UDC 342.9(474.2)

HUMAN RIGHTS PERSPECTIVES ON LAW AND TECHNOLOGY – A PRACTICAL EXAMPLE: E-GOVERNANCE IN ESTONIA[1]

K. NYMAN METCALF[a]

[a]*Tallinn University of Technology, 5 Ehitajate Tee, Tallinn 19086, Estonia*

Changes in society caused by technology also lead to legal changes. Through history, there has quite often been concern about whether law should prevent or restrict new technologies or instead encourage innovation. This is nothing new. Changes are however increasingly rapid and potential effects on protection of rights more frequent. Technology can also help protect rights and for example assist effective governance, as is shown with the example of Estonia.

Keywords: human rights; e-governance; technology; Estonia.

Acknowledgements. The article is based on lectures given in Minsk in December 2019 supported by the Raul Wallenberg Institute of Human Rights and Humanitarian Law.

ПРАВО И ТЕХНОЛОГИЯ С ТОЧКИ ЗРЕНИЯ ПРАВ ЧЕЛОВЕКА НА ПРИМЕРЕ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В ЭСТОНИИ

К. НЬЮМАН МЕТКАЛФ[1)]

[1)]*Таллинский технологический университет, Эхитаятэ тээ, 5, 19086, г. Таллин, Эстония*

Изменения в обществе, вызванные развитием технологий, приводят к изменениям в законодательстве. В процессе исторического развития поднимается вопрос о том, должно ли законодательство препятствовать новым технологиям, ограничивать их или же, наоборот, поощрять инновации. В этом нет ничего нового. Однако изменения происходят все более стремительно, а их возможное воздействие на защиту прав ощущается все чаще. Технологии могут также способствовать защите прав и, например, эффективному управлению, как это показано на примере Эстонии.

Ключевые слова: права человека; электронное правительство; технологии; Эстония.

Благодарность. Статья основана на лекциях, прочитанных в Минске в 2019 г. и поддержанных Институтом прав человека и гуманитарного права им. Рауля Валленберга.

[1] Preparation of the article is organized by Raoul Wallenberg Institute of Human Rights and Humanitarian Law in the context of academic cooperation with the Belarusian State University and other Belarusian universities. This academic cooperation has been supported by the Government of Sweden represented by the Swedish International Development Cooperation Agency (Sida). Opinion of the authors expressed in this article may not coincide with the viewpoint of the Institute or Sida.

Образец цитирования:
Ньюман Меткалф К. Право и технология с точки зрения прав человека на примере электронного правительства в Эстонии. *Журнал Белорусского государственного университета. Международные отношения*. 2020;1:69–76 (на англ.).

For citation:
Nyman Metcalf K. Human rights perspectives on law and technology – a practical example: e-governance in Estonia. *Journal of the Belarusian State University. International Relations*. 2020;1:69–76.

Автор:
Катрин Ньюман Метклаф – адъюнкт-профессор коммуникационного права юридического факультета.

Author:
Katrin Nyman Metcalf, adjunct professor of communications law, TalTech Law School.
katrin.nyman-metcalf@taltech.ee

Introduction

Changes in society caused by technology also lead to legal changes. Through history, there has quite often been concern about whether law should prevent or restrict new technologies or instead encourage innovation. This is nothing new. There are well known and amusing examples, often quoted by authors, about how English law of the 1860s required a man to walk ahead any motor vehicle with a red flag, warning people on the road [1], or how in 1899 it was (allegedly) written that the US Patent Office could be closed as anything that could be invented was already invented[2]. These examples show how difficult it is to understand what the effects of technology may be, as well as illustrate the anxiety about how to fit technological advances into the legal system. Technological change has been a lot more rapid in the past decades than in previous centuries and technologies now form a greater part of our daily lives. Thus, it is not surprising that the questions of how law and technology fit together and if technology may affect human rights have achieved prominence in the debate in recent years.

