Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union

Report Full Version

*Paloma Krõõt Tupay**

If we define law as a system of rules which a particular country or community recognizes as regulating the actions of its members and which it may enforce by the imposition of penalties, then the question arises: Which are the rules suitable for a digital county? Are people's rights in a digital nation better protected or do they need enhanced safeguards? Does rights' protection in the digital era need a new approach? Does a digital society have to leave behind the principle ideas of private life and informational self-determination? Searching for answers to these questions, the following long version of this report on Estonia (for the short version see EDPL 2020-2) first introduces the reader into the meaning and content of the Estonian 'e-state'. On that basis, it then reflects on the digital nation's impact on the individual and his or her rights and by this, on the questions the legal system has to provide answers for in a digitsed society.

I. Introduction: The Success Story of 'E-Estonia'

In December 2017, The New Yorker published an article with the headline 'The Digital Republic'.[1] The digital republic described therein is Estonia. Almost 90% of the Estonian population uses the Internet regularly, 99.6% of banking transactions are done electronically, 99% of public services are available online, without queueing.[2] Only marriage, divorce and the sale of real estate cannot be concluded exclusively online.[3] More than 95% of people submit their income tax return online, 95% of data stored by hospitals and family doctors is digital.[4] Entrepreneurs establish new businesses and submit their annual reports via the e-business register.[5] Since 2002, more than 500 million Estonian digital signatures have been used, more than in the rest of the European Union altogether.[6] To put it in the words of the President of Estonia, Kersti Kaljulaid: 'globally there is no other digital nation that has a state'.[7]

* Dr iur Paloma Krõõt Tupay, Lecturer in Constitutional Law, School of Law, Department of Public Law, Tartu University, former legal adviser to the President of Estonia. For correspondence: <palomakreet.tupay@ut.ee>. The author thanks Monika Mikiver and Maris Juha for their valuable advice and helpful suggestions. The responsibility for the correctness of any information, statement and opinion stated in the report resides solely with the autor. An abridged version of this report was published in issue 6(2) EDPL.

1 Nathan Heller, 'The Digital Republic' *The New Yorker* (18 and 25 December 2017) <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>. All URLs in this contribution were last accessed 1 May 2020.

2 Enterprise Estonia, 'e-Estonia facts' <https://toolbox.estonia.ee/media/1780>.

3 Enterprise Estonia, 'e-governance' <https://e-estonia.com/solutions/e-governance/>. Concerning the obligatory involvement of the notary in agreements concerning the transfer of real estate, there are already initiatives to replace the necessity of physical presence of the parties by video transmission.

4 ibid.

5 Enterprise Estonia, 'e-Estonia guide' (2019) 4, 9 <https://e-estonia.com/toolkit/>.

6 ibid.

7 Speech of the President of the Republic of Estonia, 2 November 2018 at Columbia University <https://president.ee/en/official-duties/speeches/14790-president-kaljulaid-at-columbia-university/index.html> .

In the last 29 years, Estonia - a country of 1.3 million inhabitants, a bit larger than the Netherlands[8] and half-covered by forest - has strode forward in seven-league boots. Estonia regained independence in 1991, which ended a period of more than 50 years occupation by the Soviet Union. The traces the foreign rule left on the country where immense. The economy was on its knees, the state system ailing. Everything had to be reinvented from scratch, and the Estonians did so. One of the things they did was to put their long dream of a free, democratic country on solid ground: on 24 June 1992 Estonians adopted the Constitution of the Republic of Estonia (EC) by popular vote.[9] The task fulfilled by the fathers and mothers of the Constitution, who had themselves been kept forcibly away from the developments of the democratic legal systems for so long, is impressive. They had managed to draw up in less than a year – with not much more than the periodic help of different international legal experts – a new constitution, that laid ground for a legal state order that has been in force since. The EC has been called one of the 'interesting constitutions' of modern times[10] and gained special attention on grounds of its modern fundamental rights catalogue.[11]

Still, despite a resolute money reform, privatisation and a clear decision in favour of a liberal market economy, Estonia was in the beginning of the nineties a very poor country, with an average monthly income of 30 dollars in 1992.[12] From the need to build up a country affordable for its small number of inhabitants and the necessity to find something that would put Estonia on the map, the decision of embracing the newly arisen interest for an 'information society' was born.

Based on a respective initiative on European Union (EU) level,[13] a group of experts published in 1994 its project 'Estonia's way into information society'.[14] In 1997, the so-called Tiger Leap Program was launched. Its aim was to equip Estonian schools with information and communication technology and the knowledge of how to use it. This program is considered one of the cornerstones of the 'Internetisation' of the Estonian society.[15] In 1998, the Estonian parliament adopted formally the 'Principles of Estonian Information Policy', designating the following four main aims: modernisation of legislation, promotion of the private sector, enhancing communication between the state and its citizens and awareness concerning the problems of an information society.[16] One of the key elements of the successful implementation of the e-state has been the close cooperation of the state and the private sector, especially Scandinavian banks interested in this new market and its opportunities.[17] The banks were also pioneers in offering customers their services online.

From 2000, the so-called e-Cabinet provides the means for a paper-free governmental decision-making process.[18] In the same year, the Estonian electronic tax board was introduced and reached a major developmental milestone with the introduction of automated tax declaration forms helping to reduce drastically the time spent by private individuals and en-

8 Netherlands total: approx. 41.5 sq km. Estonia: approx. 45.2 sq km. Source: Living in the EU <https://europa.eu/european-union/about-eu/figures/living_en>.

9 The Constitution of the Republic of Estonia (*Eesti Vabariigi Põhiseadus* 1992), English translation accessible at the State gazette <https://www.riigiteataja.ee/en/eli/521052015001/consolide> . Since 1 June 2010, the Estonian state gazette Riigiteataja is published online exclusively at <https://www.riigiteataja.ee> and contains next to the official Estonian legal acts English translations of several of them. English translations of Estonian legal acts are available at <https://www.riigiteataja.ee/en/>.

10 Manfred H. Wiegandt, 'Grundzüge der estnischen Verfassung von 1992' (*Main features of the Estonian Constitution from 1992*) (1997) 45 JöR 151, 151.

11 See further Wolfang Drechsler and Taavi Annus, 'Die Verfassungsentwicklung in Estland von 1992 bis 2001' (*The Evolution of the Constitution in Estonia from 1992 to 2001*) (2000) 50 JöR 473, 481 ff ; see also Peter Häberle, 'Verfassungsentwicklungen in Europa – aus der Sicht der Rechtsphilosophie und der Verfassungslehre'(*Evolution of constitutions in Europe – from the viewpoints of legal philosophy and constitutional theory*) (1994) AöR 169, 197 f.

12 Speech of the President of the Republic of Estonia (n 8).

13 European Commission White Paper on 'Growth, competitiveness, and employment' (1993); see also Bangemann Group report on the global information society (1994).

14 Tarmo Kalvet, 'The Estonian Information Society Developments Since the1990s' (2007), no 29 PRAXIS publication 10 <http://praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf> accessed 17 January 2020.

15 Pille Runnel et al, 'The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice' (2009) Journal of Baltic Studies 29.

16 The document (in Estonian) can be found at the homepage of the State gazette (n 10) <https://www.riigiteataja.ee/akt/75308> accessed 17 January 2020.

17 See also Kalvet 16 f (n 15).

18 e-Estonia guide 8 (n 6).

trepreneurs on filing taxes. An employee will nowadays spend less than five minutes in filling out his or her tax declaration.[19]

On 1 May 2004 Estonia became a member of the EU. Only one year later it was the first country in the world to introduce e-voting. At the elections to the European Parliament in May 2019 over 45% of the votes were cast online.[20] Like in all EU countries, the directly binding and applicable EU's General Data Protection Regulation (GDPR),[21] alongside with Directive (EU) 2016/680[22] establishing rules for the protection of individuals with regard to the processing of their personal data by police and criminal justice authorities, harmonize since 25 May 2018 data protection also in Estonia. The reformed EU data protection law's aim is to compromise on and harmonize the hitherto rather varied approaches of EU member states to data protection. Although the reformed EU data protection law allows for special national provisions and differences especially on questions concerning data handling by public authorities,[23] data processing in Estonia cannot be discussed without incorporating the direct as well as indirect effects of the respective EU law.

II. The E-State's Foundations

The two pillars of Estonian digital life are called digital ID and x-road.

1. Digital ID

In Estonia, the identity of every person – be it citizen or foreign resident – is based on a permanent individual ID code. The ID code consists of 11 numbers, of which the first indicates the person's gender (even numbers for women, uneven for men) and the following six correspond to the person's birth date[24]; the next three are serial numbers for people born on the same day and the last one serves as control number.[25]

This ID code may be published for the purpose of identification of the person. The Estonian Data Protection Inspectorate (DPI) has affirmed that the ID number is, just like the birth date, is not considered to be sensitive, ie a special category of data.[26] The regulation foreseeing the string of numbers of the ID number has never been legally contested. The only mandatory identification document in Estonia, the ID card, carries inter alia the card holder's photo and ID code and serves as personal identification document. Additionally, the card's chip includes two electronic certificates: one allowing for the digital authentication of the person – the digital ID - , the other one enabling the card holder to sign documents electronically.[27]

The digital identity of an Estonian citizen is generated automatically when the doctor enters the birth data of a child into the e-health system. Later, the parents can add the child's name to the digital identity – online.[28] Therefore, every Estonian citizen has a

19 ibid 4, 6.

20 Estonian National Electoral Committee, 'Statistics about Internet voting in Estonia' <https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia> .

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

22 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016) OJ L 119/89.

23 See eg Jürgen Kühling and Florian Sackmann, 'Datenschutzordnung 2018 – nach der Reform ist vor der Reform?!' (2018) NVwZ 681; Holger Greve, 'Das neue Bundesdatenschutzgesetz' (2017) NVwZ 737, 737 f.

