law and competition law and administrative and management sciences with governance and risk management perspectives. The model of law as planning and active duty of care advising in the design of ecosystem architecture, participation rules and standards, data structures and processes and finally the interfaces and applications also requires that.

Psychologic models of legitimacy and trust, for example that of Tom R. Tyler's criminologically oriented model of the obedience and trust on law, provide additional useful perspectives to the development of the law of digital platforms of public administration. Procedural fairness concerns in the future both human to human, human to machine and machine to machine interactions

119 *See* para 4 of the preamble of the GDPR: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties..". *See* also Finnish Parliament Constitutional Law Committee Opinion PeVL 14/2018 vp. - HE 9/2018 vp.

when more or less intelligent capacity is added to the machines. Recent discussion also shows that emotional intelligence can at least to certain extend to be added to the intelligent machines with even today's techniques of machine learning.

Principles of administrative law, in particular the service principle, provide even today a good collection of long time savoir-faire and a good point of departure to development of procedural fairness and emphatic encounters in law, which are needed to maintain and develop trust. Digital platforms of public administration are one of the future essence and realisations of service principle and the very same principle can guide in the construction of choice and consent to the digital interfaces.

The fundamental underlying idea of the contextual realism is to care for the relevance and efficiency of rights (effet utile) in the digital environment. Legal certainty contributes to generalised trust and creates trust between potential and actual transaction partners. Legal certainty in digital platforms depends on the rights by design and default and on the good information management practises – once again long time topics of and contributions by Nordic legal informatics. Demonstration of the writing of data protection to the risk management and processes of information systems is also the core of the principle of accountability as it is understood in the GDPR. Legal certainty and accountability as such contribute to the trustworthiness of the platform infrastructure and applications and to the trust towards the platform and the whole ecosystem resting on the platform.

Legal certainty and effectiveness and efficiency of rights depend also on the active and up-to-date supervision and enforcement of the rights. The GDPR and the digitalisation of public administration elevate the societal role and significance of the oversight provided by data protection authorities. In the evolution of the law to partly unknown waters of digital platforms and service ecosystems the general supervision of law can make significant contributions as it has done to fill lacunaes and remedy shortfalls and contradictions in the past and provided juridical leadership in the application of new information rights. In Nordic law, particularly in Sweden and Finland the Supreme Guardians of Law the Parliamentary Ombudsman and the Chancellor of Justice contribute to the evolution of the principles of law to meet the needs of digital society and administration based on platforms. Supreme Guardians of Law also supervise the data protection authorities and by doing both they are significant actors of maintaining and building trust in digital administration and digitalised society. Their specific advantage is the long time focus and experience on the procedural fairness and on their proactive capacity to act in the difficult balancing of various rights and with their right of initiative to act also on the occasions where current law and its application leave individuals and enterprises without adequate protection.

Automation