The more technology becomes a part of our everyday world, the more ethical issues arise. Whether technology should be limited is not only a question of what it actually can do in practice or even of whether the law sets certain limits: it is also a question of whether policy decisions should be taken to limit technology for ethical or other reasons. Maybe not everything than *can* be done *should* necessarily be done. Reasons to limit technological advancement may be that it would present unforeseeable risks to humans or the environment or that it would dehumanise society. The role of law is to consider these "soft" aspects in addition to the more practical ones of liability, standards and similar. Legal obstacles to technical progress fall into two quite distinct categories: the obstacles caused by specific provisions in laws, which are temporary obstacles as legislation can be changed; and legal obstacles due to something being against fundamental human rights or ethics. The latter kind of obstacles can mean that certain technological progress should be limited or at least adjusted through regulation and laws.

Quite often, the legal discussion about the interrelationship between law and technology focuses on the possibilities or difficulties of the legal system to mitigate risks connected with technology. However important this is, it should not be forgotten that technology can also support the legal system, support the implementation of human rights and the rule of law. This can be seen for example in the context of "privacy by design" to implement data protection standards or by "automatic" transparency. As more and more countries get interested in introducing or increasing their use of e-governance, ways of applying technology to improve protection of rights provide an interesting area of study. Estonia is a world leader in e-governance, both as it started very early and thus already has considerable experience, and as its e-governance solutions are widely used by the population. In this article we look at the Estonian e-governance to see a practical example of what positive and proactive relations between law and technology can look like.

First, we touch upon general considerations of the interrelationship between law and technology, looking at risks as well as opportunities. In particular, we focus on principled issued such as human rights and rule of law (rather than on very essential but more practical legal questions of liability, intellectual property or details of data protection). The theoretical discussion is put in a practical context by presenting some examples of a digital society in practice, more specifically the very advanced e-governance applied in Estonia. It may be said already here in the introduction that this article raises more questions than it answers: this is inevitable for the fast-moving topic and it should not be a problem, provided that the questions raised give a better understanding of how to approach the issue, what questions to ask and whom to involve in the debate. The contribution we seek to make with this article is to highlight what issues we should think about, how and why.

An era of conflict and contradiction?

There are many examples of how modern technology creates situations in which different rights conflict with one-another – or even the technology as such appears to provide challenges to rights. We see many discussions on whether security or privacy should be given greater weight, for example in connection with facial recognition technology, CCTV or other surveillance systems. The possibility to sacrifice some privacy for convenience or efficiency adds another aspect to this balance. There are various systems for being able to pass quicker through airport security by giving information in advance for example. As security procedures get more and more inefficient and slow, we are many who are tempted by such possibilities. It is a le-

[2] Attributed to Charles H. Duell, commissioner of the US Patent Office. The quote is widely repeated in books or on-line, even if there is no actual evidence it was said or any credible original source. It is quoted as 1889 or 1899 in different places. These examples are mentioned by T. Kerikmäe and K. Nyman Metcalf (2020) in "The rule of law and the protection of fundamental human rights in an era of automation" (forthcoming) in the book "Smart technologies and fundamental rights" edited by J. S. Gordon.

gitimate question if everybody understands the possible drawbacks and whether the consent we may give is really informed as well as truly voluntary.

It is important to be aware of the fact that there is not one clear and correct answer to what should be given greater weight: privacy or security. It has to be seen case-by-case, situations change over time, there are fundamental political differences between viewpoints and so on. Consequently, it is a debate that should be ongoing with as many different interests as possible represented in the discussions. It is not something that one day will be solved. If the questions of today would be finally settled, technology will most likely entail new questions in the near future.