24 Eg in case of 10 December 1977: 101277.

25 See further, Electronic Identity (eID) Application Guide, A Short Introduction to eID <https://eid.eesti.ee/index.php/A_Short_Introduction_to_eID>. As to the legal regulation: Population register Act para 39 s 1: 'A personal identification code is a number formed on the basis of the sex and date of birth of a person which complies with the standard of the Republic of Estonia and allows the specific identification of a person.'

26 See respective information on the Estonian Data Protection Inspectorate's homepage: <https://www.aki.ee/et/kas-isikukood-delikaatne>; Sensitive data are today considered to be special categories of data, see also recital 10 GDPR and art 9 GDPR.

27 The digital ID can nowadays also be accessed via mobile phone – the so-called mobile ID – and directly online, as 'smart ID' service. The mobile ID, that has the advantage that the mobile ID can be used without a card reader, is based on a special SIM-card, which can be obtained from the mobile phone operator, see further <https://www.id.ee/index.php?id=36882>. The smart-ID is an app that can be used on a modern smartphone or a tablet. It enables the user to access e-services or digitally sign Document without the additional need of a special SIM-cards or a card-reader <https://www.smart-id.com/>.

28 Ministry of the Interior, information on the Population Register, 'Personal identification code' <https://www.siseministeerium.ee/en/population-register>; also: Speech of the President of the Republic of Estonia (n 8).

digital ID, which is assigned also to every foreign permanent resident of Estonia.[29] This digital ID enables the person to identify him- or herself online and thus use the services provided by the state. Additionally, this way of authentification can also be used by private service providers. Therefore, the digital ID is in practice also used as online banking ID and as supermarket client card.

2. X-tee and the Once-Only Principle

The X-tee (English: x-road), the data exchange layer for the nation's various public and private sector e-service databases and other information systems,[30] forms today the heart of Estonian digital services. It links the different databases and information systems and allows for fast and secured internet-based data exchanges between them,[31] thus making it – inter alia – possible to present one's tax declaration within a few minutes: the tax and customs board forwards the taxpayer a pre-filled declaration in which information obtained by other institutions – in this case, the population register and the commercial register[32] – has already been inserted. The taxpayer can simply approve the declaration with his or her digital signature or make necessary amendments before doing so.[33]

The idea that the public authorities should never ask a second time for information the person or institution has already provided to the authorities, has also been written into law. According to the Public Information Act's (PIA) § 43[1] section 3: 'Collection of data in the database shall be based on the one-request-only principle'.[34] This idea, named also the 'Once Only Principle', has also been embraced at EU level. In 2009, the Ministerial Declaration on e-Government stated that the members' intent to jointly investigate how member states' public administrations can reduce the frequency with which citizens and businesses have to resubmit information to appropriate authorities.[35] The EU ministers responsible for e-Government reaffirmed in the Tallinn e-Government declaration of 2017 their commitment to implement the once-only principle for key public services[36] and the European Commission declared to launch a pilot project for the 'Once-Only' principle and explore the possibility of its EU wide application in its Digital Single Market Strategy.[37] However, the application of the 'once only' principle raises also questions regarding its compatibility with EU data protection law, especially the purpose limitation principle, according to which personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.[38] Since the adoption of the Data Protection Directive in 1995,[39] the purpose limitation principle constitutes one of the EU's data processing basic concepts and is today laid down in Article 5 paragraph 1 (b) GDPR. The limitation of the

29 Identity Documents Act (*Isikut tõendavate dokumentide seadus* 1999) para 6 and para 20[1] s 2, <https://www.riigiteataja.ee/en/eli/529032019005/consolide>.

30 Homepages, Excel spreadsheets, slides etc may constitute other information systems, see: Andmekaitse Inspektsiooni Andmekogude Juhend (*The Estonian Data Protection Authorities' Guidelines on databases*) (updated version 2016, Estonian only) 3 <https://www.aki.ee/et/juhised> .

31 Further information can be accessed at the Information System Authority's homepage 'Data Exchange Layer X-tee' <https://www.ria.ee/en/state-information-system/x-tee.html>.

32 Employers are required to register the persons employed by them in the employment register, which is maintained by the Tax- and Customs-Board itself.

33 Estonian electronic tax filing is explained in more detail as showcase at <https://scoop4c.eu/showcase/electronic-tax-filing-e-tax>. The SCOOP4c project is project launched by the European Commission in 2016 exploring how the once-only principle in public service provisioning can be implemented at European level..

34 Public Information Act (*avaliku teabe seadus* 2000), English translation accessible at the State gazette (n 10) <https://www.riigiteataja.ee/en/eli/529032019012/consolide>; similarly, ibid, the General Part of the Economic Activities Code Act's (*Majandustegevuse seadustiku üldosa seadus* 2014) para 13 prohibits economic administrative authorities to require from undertakings already submitted information.

35 Ministerial Declaration on eGovernment, the so-called Malmö-Declaration of 18 November 2009, accessible at <https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration>.

36 Ministerial Declaration on eGovernment - the Tallinn Declaration of 6 October 2017, ibid.

37 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (SWD(2015) 100 final, 6 May 2015). Ongoing EU-projects on the implementation of the once-only principle are eg the SCOOP4c project (fn 33) and the TOOP project, which aims to explore the poosibilities of the application of the once-only principle across borders (see further at <http://www.toop.eu/info>).

38 See further Mario Martini and Michael Wenzel, ''Once only' versus 'only once': Das Once-only-Prinzip zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit' (2017) DVBl 749.

39 See art 6 para 1 b) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, 31.

data handling purpose aims at enhancing trust between the data subject and the data controller, by limiting the controller's right to pass on the data subject's personal data to an unlimited number of data processors unknown to the individual concerned.[40] It is considered a 'cornerstone' of the right to data protection and forms as such also part of the OECD Privacy Guidelines[41] and the (updated) Council of Europe's Convention 108 on data protection.[42] The 'once only' principle foresees a comprehensive exception therefrom.

When creating the concept of the x-layer, it was initially held that the data obtained by the authorities in the conduct of their tasks belongs to the state as a whole.[43] According to the Estonian Data Protection Authority's guide on databases from 2016, the right to (re-)use data obtained on a previously different purpose is based on the data processor's legitimate right to use data in order to perform its public tasks.[44] This legal basis can again be deducted from the GDPR, according to which data processing shall be considered lawful if it s compliant with a legal obligation to which the controller is subject (Article 6 (1)(c) GDPR or/and necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e) GDPR)).[45]

At EU level, the European Data Protection Supervisor (EPDS) presented his opinion on the 'once-only' principle in 2017. Welcoming the Commission's proposal to modernise administrative services and agreeing that easing administrative burden on individuals or organisations, increasing efficiency of administrative procedures and saving time and resources are worthwhile public interest objectives, he notes that these do anyhow not constitute a separate ground under Article 2 (1) GDPR which would provide a general legal reason for restricting the principle of purpose limitation.[46] The EPDS therefore proposes inter alia to state that the proposal does not in any way aim to provide a restriction on the principle of purpose limitation pursuant to Articles 6(4) and 23(1) GDPR.[47] Regrettably, the EDPS does not substantiate how this statement could be considered to be well founded.[48] According to the European Digital Rights (EDRi) advocacy group the once-only idea could potentially reduce citizens' control over their personal data. Therefore, its implementation has to prioritise privacy by design and default.[49] Additionally, the EDRi points at the need to adequately assess and solve the risks that follow from the fact that the implementation of the once-only-principle can lead to more profiling of citizens.[50]

III. The Idea of an Open Information Society

The underlying idea of the Estonian digitisation is that of an open information society.[51] The fundament for this idea can also be found in the Estonian Constitution. According to paragraph 44 EC, everyone has to have free access to public information and state agencies and local governments have the duty to in-

40 See also Ioannis Revolidis and Alan Dahi, 'Further Processing of Personal Data – Is there a Future for the Purpose Limitation Principle in the Upcoming General Data Protection Regulation?' (2015) ZD-Aktuell 04618.

41 The OECD Privacy Guidelines, ch 1. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) Part Two. Basic principles of national application, p 9.

42 Amending protocol (CETS No 223) amending the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018 art 5 s 4 b.

43 Riina Kivi, 'Riigi andmekogude hetkeolukord ja Andmekogude seadus' in Infotehnoloogia avalikus halduses. Riigi Infosüsteemide Osakonna Aastaraamat (*Yearbook of the state information systems department*) (2003) ch 10.1.

44 The Estonian Data Protection Authorities' Guidelines on databases (n 31) 12.

45 Justiitsministeerium, 'Isikuandmete kaitse uue õigusliku raamistiku kontseptsioon' (10.05.2017 toimiku nr: 17-0584) (*Concept of the new legal framework on the protection of personal data*, Estonian Ministry of Justice 10 May 2017) 10 f, 33 <http://eelnoud.valitsus.ee/main/mount/docList/db80bf57-35ca-41e3-be15-827a2f056fdd#aek0ABB0>.

46 European Data Protection Supervisor, 'A digital Europe needs data protection'(2017) 6, 10 <https://edps.europa.eu/press-publications/press-news/press-releases/2017/digital-europe-needs-data-protection-0_en> accessed 17 January 2020.

47 ibid 13.

48 An national level, the author is at present undertaking a legal analysis on this question together with PhD student Monika Mikiver.

49 European Digital Rights, 'Analysis: A truly Digital Single Market?'(2015) 2 <https://edri.org/files/DSM_Analysis_EDRi_20150617.pdf> accessed 17 January 2020.

50 ibid 8 ff.

51 See Kalvet (n 15).

form citizens about their activities and give them access to information the institutions own about them.[52] Furthermore, everyone has the right to address notices and statements to governmental and local authorities and receive answers to them as provided by law according to paragraph 46.[53] This right, unknown to Estonia's previous constitutions, was included in the new EC with an explicit referral to countries under the rule of law, where in the view of the Constitutional Commission such a right had to apply.[54] The open information society's legal framework is today laid down in the PIA which aimed to establish a basis for the transparent exercise of public power, which would enable the public to control its execution.[55] In addition, the hoped-for cost-efficiency of public administration was an additional important argument for a small and young' country as Estonia to embrace digital solutions.[56]

1. Obligation to Disclose Information

According to the PIA, governmental agencies and institutions as the chancellery of the Estonian parliament (*Riigikogu*), the office of the president, the Office of the Chancellor of Justice, the courts, and legal persons in public law are required to maintain websites for the disclosure of information (paragraph 31 PIA). All data contained in public databases to which access is not restricted as well as data which the holder of the database considers necessary to make publicly available, shall be published online (paragraph 28, pages 30 and 32 PIA). Amongst other, information concerning public institutions, including their budgets as well as civil servants' salaries have to be public (paragraph 28 PIA). The disclosure obligation applies also for draft acts and regulations and for court decisions, furthermore, for the lists of members of political parties (paragraph 28, pages 15-17, 29 and 28 PIA). Apart from that, the PIA interdicts to restrict the publicity of supervisory and disciplinary measures and offences that are not yet time-barred (paragraph 36(1), page 12 PIA).

3. Obligation to Maintain a Document Register

Furthermore, the PIA establishes the obligation of any public institution to maintain a document register, ie a public digital register that records all documents received by the agency and prepared by it. As far as access is not limited on special grounds – eg information obtained in the course of criminal proceedings, information containing special categories of data[57] etc. – all document contents can be freely accessed by anyone (paragraphs 12 (4) (1) and 35 PIA). Paragraph 14 PIA gives everyone the right to request information from the holder of it, without the need for special justification.

4. Official Databases

The PIA sets also the rules for databases the state, local governments or other persons maintain for performing public duties provided by law. As a rule, these have to be public, as long as the law does not provide otherwise (paragraph 43(8) PIA). The public databases – such as the population register, the land register, the criminal records database, the register of farm animals and other – may contain any information associated with the performance of a public duty (paragraph 43 (1) PIA). According to the law a database does not necessarily have to be kept in digital form, but as it shall in general be registered in the administration system of the state information

52 EC para 44. '(1) Everyone is entitled to free access to information disseminated for public use. (2) Pursuant to a procedure provided by law, all government agencies, local authorities, and their officials have a duty to provide information about their activities to any citizen of Estonia at his or her request, except for information whose disclosure is prohibited by law and information intended exclusively for internal use. (3) Pursuant to a procedure provided by law, any citizen of Estonia is entitled to access information about himself or herself held by government agencies and local authorities and in government and local authority archives. This right may be circumscribed pursuant to law to protect the rights and freedoms of others, to protect the confidentiality of a child's filiation, and in the interests of preventing a criminal offence, apprehending the offender, or of ascertaining the truth in a criminal case. (4) Unless otherwise provided by law, citizens of foreign states and stateless persons in Estonia enjoy the rights specified in para s two and three of this s equally with citizens of Estonia.' (see also n 10).

53 ibid para 46.

54 Viljar Peep (ed.), 'Põhiseadus ja Põhiseaduse Assamblee' (*The Consitution and the Constitutional Assembly*) (Juura 1997) 551.

55 Explanatory memorandum to the Public Information Act draft act no 462 (20 June 2000) 18. All parliamentary draft acts incl therewith connected documents can be accessed in Estonian at the homepage of the parliament of Estonia at <www.riigikogu.ee>.

56 ibid.

57 see n 29.

system that allows the database to become part of the data exchange layer x-tee, it usually has to (paragraph 43(1), (2) and (7) PIA).

5. Limits of Disclosure

The law also provides for the grounds to classify information as internal. According to the PIA, information that could endanger foreign relations, inner security or military defence (paragraph 35 PIA, p 3-6) shall not be disclosed. The obligation of non-disclosure applies also to information containing special categories of personal data, ie data containing details of a person's family life or health and information that significantly breaches the inviolability of private life (paragraph 35, pages 11-14).

Private life is protected also under Estonian constitutional law. According to EC paragraph 42, government agencies and local authorities may not gather or store information on its citizens' convictions against the will of the concerned individual. The EC's paragraph 26 protects everyone's right to privacy and the Estonian State Court has already in 1994 acknowledged the right to informational self-determination.[58] The court has not itself specified this rights' content, but only stated its validity. From its 'creation' by the German Constitutional Court in 1983 it can be derived that it comprises the individual's right to decide if and to what extent the person's data is collected and stored by the state.[59] The Estonian personal data protection act (PDPA) ensures the individual's right to protection of his or her data. The PDPA is considered to be *lex specialis* in relation to the PIA.[60]

6. Obligation to Inform the Data Subject

The individual's right to know who is processing his or her data is protected by a right of inquiry. As enshrined in EC paragraph 44 section 3, every Estonian citizen is by law entitled to access information held by the authorities about him- or herself. This right may be invoked by a request for information collected upon performance of public duties[61] or by a request for explanation.[62] The request can be submitted by anyone and does not require a legitimate interest. Anyhow, the law also provides for grounds on which the addressee has the right to decline the request, eg in case restrictions on access apply to the information requested on grounds of their use in criminal or misdemeanour proceedings or in case it contains personal data and access to it could significantly breach the inviolability of private life of the data subject.[63] Siminarly, in EU law the GDPR's Articles 13 and 14 forsee the data controller's obligation to inform the data subject about the processing of his or her data and so does respectively the PDPA.[64]

Additionally, in Estonia any person can, by logging in into the State Portal – an online portal, from where public e-services and information about state-related activities can be retrieved[65] – access the personal data usage monitor. The monitor allows the data subject to check which public authority has been accessing his or her personal data in an online database.[66] However, not all databases' managers have yet decided to make use of this possibility, as joining the monitor is (today) optional.[67] Currently, the databases of the Citizenship and Migration Board, the Population Register, the Medical Prescription database, the Social Services database and the Unemployment In-

58 Judgment III-4/A-1/94 of the Constitutional Review Chamber of the Estonian Supreme Court from 12 January 1994, English translation available at <https://www.riigikohus.ee/en/constitutional-judgment-III-4A-194> accessed 17 January 2020: 'The lack of thorough regulation by laws and covert nature of the measures deprive a person of the right to informational self-determination, the right to choose his or her behaviour and the right to defend himself or herself.'

59 Judgment 1 BvR 209, 269, 362, 420, 440, 484/83 of the Bundesverfassungsgericht from 15 December 1983 (*Volkszählungsurteil*) II 1 b).

60 PIA, para 2 s 2 (n 35).

61 PIA, paras 1 and 6.

62 Response to Memoranda and Requests for Explanations and Submission of Collective Proposals Act (MRSA) (*Märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise esitamise seadus* 2004) para 2 s 2 <https://www.riigiteataja.ee/en/eli/501112016001/consolide>.

63 See PIA, para 23 ec 1 p 1) in conjunction with para 35 (n 35) and MRSA, para 1 s 3 (n 78) respectively.

64 See Personal Data Protection Act (*isikuandmete kaitse seadus* 2007, new version of 2019) paras 22 - 24 <https://www.riigiteataja.ee/en/eli/523012019001/consolide>.

65 The State Portal can be accessed (in Estonian, English and Russian) at <https://www.eesti.ee/et/>. For further information about the State Portal see <https://www.ria.ee/en/state-information-system/state-portal-eestiee.html>.

66 For more technical information, see information about the personal data usage monitor on the software development platform: <https://github.com/e-gov/AJ/issues/4>.

67 According to the information provided at the software development platform: <https://github.com/e-gov/AJ/blob/master/doc/spetsifikatsioonid/Tehniline_kontseptsioon.md>.

surance database apply the monitor.[68] Altogether, the government's information system comprises more than 1700 databases.[69] The manager of the database can also decide to restrict the data subject's access to information provided by the data monitor on grounds provided by law, for example on the basis of the PDPA that provides legal grounds on which the fact of data processing is not displayed, for example in cases this is deemed necessary for the detection or persecution of crimes or if this is considered to be necessary to protect other peoples' rights or national security.

IV. The Individual and the E-state – A new Beginning or the End of Self-Determination?

1. Databases and Personal Data

According to the law, public databases are established by law or by virtue of law,[70] but the type and composition of data collected in them is regulated in the statute of the respective database.[71] However, the establishment of a database as well as changes to the composition of its data shall be approved by the DPI.[72] An example that has raised questions is the Estonian Communicable Diseases Register (ECDR).[73] According to the statute, the sick person's profession, address and socio-economic status is amongst the data to be collected,[74] the register also foresees the registration of animal and tick bites.[75] Additionally, the data of the ECDR is stored 'permanently', ie forever.[76] The compatibility of this regulation with Article 5 GDPR, according to which only data necessary for the achievement of the processing purpose may be collected (data minimisation principle) and shall be deleted when no longer necessary (storage limitation principle), raises questions.[77] As can be seen from this example, the many registers maintained by the Estonian public institutions need careful permanent analysis in order to ensure their conformity with current law.

Another risk to be constantly kept in view are possible data leaks resulting from human failure. Such data leaks mostly occur where data that should be classified as internal (see above, III.4.) is mistakenly not. Where such leaks occur, their effect is significant. From last year, two major examples can be recalled. In one case, hundreds of children were affected, as a journalist found out that data on children's behaviour, mental condition and psychiatric reports had been publicly displayed in the schools' management information system for years.[78] In another similar case, information about conscipts' characterisations, health data and disciplinary proceedings, containing details of their behaviour, private life and psychological condition, had been publicly accessible in the Estonian Defence Forces register over years.[79] Interestingly though, such cases have not had a wider impact on peoples' confidence in the public registers. Also, questions of possible compensations for those affected by such leaks have not yet been a public issue of debate. This may for one reason be owed to the reluctance of the individual to sue the state as the evidently more powerful party. Additionally, the leak-

68 The databases of the Citizenship and Migration Board is managed by the Police and Boarder Guard Board, the Population Register by the Ministry of the Interior, The Medical Prescription database by the Estonian Health Insurance Fond, the Social Services database by the Ministry of Social Affairs and the Unemployment Insurance database by the Unemployment Insurance Fund.