Another apparent conflict, which is not necessarily caused by technology but exacerbated by new means of communication, is the conflict between freedom of expression and reasons to restrict certain expressions. Privacy or data protection restricts access to information and transparency and may thus restrict freedom of expression. All these rights and freedoms are well worth protecting and it is inevitable that a careful balancing must be made. Data is not only protected in electronic form, also paper-based data should be protected, but given the many ways in which people can communicate directly even with a large, undetermined audience while at the same time more and more data about people is gathered and kept, there will be an increasing number of such potentially conflicting cases. The ease of communicating without going through "gatekeepers" in the form of editors, broadcasting station management or similar furthermore leads to new situations of conflict between freedom of expression and hate speech. Data protection rules – first via European Court of Justice (CJEU) case law [2], and later codified in the EU General data protection regulation (GDPR) [3], have added conflicts of their own, like between the right to be forgotten (right of erasure, Art. 17 of GDPR) versus transparency and historical truth.

In addition to an era of apparent conflict and contradiction, we are also in a situation in which many borders that have been very important for the legal system lose importance or at least change fundamentally. In cyberspace, there are no physical national borders, which makes the question of jurisdiction challenging. However, this is not the only border that changes its importance. There are no (clear) borders between public and private or between civilian and military legal issues [4, p. 70]. We have private companies that are more powerful than many states and that in fact set ethical and other standards for the most important communication spaces. As for the military-civilian question, it is possible to launch attacks by mobile phone, so old established questions of humanitarian law like attribution of hostile acts to decide who is a combatant or designation of what is regarded as a weapon take on a different meaning.

For the specific sphere of communications law, the distinction between transmission and content has more or less lost its meaning. For as long as telecommunications and broadcasting have existed, the distinction between point-to-point or point-to-multipoint communication has been important for regulation. Point-to-point means that the entities that communicate with one-another are known entities[3], you know who you call. This means that the state has no legitimate interest to intervene regarding the content of the communication. It is possible that the content is illegal, like when people make a phone call to plan a crime, but it would not be the telecommunications company that would be liable for this illegality. Laws and regulation primarily deal with technical aspects of the communication, its transmission. As for point-to-multipoint, this means that anyone with a certain equipment can receive the content. In such case, even in societies with freedom of expression, there are legitimate reasons for authorities to take an interest in the content. Such interest should not amount to prior control and censorship, but it can mean specific rules and monitoring regarding incitement to hatred and violence, requirements about not showing violence or pornography on television before a certain time and similar. Broadcasters often need a licence or authorisation, which establishes a certain amount of control over what goes on in the sector. Internet upturned this distinction between types of communication and consequently types of regulation: internet can be point-to-point or point-to-multipoint, a mixture of the two, multipoint-to-multipoint and maybe even something else entirely. Communications law is still grappling with how to deal with internet. If the early days of internet saw a lot of romantic notions of cyberspace being an area of cooperation and no restrictions, more recent attempts focus on how to implement at least some regulation. Internet quickly became too important to be left totally unregulated. However, to regulate something that is not only very fast-moving but that furthermore developed for some time already without many rules is indeed like trying to put a reluctant genie back into the bottle! The huge benefits that internet has brought for freedom to communicate as well as to access information – two sides of the human right of freedom of expression – should not suffer, but regulation should only deal with the negative sides.

Technology does not only pose challenges: it can also help to enforce rules and to make the world safer in different ways. For example, requirements of pro-

[3] The possibilities of group calls or of people calling numbers without knowing to whom they belong do not change the basic definition of what is a point-to-point communication, as the basic truth that the parties can be identified and are not an undetermined part of the general public still applies.

tecting data can be met with technology that more or less automatically applies requisite rules. There are many ideas of how to use technology for enforcing contracts or other types of commitments. This is what is referred to self-executing commitments or sometimes smart contracts. As artificial intelligence (AI) develops, there are likely to be more and more ways of using this in legal situations: machines "deciding" themselves and not just carrying out the exact commands of humans. It is possible to imagine that rights can be strengthened if they are "built in" to the systems, but it is natural that there are also anxieties about what will happen when decisions do not rely on discretion of human beings but rather on the very different way in which AI works. For many legal issues – those where there is a need to weigh things, like the situations mentioned above with conflict between different rights – it is difficult to imagine that AI will be able to do this. It may be one of the last situations in which the different nature of humans will be needed, with our ability to decide also in atypical situations, to take things into consideration that are not clearly delineated and so on.