69 According to the homepage of the Administration system for the state information system RIHA, the state information service comprises together with private information systems who have acceeded it, more than 2300 databases.

70 PIA, para 43^3 s 1 (n 35).

71 PIA, para 43^5 (n 35).

72 PIA, para 43^3 s 3 (n 35).

73 Nakkushaiguste ja nakkushaiguskahtluse esinemise ning haigestumise ohutegurite ja ennetamise kohta teabe edastamise kord, nakkushaiguste loetelu ja andmesubjekti isikuandmetega edastatavate andmete koosseis (*Statute on the notification procedure of communicable deseases infections and respective suspicions, hazards and prevention, list of communicable deseases and composition of personal data to be communicated* 2019) <https://www.riigiteataja.ee/akt/113032019241>; Information contained in the Communicable Deseases Register is exchanged via the communicable deseases database NAKIS; for more information, see: <https://www.terviseamet.ee/et/nakkushaigused-menuu/tervishoiutootajale/nakis> (in Estonian).

74 ECDR, para 1 s 5, p 3 (n 89).

75 ECDR, para 1 s 1, p 53.

76 ECDR, para 12 s 1.

77 GDPR, art 5.

78 Eeva Esse and Priit Pärnapuu, 'Sadade laste delikaatsed dokumendid rippusid aastaid avalikult internetis' (*Delicate documents of hundreds of children were for years publicly on the internet*), Estonian Newspaper *Postimees* (16 October 2018) <https://radar.postimees.ee/6429640/sadade-laste-delikaatsed-dokumendid-rippusid-aastaid-avalikult-internetis>.

79 Eve Loonde et al, 'Kaitseväe salajased dokumendid rippusid aastaid avalikult internetis' (*Secret documents of the Estonian army were for years publicly on the internet*), Estonian Newspaper *Eesti Päevaleht* (8 November 2018) <https://epl.delfi.ee/eesti/kaitsevae-salajased-dokumendid-rippusid-aastaid-avalikult-internetis?id=84260115>.

ing may not cause a measurable damage and the feeling of shame may prevail.

2. The Land Register

As a German data-leak in 2019 confirmed, the online publication of property owners' home addresses and their real estates may in some countries be considered a danger to certain people's safety, eg FOR politicians and persons of public interest.[80] In a small country like Estonia, where the home address of the prime minister is commonly known, the general online publicity of the land register provided for by law had long been considered unproblematic.[81]

At the end of 2019, however, the Ministry of Justice declared that in future, access to other persons' land register data will only be granted on condition that the interested person authenticates him- or herself online via ID-card, mobile-ID or internet bank link.[82] The ministry justified this decision on the grounds that an increasing number of citizens had written letters to the ministry and to the Chancellor of Justice, expressing their dissatisfaction with the fact that anyone could freely look up online which properties they owned. The Ministry further stated that the identification of the person would, on the one hand, enable the owner to see who had accessed his or her data in the land register and thus, by hopefully reducing the number of requests out of pure curiosity, enable a better protection of their data. On the other hand, the Ministry argued that authentication does not violate the legally required public access to the land register.[83] However, the Ministry did not specify whether it considered that there was a restriction of the publicity of the register. As the requirement of authentication is a purely technical solution and has no legal basis, its effectiveness remains uncertain.

It should be noted that the Ministry of Justice has linked the new regulation specifically to the EU data protection reform of 2018 and considerations of respective national amendments.[84] In the author's view, the increased interest of citizens in the protection of their personal data can also be associated not least with the EU's active stance in this regard.

3. Court Rulings

According to the EC paragraph 24 sections 3 and 4, court proceedings and the declaration of the court decision are usually public. The obligation to publish court rulings online forms part of the transparency principle established by the PIA.[85] When adopting the PIA in 2000 and regulating therewith the obligation to publish court rulings online, the lawmaker did not separately explain the regulations' proportionality,[86] nor did the State Court have to explain itself on that question.

Later attempts by the Ministry of Justice to restrict the principle of the publicity of court rulings have been met with harsh criticism. In 2014, the Ministry of Justice made public an amendment proposal, according to which the names of most convicted in rulings published online would have been substituted by initials – with the exception of certain serious crimes, such as trafficking in human beings, rape, murder crimes against the state and others – while access to the names of convicted persons would have been purchasable for four euros.[87] The explanatory memorandum commented on the proportionality of the proposal. But contrary to the newspapers' strong criticism that the proposed amendment would restrict the freedom of the press and information,[88] the

80 'Private Daten von Hunderten Politikern und Künstlern veröffentlicht' (*Private data of hundreds of politicians and artists published*) MDR aktuell news portal (4 January 2019) <https://www.mdr.de/nachrichten/politik/inland/persoenliche-daten-von-politikern-gehackt-100.html>.

81 See the electronic property register's homepage (English version): <https://www.rik.ee/en/e-land-register>.

82 'Kinnistusraamatus saab edaspidi otsinguid teha vaid ennast autentides' (*In future, searches in the land register can only be carried out under the condition of authentication*) Information by the Ministry of Justice (26 November 2019) <https://www.just.ee/et/uudised/kinnistusraamatus-saab-edaspidi-otsinguid-teha-vaid-id-kaardiga>; see also: II.1.

83 Land Register Act (*Kinnistusraamatuseadus* 1993) para 74 (see also n 10).

84 Newspaper *Postimees* (12 February 2019) <https://tehnika.postimees.ee/6521532/lugeja-kusib-kas-uus-e-kinnistusregister-ohustab-inimeste-privaatsust>.

85 PIA, para 29 s 1 and para 28 s 1 no 29 (n 35).

86 Explanatory memorandum to draft act no 462 (n 56).

87 Amendment act to the criminal procurement act and therewith connected acts, draft act no 578 SE (12 January 2014) <https://bit.ly/3gfvtcX>.

88 Tarmo Vahter, 'Riik hakkab kurjategijate nimesid müüma' (*The state plans to sell the names of criminals*), Estonian newspaper *Eesti Ekspress* (23 January 2014) <https://ekspress.delfi.ee/kuum/riik-hakkab-kurjategijate-nimesid-muuma?id=67659517>; Tarmo Vahter, 'Kohtuotsuses olgu nimed, mitte initsiaalid' (*Court rulings shall contain names, not initials*) Estonian Newspaper *Äripäev* (6 March 2014) <https://www.aripaev.ee/blog/2014/03/06/kohtuotsuses-olgu-nimed-mitte-initsiaalid>.

Ministry of Justice explained that the amendment was motivated by administrative reasons primarily. This was due to the fact that the implementation of the obligation to exchange the convicted names' with initials when their punishment becomes time barred had proven to be problematic, as copies of the previous personalized rulings could still be circulating on the internet and the fulfilment of the obligation caused a considerable administrative burden.[89] However, the amendment was not approved by the parliament. In 2018, the amendment proposals encompassing the enactment of the GDPR did ia. propose to shorten the period of time of publication of convicted names' depending on the severity of the offence committed.[90] According to the draft's memorandum, the publication of court rulings serves the interests of the public, such as transparency and control of the court, legal clarity, monitoring and harmonising of the application of law, general and specific deterrence.[91] However, the memorandum argues that not all of these aims require the publication of the name of the convicted during the whole length of his or her conviction, but can be achieved also with less intrusive measures, eg an individual request for access to the criminal records.[92] The proposed amendment did not become law.[93]

The extent to which the personal information of the litigants is published, has been adjusted over time. At present, in civil and administrative court rulings, the litigant (being a natural person) can request the non-publication of his or her name and ID code (or birth date).[94] In criminal proceedings, the defendant's name and ID code (or birth date) are replaced by initials or characters in case of minors, except in the case the minor is a third time offender. If the decision contains sensitive data or personal data the publication of which is restricted by law, the court shall refrain from the disclosure of the person's identity by replacing the defendant's name by initials or publishing only the conclusion or final part of the decision.[95]

4. Criminal Records

One of the most well-known Estonian databases is the Criminal Records database.[96] The database contains information about current convictions for misdemeanours and criminal offences. Since 2012, access to the criminal records of other people costs four euros per request. This is how much a person has to pay to get to know if the individual concerned has valid criminal offences.[97] No additional condition (legitimate interest or similar) has been since required. However, a person can check his or her own personal record for free. The lawmaker argued that due to the fact that court rulings were anyhow public and did not contain sensitive data,[98] there was no reason to restrict access to criminal records.[99] This argumentation has neither been contested by the Estonian public nor the courts.

However, the entry into force of GDPR has led to the conclusion that the respective regulation needs

89 'Justiitsministeerium põhjendab tapjate, röövlite ja väljapressijate kaitsmist' (*Ministry of Justice justifies the protection of killers, robbers and racketeers*), Estonian newspaper *Eesti Ekspress* (24 January 2014) <https://ekspress.delfi.ee/kuum/justiitsministeerium-pohjendab-tapjate-roovlite-ja-valjapressijate-kaitsmist?id=67671423>.

90 Explanatory memordandum to the Implementation Act to the Data Protection Act (IADPA), draft act no 650 (4 June 2018), 42 f <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/96c37d10-383c-40ad-87be-a8583008b994/Isikuandmete%20kaitse%20seaduse%20rakendamise%20seadus>; critical commentary on the planned changes: Tarmo Vahter, 'Kes kurat loob Eestis riiki, kus keegi midagi teada ei tohi?!' (*Who the hell creates an Estonian state in which no-one is allowed to know anything?!*) Estonian newspaper *Õhtuleht* from 21 June 2018 <https://www.ohtuleht.ee/883784/kes-kurat-loob-eestis-riiki-kus-keegi-midagi-teada-ei-tohi>.

91 ibid 62.

92 ibid.

93 Implementation Act to the Data Protection Act, draft act no 778 (13 December 2018) <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9d1420bb-b516-4ab1-b337-17b2c83eedb1/Isikuandmete%20kaitse%20seaduse%20rakendamise%20seadus778>.

94 Code of Civil Procedure (*Tsiviilkohtumenetluse seadustik* 2005) para 462 <https://www.riigiteataja.ee/en/eli/512042019002/consolide>; Code of Administrative Court Procedure (*Halduskohtumenetluse seadustik* 2011) para 175 <https://www.riigiteataja.ee/en/eli/521032019005/consolide> (see also n 10).

95 Code of Criminal Procedure (*Kriminaalmenetluse seadustik* 2003) para 408[1] s 2 <https://www.riigiteataja.ee/en/eli/515052019002/consolide> (see also n 10).

96 See also the Centre of Registers and Information System's homepage: 'Criminal Records Database' <https://www.rik.ee/en/criminal-records-database>.

97 According to the Criminal Records Database Act (*Karistusregistri seadus* 2011) para 19, information on offences of minors is excluded from the general publicity of criminal records; however, as an exception, access shall be granted i.a to an employer upon hiring the minor. The legal regulation is accessible in English at: <https://www.riigiteataja.ee/en/eli/ee/501042019021/consolide/current> (see also n 10).

98 Today named 'special categories of data' (see n 27).

99 Explanatory memorandum to the Criminal Records Database Act, draft act no 762 (13 December 2018) 2 <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8ffa1f1d-8dea-9b9b-53f1-ddf8f342a164/Karistusregistri%20seadus>.

to be amended, as it is not compatible with Article 10 GDPR, which stipulates that personal data relating to criminal convictions and offences shall be carried out under the control of official authority exclusively or if the respective legal base provides for appropriate safeguards for the rights and freedoms of the data subject.[100] According to the amended Criminal Records Database Act (CRDA) paragraph 15 section 1, in force since 1 March 2019:

> Everyone has the right to obtain data from the database concerning himself or herself or any legal person. When data of another person are request, the legal basis or objective of requesting the data has to be confirmed in the query.

As to the explanatory memorandum, criminal records of other natural persons will be accessible also in future on the grounds laid down in article 6 GDPR. That is, with the data subject's prior consent, on the basis of a respective legal base, if the processing is necessary for the performance of tasks of public interest, for the exercise of official authority, for the performance of a contract, for the protection of vital interests of the data subject, in case of preponderate legitimate interests of the controller or for the exercise of the press and information freedom.[101] The memorandum adds that the indicated grounds are neither separately controlled nor evaluated by the registrar.[102]

As of January 2020, the cited legal regulation has not been put into practice and online queries concerning criminal records of third persons do not require the entry of a special reason. It is also questionable if the requirement of 'control' by an official authority or respective safeguards, as set out by Article 10 GDPR can be considered fulfilled in case the right to obtain data on criminal convictions of third persons (CRDA paragraph 15 section 1) is in no way controlled by the authorities.

7. Parties' Membership and the Practice of Disclosure

The PIA includes also the obligation to disclose political parties' membership lists. The lawmaker did not comment on the grounds of that legal regulation, but the Estonian Chancellor of Justice did, who has analysed the act's lawfulness twice. In 2003, the then Chancellor of Justice Allar Jõks questioned the constitutional conformity of the regulation. Politicians and the public opinion did not follow the chancellor's concerns[103] and in his final conclusion that was published in 2004, he, too, took the view that the regulation did not infringe fundamental rights.[104] The arguments in favour of the regulation are in line with the opinion of the next Chancellor of Justice Indrek Teder, who in 2008, reiterated the view of the regulation's constitutional conformity.[105] According to these concurring opinions, a political party is not a secret or intimate organisation.[106] Therefore, it has to abide by the transparency principles stemming from democratic rule. Both opinions deem the arguments in favour of the publicity of political party affiliation to be significant, as it prevents corruption and conflict of interest and allow for a value-based execution of public power. Compared to that, the infringement of the individual's rights is considered moderate.[107] The chancellor of Justice's view of 2004 adds that a politically active person joining a political party has to be ready for an increased disclosure of his or her beliefs and acts and belonging to a political party is not obligatory.[108] Responding to the possible danger of stigmatisation and discrimination it is said that discrimination is forbidden by law and anyone discriminated against has the right to take legal measures.[109] Neither of the opinions made a difference between so-called ordinary party members and politicians. Nor did any of both address the probability and prospect of success of (potential) party members to take legal action against possible discrimination.

---

100 Explanatory memordandum to the IADPA 44f (n 97).

101 ibid, 45.

102 ibid.

103 Baltic News Service/Estonian news portal delfi from 26 July 2003: 'Jõks salastaks erakondade nimekirjad' (*Jõks would hide political parties' the membership lists*) <https://www.delfi.ee/news/paevauudised/eesti/joks-salastaks-erakondade-nimekirjad?id=6048372>.

104 The Chancellor of Justice's opinion nr 6-8/1443 from 30 September 2004.

105 The Chancellor of Justice's opinion nr 6-1/080996/00808156 of 28 November 2008 <https://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_puudmine_erakonnaliikmete_nimekirjade_avalikustamine_loppvastus.pdf>.

106 The Chancellor of Justice's opinion nr 6-8/1443 from 2004, 3 (n 111).

107 ibid.

108 The Chancellor of Justice's opinion nr 6-1/080996/00808156 from 2008, 8 (n 112).

109 The Chancellor of Justice's opinion nr 6-8/1443 from 2004, 3 (n 111).

Although Estonian political parties have been private organisations for more than 25 years now,[110] it is in the light of the country's historical background that people's attitudes towards political parties must be understood. During the time of Soviet Occupation, from 1940 until 1990, there was only one lawful political party, the Communist Party of Estonia. It was understood to be the extension of (Soviet) state power, not a tool to place political power into peoples' hands.[111] Extensive regulations on party financing and organisation adopted after regaining independence are likely to have confirmed the impression of political parties as centres of political power.[112] Also today, public trust in political parties is low,[113] civil and state control over their acting is deemed necessary and justified, as the Chancellor of Justice's opinions confirm. Additionally, Estonia's small size cannot be neglected in this regard. Patronage between higher state servants and political careers can hardly be excluded, it may in many cases even be justified by the simple lack of qualified leaders and masters of their craft.[114]

From the fact that court rulings, party affiliation and criminal records are public or at least publicly accessible, a new issue arose in the beginning of 2019, shortly before the Estonian parliamentary elections in March 2019. A media outlet published online and in the newspaper all names of party members serving sentences and those with valid – and partly also time-barred – offences and misdemeanours, including the acts committed by them.[115] While some political parties' statutes had regulations in force, excluding from membership for example people serving a sentence, others lacked respective regulations. Reacting quickly, the parties decided whom to exclude from the party and whom not. The parties' reactions were different: Some excluded only those whose convictions' were not yet time-barred, others decided to exclude members who had committed certain serious crimes and one small party decided to not exclude anyone, as according to their spokesman, people should have the right to go on with their lives after conviction.[116] Although it was mentioned on the fringes of the discussion that especially the disclosure of the names of those people whose conviction was already time-barred, might be very unpleasant for them, the public as well as the parties generally DID not call into question the behaviour of the journalists. There were also no debates concerning the legality of such a disclosure, as the journalists investigation was clearly in line with current law. According to the CRDA, a person's name in the respective court decision shall be replaced by initials after the punishment has been time-barred.[117] Anyhow, this regulation does not apply for certain offences, including murder, manslaughter and offences against minors, but also trafficking of narcotics, affiliation in criminal organisations and money laundering.[118]

The practice of public disclosure of infringements is not uncommon in Estonia. In the beginning of the 2000s, the city of Tartu had the practice of publishing online those people's names and debts, who owed

110 According to the Political Parties Act (*erakonnaseadus* 1994) para 1 s 2, political parties are in their legal nature non-profit organisations: <https://www.riigiteataja.ee/en/eli/513042015011/consolide> (see also n 10).

111 See also Allan Sikk, 'From Private Organizations to Democratic Infrastructure: Political Parties and the State in Estonia' (2006), 22(3) Journal of Communist Studies and Transition Politics 341, 345 f.

112 Compare ibid, 344; Ülle Madise and Allan Sikk, 'Die Institution der politischen Partei in Estland' in: D. Th. Tsatsos et al (eds), 'Parteienrecht im europäischen Vergleich, Die Parteien in den demokratischen Ordnungen der Staaten der Europäischen Gemeinschaft (2nd edn, Nomos 2006), ch 4, 4, 16 f.

113 According to the Europstat barometer of Februay 2019, political parties constitute with a support of 18% the least trusted Estonian institution, see: <https://ec.europa.eu/estonia/news/20190219_Eurobarometer_et> accessed 17 January 2020.

114 See also Madise and Sikk 7 f, 18 (n 119).

115 See for example: Joosep Tiks and Priit Pärnapuu, 'Peksjad, vargad, pedofiilid. EKRE liikmeskond kubiseb kurjategijatest' (*Violent criminals, thiefs, pedophiles. EKRE's supporters camp is overcrowded with criminals*), Estonian newspaper *Eesti Päevaleht* (22 January 2019) <https://epl.delfi.ee/eesti/kriminaalipaanika-pani-reformierakonna-enda-liikmete-hulgast-kurjategijaid-otsima-neid-leiti-ligi-pool-tuhat?id=85234743>; Joosep Tiks and Priit Pärnapuu, 'Punaste rooside okkad tilguvad verest. Sotside liikmeskonnas 165 kriminaali' (*The thorns of the red roses drip of blood. The membership of the social democrats membership 165 criminals*), Estonian newspaper *Eesti Päevaleht* from 30 January 2019 <https://epl.delfi.ee/eesti/punaste-rooside-okkad-tilguvad-verest-sotside-liikmeskonnas-165-kriminaali?id=85188135>; Joosep Tiks and Priit Pärnapuu, 'Kriminaalipaanika pani Reformierakonna enda liikmete hulgast kurjategijaid otsima. Neid leiti ligi pool tuhat, Estonian newspaper' (*Criminals' panic made the Reform party search for criminals in its own rows. Approximately half a thousand were found*), Estonian newspaper *Eesti Päevaleht* from 5 February 2019 <https://epl.delfi.ee/eesti/kriminaalipaanika-pani-reformierakonna-enda-liikmete-hulgast-kurjategijaid-otsima-neid-leiti-ligi-pool-tuhat?id=85234743>.