There are fundamental questions of whether machines can do anything and should be allowed to do anything, which will need to be addressed, but on a more day-to-day level, there are things to do even with the kinds of AI that already exists. The European Union (EU) in its White paper on AI [5] has called on EU member states to build "ecosystems of trust". These should be based on the key principles that the EU has enumerated on responsible and trustworthy AI as well as strengthened by using systems of impact assessment of AI. Fundamental rights as well as consumer rights need to be protected. The Council of Europe has elaborated principles of AI and human rights [6]. Such measures aim to mitigate the apparent conflicts and contradictions.

The new reality

The spread of technology in society, with more and more areas in which it is deployed and has an essential role brings with it challenges for lawmakers as well as for those applying law. A big mistake would be to expect there to be clear answers to the points made above, about possible contradictions. For lawmakers, it may appear tempting to pass laws that are as complex as the technologies they seek to regulate. This is however often not the best approach – indeed, it may even be counterproductive. There are different reasons for this. First, there is a temptation when something is complicated to find an easy solution to point to, to be able to say that the issue has been dealt with – tick the appropriate box and regard the matter as closed. However, technology permeates so many levels of society and in so many different ways that it is highly unlikely that all of this can be taken into consideration in one law. What may happen is that instead of finding the one easy solution, many issues are in fact left without attention – the legislator thinks that if there is a "digital law", why worry about things anymore!

Second, having special legislation for digital issues risks creating a parallel structure – for governance, commerce or whatever it is. Laws should focus on the *content*, the *substance*; what transaction is being made, what kind of data is being dealt with and so on. The method of performing a transaction or the form in which data is held should not be a decisive issue. Of course, there are some issues that are different in the digital or cyber world, like the way to identify oneself [7]. Such issues tend to be horizontal in nature, meaning that they can be dealt with in the same way for different contexts – suitably by the same law. Thus, a special law on digital identity and signature is needed and this law – and the digital identity system – should be the same for all various contexts, whether it is a signature to submit a tax declaration or a request for planning permission, whether its is a contract between two companies, signed by company executives, or a request from a citizens to access certain data from a public body. As far as the actual laws governing these various transactions are concerned, these should be separate and relate to the transaction: the tax law, the law on planning permissions, contract law and so on. There is no need to say anything about the form of the transactions in such laws. It is enough that we know that if the law mentions a signature or a document, this can also be a digital one – following the requirements in the specific digital signature law. To sum up: make sure the sector-specific legislation is suitable but for new legislation, focus only on the horizontal issues.

This approach means that most legislation does not have to be changed even if the way of doing certain transactions changes a lot, due to technology. The legal work involved is largely that of going through existing legislation in almost any field to see if there is anything in the laws that is not possible to do or that is unclear in a digital world. This can range from simple form requirements (that a document has to be on blue paper, that a line needs to be underlined with red, etc.) to procedures that appear to require physical presence. Such provisions need to be changed. If they serve no purpose, they can perhaps be eliminated or otherwise some special digital system can be created to replicate what was special in the analogue world. This is another reason why special "digital laws" can be a bad idea, as this may mean that not enough attention is paid to such a comprehensive overview. That may mean that unclear provisions are left undetected until when some transaction is already undertaken. Rule of law includes the requirement of legal certainty. Parties to a transaction need to know what applies, so if there is a new technical way to do something, the law must be clear about what exactly is required for the transaction to be recognised in all relevant contexts, including as evidence in court if needed.