116 Marvel Riik, 'Üle 2000 partei-kriminaali: millised erakonnad on oma hingekirjast kurjategijad välja visanud?' (*Over 2000 party criminals: which parties have thrown the criminals out of their memberships lists?*), Estonian newspaper *Õhtuleht* (6 February 2019) <https://www.ohtuleht.ee/939948/ule-2000-partei-kriminaali-millised-erakonnad-on-oma-hingekirjast-kurjategijad-valja-visanud>.

117 CRDA, para 28 (n 106).

118 ibid.

the city money. Similarly, the Estonian police used to publish the names of those caught drunk-driving.[119] Both measures were taken without a respective legal regulation and were abandoned only after years without having had to face any legal consequences. However, similar practices have proven to be effective. Between 2010-2016, child support debtors were published online.[120] Already in the first nine days of the application of the measure outstanding sums in the amount of half a million euros were paid.[121] Such practices have been successfully applied also in the private sector. In 2008, a debt collection agency published on a billboard at one of the most frequented crossings in Tallinn a list of debtors who were legal persons in law, including their board member's names. The Estonia data protection agency argued that as the information on these debts was in accordance with the principle of publicity of public administration available to everyone on the commercial register, the publication did not breach privacy law.[122] The State Court confirmed the legality of the publication, as it considered it to be justified.[123]

As the aforementioned cases show, Estonian law considers the publication of offences committed by the delinquent to be part of public punishment by the society. This approach is likely to be in conflict at least with those European countries, which have a functioning rehabilitation legislation and policy in place. Ivo Pilving, today judge at the Supreme Court in Estonia, noted with respect to the proportionality of the disclosure of drunk drivers and debtors of communal debtors in 2004 that before applying public disclosure as a preventive measure, the lawmaker had the obligation to evaluate and, as far as necessary, to adjust the preventive effectiveness of the existing punitive measures. To ensure its proportionality, the state has to be able to control every penalty imposed by it. This is not given in the case of pillory, where the impact of the measure does not depend on the committed act's severity but on the (accidental) media and public's reaction.[124] Pilving referred also to the fact that the public stigmatisation of debtors may not have any positive effect where the debtor is simply lacking money, but even hinder him or her to find or keep an employment that makes the reimbursement of the debt possible.[125] Regrettably, these arguments have not gained further attention neither by the Estonian legislator nor by the public.

5. Profiling for the Person's Best Interest?

In 2017, the problem of the NEET youth ('youth neither in employment nor in education or training') became an issue of enhanced public awareness in Estonia. To tackle the problem, the government presented a legal amendment, with which it aimed to enhance the rapproachment of those young persons between the age of 16-26 into the labour market or into education. According to the amendment, the local authority where the young person is resident has the right to identify on its own initiative if that person may need assistance. This is assumed if the young person does neither work nor study and does not have any well founded reason for not doing so (reasons for exluding a person from the list are eg registration as unemployed, entrepreneurship, imprisonment, military service etc).[126] For the purpose of identifying

119 See also Paloma Krõõt Tupay and Monika Mikiver 'Der estnische E-Staat - zukunftsweisendes Vorbild oder befremdlicher Einzelgänger?' (*The Estonian E-state – forward-looking role model or odd maverick?*) (2015) 1 Zeitschrift Osteuropa-Recht 2, 27 f; Ivo Pilving, 'Sugupuud müügiks ja roolijoodikud häbiposti?' (*Genealogical records for sale and drunk drivers to pillory?*) (2004) II Juridica 75, 79.

120 From 2016, the information can be obtained by anyone who has access to the Estonian e-services by entering the person's name and ID code or birth date in the register of maintenance debtors. The legislator justified the amendment not by reason of a better rights protection but by the aim to avoid the duplication of data, see explanatory memorandum to the to the Code of Enforcement Procedure act and therewith connected acts amendment act, draft act no 803 (1 December 2014) <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6e9fb22e-69d1-449d-93a1-40fe2415c1a4/T%C3%A4itemenetluse%20seadustiku%20muutmise%20ning%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus>; child support debt information service <https://www.eesti.ee/eng/services/citizen/perekond_1/elatisvolgnevus>.

121 Report of the Estonian newspaper *Äripäev* from 10 June 2014, 'Häbipost tõi tagasi pool miljonit eurot' (*The whipping post brought the tax office half a million euro*) <https://www.aripaev.ee/article/2014/6/10/maksuameti-habipost-toi-juba-tagasi-pool-miljonit-eurot>.

122 Erik Rand, 'Andmekaitseseadus võlgades firma juhatust häbipostist ei päästa' (*The data protection act does not safe the indebted manager*). Estonian newspaper *Äripäev* (7 January 2009) <http://arileht.delfi.ee/news/uudised/andmekaitseseadus-volgades-firma-juhatust-habipostist-ei-paasta?id=51154582>.

123 Judgment 3-2-1-67-10 of the Civil Chamber of the Estonian Supreme Court (21 December 2010), 19. The decisions of the Estonian Supreme Court can be accessed on the court's homepage at <https://www.riigikohus.ee/> accessed 17 January 2020.

124 Pilving 83 (n 126).

125 ibid.

126 See for details the Social Welfare Act (*sotsiaalhoolekande seadus* 2015) para 15(1) <https://www.riigiteataja.ee/en/eli/522032019017/consolide> (see also n 10).

such persons, the Social Services and Benefits Registry is automatically screened for people who match those criteria twice a year. In order to determine the real need for assistance, the local authority may then contact the young people identified. If the person does not wish for his or her data to be processed, the processing of data shall be concluded upon receipt of a respective application.[127] The lawmaker did not make it a further point of discussion that the name and ID code of those young persons who decline further data processing by the local authority in this regards will anyhow be recorded in the database until the person's 27th birthday.[128] Such information may again lay ground for negative interpretation, as the young person has declined to accept help offered to him or her. Anyhow, the grounds for not working or studying are not known to the authorities; the young person can be touring the world, writing a book or similar.

The Estonian Data Protection Inspectorate's Director General and the Chancellor of Justice called into question the regulation's conformity with the EC paragraph 26 second sentence, according to which the public authority may interfere in any person's private and family life only in cases and pursuant to a procedure provided by law to protect public health, public morality, public order or the rights and freedoms of others, to prevent a criminal offence or to apprehend an offender.[129] According to their views, the 'preventive' interference into young persons' rights caused by the automatic screening of the Social Services and Benefits database might not be in accordance with the provision which requires a concrete danger for a legally protected right. Anyhow, the law was proclaimed by the president and entered into force in April 2018 and has so far not been contested before a court. The question of the conformity of the legal amendment was handled by the media on some occasions but did not gain the public's particular attention.[130]

6. Any Problems with the Digital Divide?

A recent decision delivered by the Estonian Supreme Court *en banc* addressed inter alia the legal regulation obliging unexceptionally all non-profit organisations to present annual reports to the non-profit associations and foundations register in digital form.[131] As an alternative, a notary public may be authorised by the organisation with the electronic presentation. According to the Notary Fees Act, this service currently costs 25 euros and 55 cents.[132] Failure to present annual reports leads to the deletion of the organisation from the register.[133] In the case at hand, the party claiming the unconstitutionality of the regulation was a small non-profit association which did not act for the public benefit nor carry out any economic activity. The court ruled the regulation demanding the presentation of annual reports exclusively in electronic form constitutional, with a minority of five judges out of 16 presenting dissenting opinions in this question.[134] According to the court, the regulation makes administration simpler and more effective and reporting more transparent and comparable.[135] As the decision notes, it may be assumed that a private legal person is today able to communicate with the state electronically.[136] The dissent-

127 ibid para 15(1) s 8: 'If the person who is 16-26 years of age does not wish for his or her data to be processed, the processing of data shall be concluded upon receipt of an appropriate application from the said person. Upon first contact with a person who is 16-26 years of age, the local authority shall ask the person for consent to further process his or her data. If the person does not give his or her consent, the further processing of data will be stopped. In order to rule out any further data processing only the personal identification code of the person shall be stored in the Social Services and Benefits Registry until the person attains 27 years of age.'

128 ibid.

129 Data Inspectorate's opinion no 1.2.-4/18/111 from 13 January 2018; Opinion of the Chancellor of Justice no 18-2/170578/1701993 (10 May 2017); see also III.4.

130 Laura Mallene, 'Andmekaitse Ossinovskile: erinevalt nõukogude ajast ei ole mittetöötamine kõlblusvastane' (*The Data Inspectorate to Ossinovski: Opposite to Soviet times not working is not immoral*) Estonian newspaper *Eesti Päevaleht* (8 May 2017) <http://epl.delfi.ee/news/eesti/andmekaitse-ossinovskile-erinevalt-noukogude-ajast-ei-ole-mittetootamine-kolblusvastane?id=78144546>; Monika Haukanõmm, 'Lapsed ei tohi olla vahend süsteemi katsetamiseks' (*Children may not be a tool for testing the system*) Estonian newspaper *Õpetajate Leht* (26 January 2018) <http://opleht.ee/2018/01/lapsed-ei-tohi-olla-vahend-susteemi-katsetamiseks/>; <http://opleht.ee/2018/02/riik-ulatab-noortele-oppima-ja-toole-asumiseks-abikae/>.

131 Judgment 2-17-10423 of the Estonian Supreme Court *en banc* from 2 October 2018.

132 Notary Fees Act (*Notari tasu seadus* 1996) para 31 p 25 <https://www.riigiteataja.ee/en/eli/512022018001/consolide> (see also n 10).

133 Non-Profit Associations Act (*mittetulundusühingute seadus* 1996) para 36[1] s 3 <https://www.riigiteataja.ee/en/eli/526032019007/consolide> (see also n 10).

134 Judgment 2-17-10423 (n 147). Dissenting opinion of the Judges Peeter Jerofejev, Henn Jõks, Ants Kull, Villu Kõve and Malle Seppik.

135 ibid; judgement's p 56; 59.1.

136 ibid; judgement's p 59.1.

ing opinion in this question rated the regulation to be disproportionate, as it does not allow for any exceptions for particular cases, as foreseen in many other regulations.[137] The possibility of turning to a notary is not enough to consider the requirement constitutional, as it demands additional financial and time consuming expenditures by the person.[138]

Following the judgement, the Chancellor of Justice asked in an opinion piece, if a person had the right to live without internet. If not, she suggested, the implementation of a fundamental obligation to its use should be considered.[139] Apart from that, the court's ruling did not gain any public attention. But the case serves as a reminder for an important aspect of digitisation: if digital solutions shall serve society as a whole, risks of a 'digital divide' have to be bestowed sufficient attention.

7. Health Data – a Wanted Asset

Estonia has also one of the world's most developed e-health systems. 99% of health data is digitised and 99% of prescriptions are digital.[140] The Estonian e-health Record is a nationwide system that integrates data from different healthcare providers and generates comprehensive medical records of each patient, including medical diagnosis, visits to doctors, prescribed medication, x-rays and other. Healthcare providers are obliged to submit their medical information to the e-health Record.[141] By logging into the e-Patient portal with the electronic ID,[142] the patient can then access his or her personal medical record. According to § 4[1] Health Services Organisation Act (HSOA), all health care providers, who have a legal obligation to maintain confidentiality, have the right to process personal data required for the provision of a health service, including personal data of special categories, without the permission of the data subject. However, the patient can choose to opt out of the rule of data sharing via the e-health Record. In this case, his or her health data is excluded from being shared between different healthcare service providers.[143]

Additionally, according to the HSOA, access to patients' health data for other persons may be provided for by law.[144] From the HSOA, it can therefore not be clearly deduced who may have access to the Record. One example of such a delegation can be found in the Insurance Activities Act (IAA). The IAA obliges public institutions and healthcare providers at the request of an insurance 'to transmit or grant' access to personal data of the data subject without his or her consent 'if the personal data are necessary to the insurance undertaking for the performance of an insurance contract and ensuring the performance thereof or for exercising the right of recourse.'[145] The norm's vague wording allows for a broad interpretation on how to secure insurancies access to the necessary data. Until today though, access is provided via public institutions and healthcare providers, the insurance companies themselves do not have direct access to the e-health Record.

Commenting on the regulations' proportionality, the lawmaker argues that the processing of health data by the insurances is justified by Article 9(2)(c) and (g) GDPR. The prompt compensation of the person entitled to insurance forms part of the public social protection system and is therefore in the public interest.[146] The legal regulations on insurance activities and the purpose limitation applying to the insurances' right to obtain data are considered suitable and specific measures to safeguard the fundamental rights and the purpose limitation interests of the data subject within the meaning of GDPR Article 9(2)(g).[147]

It should be noted in this respect that in 2015, the law and ethics working group took the view that access to the e-health database should not be given to entities lacking special expertise on the handling of

137 ibid. Dissenting opinion of the Judges Peeter Jerofejev, Henn Jõks, Ants Kull, Villu Kõve and Malle Seppik, p 28.

138 ibid; judgement's p 28 f.

139 Ülle Madise, 'Põhiseaduse areng ajaloolises ja võrdlevas vaates' (*The evolution of the constitution from a historical and a comparative perspective*) (2019) 1 Juridica 3, 10.

140 Information retrieved from Enterprise Estonia <https://e-estonia.com/solutions/healthcare/e-prescription/>.

141 Health Services Organisation Act (HSOA) (*Tervishoiuteenuste korraldamise seadus* 2001) para 59[2] <https://www.riigiteataja.ee/en/eli/508042019003/consolide> (see also n 10).

142 See above, part II.1.

143 The patient cannot exclude single information from being shared (eg on mental health), but can only choose to exclude all of his or her data from being shared. Only after that, he or she can decide on a case-by-case basis to share particular entries of his or her health record. The opt-out model's user-friendliness is therefore limited.

144 See HSOA (n 148) para 59(3) and (1).

145 Insurance Activities Act (*Kindlustustegevuse seadus* 2015) para 219 <https://www.riigiteataja.ee/en/eli/526032019002/consolide>.

146 Explanatory memordandum to the IADPA 49 (n 97).

147 ibid.

health data, as they may be unfit for its appropriate use.[148] The working group pointed to the many different cases in practice, where direct access to data systems, eg the population register, had resulted in an abuse by impermissibly broad use of this right by respective officials.[149] The working group referred also to an opinion of the EU Article 29 Working Party[150] of 2007, where the data protection experts took the view that health data collected for medical reasons should not be made accessible for third parties whose aims differ from those of the original data collector.[151] Additionally, the experts took the view that it was not enough to protect the data subject by allowing him or her to see who has checked his or her data and contest possible data infringements in court. As the private person is the weaker part of this legal relationship the responsibility to protect his rights cannot be fully delegated to him or her, because the person may not feel competent enough to assert his or her right.[152]

a. Insurance Funds and Health Data

As already pointed out by the law and ethics working group and the Article 29 Working Party,[153] there is an ever-growing interest and pressure from different private and non-private entities to get access to individuals' medical records. Notwithstanding, by the end of the same year 2015, the parliament seemed ready to adopt a legal amendment that would expressly give insurances direct and individual access to the e-health Record as such.[154] It was only for the very clear criticism from the Estonian Data Protection Inspectorate's Director General and the Chancellor of Justice that the amendment was not passed. Like before the working group, the data protection officer underlined the data subject's weaker position, which would also undermine a possible voluntary consent of the data subject, as the individual is in practice dependent on the insurance providers.[155] Providing the insurances with unrestricted access to all health data of every Estonian patient would open the opportunity for substantial misuse by persons not sufficiently competent in this field.[156] The parliament was finally convinced by these arguments and refrained from adopting the amendment. Still, this incident attests two things. First, the great interest of third parties to gain access to the information stored in the e-Health system. And second, the problem that modern legal regulations' technical content may not be fairly understandable to those – be it usual citizens or parliamentarians – who have not been thoroughly introduced to its content.

b. What Is It Worth?

If data – as is said – is the new oil, Estonia can consider itself a rich country. The question is now how to drill this oil. For the time being, the government has launched a new project to found a state enterprise, which would then be commissioned to anonymise collected health data and decide for whom, how and on which conditions the data obtained would be made accessible. [157] There have also been rumours of giving the data subjects themselves the right to decide to give health watches and

148 The Law and ethics working group (leaded by Reet Pärgmäe, set up as part of the e-health strategy by the Ministry of the Interior in 2015): 'Legal and ethical aspects for the governmental e-health strategy until 2020' (2015), 27 ff.

149 ibid, 28 f.

150 The Article 29 Working Party was an independent EU working party that dealt with issues relating to the protection of privacy and personal data and was made up of a representative from the data protection authority of each EU Member State, As of 25 May 2018, this body has been replaced by the European Data Protection Board. For more details, see: <https://ec.europa.eu/newsroom/article29/news-overview.cfm>.

151 'Legal and ethical aspects for the governmental e-health strategy until 2020' (n 155), 30, referring to: Article 29 Working Party working document on the processing of personal data relating to health in electronic health records (WP 131, 2007), 16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec11>.

152 ibid, 31 f.

153 See eg WP 131, 2007 (n 158) 5; 'Legal and ethical aspects for the governmental e-health strategy until 2020' (n 155), 27 ff.

154 Amendment act to the Working Ability Endorsement Act and other acts, draft act no 84 SE I (14 September 2015) <https://bit.ly/38jWZmZ>.

155 Letter of the Estonian Data Protection Inspectorate's Director General to the Social Committee of the Parliament from 19 October 2015, no 1.2.-4/15/1976, 3 f. The letter can be accessed at the web address of the amendment act in question (ibid).

156 ibid, 4.

157 Hans Lõugas, 'Eesti e-riigi uus suur projekt: hakkame meie rahva terviseandmetega suurt raha tegema' (*The Estonian e-state's grand new project: let's make big money with people's health data*) (Online portal digigeenius, 8 October 2018) <https://digi.geenius.ee/rubriik/uudis/eesti-e-riigi-uus-suur-projekt-hakkame-meie-rahva-terviseandmetega-suurt-raha-tegema/> and Hans Lõugas, 'Terviseandmete uue riigifirma plaan jõuab valitsusse' (*The plan on a new state enterprise for health data heads to the government*) (Online portal digigeenius from, 10 October 2018) <https://digi.geenius.ee/rubriik/uudis/terviseandmete-uue-riigifirma-plaan-jouab-valitsusse/>.

fitness trackers access to their health data.[158] No legal analysis has been presented in this regard so far. Attention has to be paid to particular commercial interests of different market players, bearing in mind the generally weaker position of the consumer.

V. Concluding remarks

1. The Estonian Understanding of Rights' Protection

The Estonians' approach to the processing and protection of their data has been depicted by a large-scale survey on the right to privacy as a human right and everyday technologies in 2014.[159] 41% of those questioned were of the opinion that the concerns about data protection were exaggerated,[160] 74% did agree with the statement that 'they have nothing to hide'.[161] 61% agreed with the claim that the state needs for a better rights protection more rights for data processing without the consent of the data subject. Likewise, 86% of Estonian inhabitants trust the Estonian police and 75% trust the Estonian army.[162] 83% of Estonian people believe that the data the state collects from them is sufficiently protected, the respective number for medical institutions is 81%.[163]

Referring to the survey of 2014, the British privacy advocate and academic Simon Davies called the results disappointing. According to him, the Estonians have not learned from their past under Soviet occupation and lack understanding for the danger that a so well informed public power in the wrong hands could bring about.[164] In the perspective of the author of this report, in order to understand the Estonian approach to data handling and protection, cultural and historical aspects of the country must not be neglected.[165] For one, Estonia has always been a small country with a population size of other countries' medium size towns; today, it has slightly more than 1.3 million inhabitants.[166] There is hardly any Estonian in his or her fourties who could get acquainted with someone he or she has never heard of. With this, clear demarcation between 'private' and 'public' life in everyday Estonian life has already long before digitisation been fluent. Secondly, Soviet occupation marked the Estonian society for more than fifty years, during which publification and sharing of personal information was common. It was not only used by the KGB, the Soviet Committee for State Security, who used civil informants as undercover agents to control the society and its members' thoughts and actions. It was also common to ensure conform behaviour by the dissemination of information between the people themselves: The employer was informed of sexually transmitted diseases of the employee, drivers caught drunk at the wheel were issued car badges starting with the number 'O',[167] divorce processes were published in the newspaper,[168] and it was the duty of the so-called comrade-courts established in each office, collective farm, school and district to judge about the insufficient education of children, improper behaviour in the familiy or cursing of their colleagues and neighbors.[169] It appears unlikely that such long-standing practices and cultural pecularities would not have any effects on the population's perceptions concerning the right to privacy.

This understanding holds in the author's view also the answer to the questions raised at the beginning of this report: legal regulations on rights' protection in a digitised country are not a primarily technical question the solutions of which can be applied in countries equally. Just as any other significant question, regulations are framed by the countries' his-

158 Paloma Krõõt Tupay, 'Sa ei põgene, vaba laps' (*You can't escape, free child*), Estonian Newspaper *Postimees* (13 November 2018) <https://arvamus.postimees.ee/6452035/paloma-kroot-tupay-sa-ei-pogene-vaba-laps>.

159 Study by the Estonian Institute of Human Rights, 'The right to privacy as a human right and everyday technologies' (2014) <http://www.eihr.ee/en/privacy-as-a-human-right-and-everyday-technologies/>.

160 ibid: methodology and results of the study, 48; summary, 4.

161 ibid 4, 49.

162 Homepage of the Ministry of Defence, 'Avalik arvamus riigikaitsest' (*Public opinion on state defence*) (autumn 2018) <http://www.kaitseministeerium.ee/et/eesmargid-tegevused/avalik-arvamus-riigikaitsest>.

163 Study on the right to privacy as a human right and everyday technologies (n 166), methodology and results of the study, 54.

164 See the critical statement of Simon Davies at the Annual Conference on Human Rights in Tallinn, Estonia, 10 December 2014, Session 1 part 5 <https://www.youtube.com/watch?v=PiTkSaJpwsw>.

165 See also Tupay and Mikiver 31 f (n 126).

166 See respective data at the Statistics Estonia homepage (as of 4 April 2019) <https://www.stat.ee/pressiteade-2019-007>.

167 See also Juhan Sepp, 'Tervislike eluviiside nimel IX' (*In the name of healthy lifestyles*), Estonian Newspaper *Nõukogude Õpetaja* (25 April 1987) 3 <https://bit.ly/3eSvUcU>.

168 For this, see also the referral in: Tiit Hennoste and Roosmarii Kurvits, 'Ei ole midagi uut päikese all' (*Nothing new under the sun*) Estonian magazine *Sirp* (8 June 2007) <https://sirp.ee/s1-artiklid/c8-meedia/ei-ole-midagi-uut-p-ikese-all/>.

169 See Kaarel Paas (ed.) 'Eesti seltsimehelike kohtute põhimäärus. Kommenteeritud väljaanne' (*Commentary on the basic regulation of the Estonian comrade courts*), Eesti raamat 1972.

torical background and society. The development of the notion of privacy has, even in a country as digitally progressive as Estonia, not generated a completely new understanding of privacy, but rather delineates a natural evolution of the perception of the relationship between the person's informational self-determination and public interest in Estonia over time. An additional argument for a less privacy-focused approach is certainly also the simple convenience of digital public administration – who would not like to present his or her tax declaration within a few minutes and replace hours of queuing at the authorities with a few simple mouse-clicks from home? However, the example of the Estonian regulation on public access to the land register shows that the understanding of data protection does by no means have to move linear in the direction of less data protection.

Digitisation does not necessarily mean the end of privacy or of self-determination as it is understood in the respective cultural space. The perception and extent to which the data handled by state authorities is made publicly available, processed or forwarded, is a question shaped by social attitudes and decided by the respective lawmaker.

At EU level, the reformed data protection law aims to constitute the basis for a common understanding of data protection within the Union. For this reason, this report also addressed its impact on national Estonian legislation and perception which has seen. As shown, the new EU data protection laws' entry into force in 2018 has led to amendment proposals and changes also in domestic Estonian law as a consequence.[170] It will be of decisive importance to further analyse and compare the application of both regulations in all EU member states, as interpretation of decisive indeterminate legal terms, such as 'public and legitimate interest', and the implementation of EU data protection law may vary significantly. At the same time, comparison and adaption of the different national understandings will be key to the best possible impact of data protection law in the EU, as this ensures a compromise based on all members states' contributions.

8. The Future of Data Protection in Estonia and the EU

In view of the almost infinite increase of ubiquitous data handling, Roßnagel stated already in 2005 that data protection needed an entirely new approach.[171] Particularly with regard to the principles of required consent and purpose limitation he argued that these were not compatible with the evolution of data processing.[172] As alternative methods to ensure adequate data protection, he proposed ia a better and more transparent technical data protection control not only at individual, but also institutional level.[173]

The EU lawmaker in turn decided to maintain the principle of purpose limitation and the general requirement of consent also in the reformed EU data protection law of 2018.[174] At the same time, the possibilities the 'once-only' idea offers for a simpler and more citizen-friendly provision of governmental services have not only found their way in national legislations,[175] but also into EU policies. However, unlike the Estonian Supreme Court, the EDPS has not accepted the easing of administrative burden and its increased efficiency as a justification for a possible limitation of data subject rights related to the digitisation of administrative procedures.[176] As data processing keeps expanding, there is a constant need for monitoring and adaption of data protection regulations. The Estonian e-state can insofar serve as a 'sandbox' for exploring possible new approaches and solutions.[177] Considering Estonia's positive experience with the application of the 'once only' principle in public administration, where the lawfulness of processing is justified by the processor's legal obligation and a respective public interest, it could be asked if the general necessity of consent, as laid down in Article 6(1)(a) GDPR, could to a broader extent be substituted by a system enabling the user to check at any time who has accessed his or her data. As the Es-

170 See eg IV.2.,3. and 4.

171 Alexander Roßnagel, 'Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung' (2005) 2 MMR 71.

172 ibid 72.

173 ibid 73 ff.

174 See GDPR art 5 s 1 point (c) and art 7. A respective critique can be found at: Winfried Veil, 'Die Datenschutz-Grundverordnung: des Kaisers neue Kleider' (2018) 10 NVwZ 686 ff.

175 See for other examples: European Commission, 'Final report: Study on eGovernment and the Reduction of Administrative Burden' (2014), highlighting as 'champions' United Kingdom, the Netherlands and Denmark, IV <https://ec.europa.eu/digital-single-market/en/news/final-report-study-egovernment-and-reduction-administrative-burden-smart-20120061>.

176 Compare II.2. and IV.7.

177 See also: Martini and Wenzel (n 39).

tonian case shows, further questions arise from that. One of them comprises the challenge to build a system transparent enough to make users trust the control systems provided by the public authorities. This includes sufficient transparency of the technological solutions used as well as about the information provided, including information on the exeptions of disclosure of information, such as data handling on grounds of state or public security.

Another challenge arising from the digitalisation of public administration is the one of adequate responsibility: To what extent should the state be liable for data leaks or the lack of sufficient (data) protection?[178] In principle, the GDPR provides a system that aims to solve this question.[179] However, as can be seen in the case of Estonia, this does not ensure that people make use of it. The grounds for that may be manifold, in case of Estonia partly also cultural, as the possibility to invoke one's rights was not acknowledged during Soviet times. Anyhow, as weaker party, the individual will generally be more reserved to claim his or her rights vis-à-vis the state. Estonian law has also not (yet) used the possibility provided by Article 80(2) GDPR, which gives member states the possibility to regulate non-profit organisations' rights to lodge collective complaints, ie hold data controllers or processors liable independently of a respective mandate by the data subject concerned.[180] A broader and simpler system of state liability for breaches of the right to privacy and data protection could enhance the authorities' efforts to ensure the protection of data subjects' rights. As the Estonian experience shows, the state may not always be motivated to end the disproportional handling of personal data promptly.[181] At the same time, personal data that becomes public knowledge has a great impact on the data subject's life.

With the adoption and entry into force of the GDPR, the EU member states have declared their willingness to not prioritise technology over the individual's rights. However, technology should not be seen as an antipode to peoples' rights, as a technologically advanced, simple and transparent system of public administration does equally serve better rights' protection and their exercise. Constant technological evolution and the nationally varying understanding of the GDPR make the coordinated comparison, analysis and development of data protection law at EU level a precondition for an effective data protection within the Union. It is the present report's aim to contribute to this process with an overview of the understanding of data protection within the framework of the Estonian e-state.

178 Compare eg above, the Estonian examples described in IV.1. and 5.

179 Compare GDPR arts 77, 78, 82; see also Karin Sein et al. Pilguheit andmesubjekti õiguskaitsevahenditele uues isikuandmete kaitse üldmääruses (*A glimpse into the legal remedies of the data subject provided by the new general regulation on data protection*) (2018) 2 Juridica 94; inter alia, Estonia has (as of today) not used the possibility to exclude or limit the right to impose administrative fines on public authorities and bodies, as foreseen in GDPR, art 83 s 7.

180 Karin Sein et al (n 187).

181 See eg above IV.4. and 5.