There are also other issues than those directly related to new technical ways of doing things that we can observe in our modern, high technology, digital world. In some instances, such matters may be even more significant for the legal system and rule of law than the actual new technology. One such issue is the role of private companies as *de facto* regulators of many essential things. It is difficult to find examples in history of companies having the kind of power that the internet platforms of today have. Google and Facebook make ethical rules and enforce them, deciding what kind of content that people in hundreds of countries can see or hear. They may take such tasks seriously, as can be seen by Facebook's new ideas on an ethical panel, but the fact remains that they do so because they feel an interest in doing it and not because they can be forced to. Today, the companies show willingness to comply with calls on them by authorities and politicians in different countries and they also respond to customer anxieties and demands. They do this because they feel it is useful for them (and perhaps because it meets the ethical principles of the owners and executives), rather than because any democratically elected authority can compel them to do so. Internet platforms keep increasing the impact they can have in many different aspects of life, so this situation where key decisions are taken outside of the power of the legislative or executive authorities of states will be even more directly felt in different circumstances.

The fact that something is different does not have to mean that it is worse. Perhaps private companies will be more responsive to what people want than political systems, which face challenges of reduced interest in politics by citizens, feelings of alienation that lead to election of irresponsible populists and so on. Through ideas of "multistakeholderism" – decision-making by organs composed of governments, companies, civil society, academia, normally on an international level – it may be possible to achieve rules that are suitable to daily reality, closer to the people, flexible and through all this more likely to be implemented than regular legislation [8]. The way that internet permits to ignore traditional borders means that different actors may be able to have a say about rules, instead of the traditional structure with a legislator, executive, judiciary and civil society and business all with their own specific roles. Multistakeholderism can be more or less complex and is usually not hierarchical, using a hybrid range of techniques for making and enforcing rules [9]. However, positive or not, the fact that the rulemaking as well as rule-implementation is different needs to be understood. Until now, the debate on law and technology has not paid very much attention to this aspect as a fundamental shift but rather focuses on isolated questions of just how much attention Facebook pays to requests made by the US Congress or the EU Commission for example – thus implicitly still presuming that these organs actually have power over Facebook. [10; 11, p. 286–287]

Estonian e-governance

In order to move be more concrete regarding considerations of whether technology is a threat to rule of law or how it may instead support implementation of rights, we shall briefly look at the Estonian e-governance system. This is a public system, a system of governance, which does not change the dynamic of what the formal roles are of authorities or of citizens [12, p. 201–203]. However, by giving citizens a complete and accessible overview over what data the authorities hold on them, how it is used, and by furthermore allowing people to decide when and where they perform administrative tasks, the Estonian e-governance system does show what may well be the future of governance: a citizen centred state.

Estonia is a world leader in e-governance[4]. This status of being the leader used to be largely due to the fact that Estonia was earlier than others in implementing technical solutions of different kinds – for example, the government went paperless in the year 2000, doing transactions immediately on-line, with ministers bringing their own computers and accessing all data electronically. Later, other countries have in some respects caught up with Estonia and there are now many different electronic governance solutions around the world, some which are more modern than what Estonia uses. It is however still possible to speak about Estonia as a world leader, partly as there are still solutions that are (almost) only used in Estonia (like being able to vote online in all forms of elections) [13; 14], partly as the Estonian e-governance is actually used to a very large extent. The digital way really is *the* way Estonian people communicate with authorities as well as perform many private transactions. On any given year, Estonians make almost as many digital signatures as the whole of the rest of the EU together.

[4] The terms "e-governance" and "e-government" are often used interchangeably. E-governance is broader, as it includes not just government. There is no generally accepted definition of the term, even if some national legislations or other instruments may include definitions. Normally, it means using information and communication technologies (ICT) to support administration in different ways – from accessing information to making different transactions on-line.

How come a small country, that only in 1991 became independent again after the Soviet period could achieve this status of a world leader? That is a question Estonians are often asked and there is not one unique answer. It was a lucky chance that there were the right people in the right places at the right time, who made the most of the fact that there was nothing to lose. Once this attitude had been adopted, thought was put into how to make the most of the fact that there were no legacy administrative solutions, neither in the form of technology, nor working methods, that prevented experimenting with new things. At the same time, efforts were made to get people to adopt the new solutions. This was done in different ways. One important factor was the close cooperation between the public and private sector, which meant that the digital identification system – a crucial backbone of any e-governance – was developed as a public-private-partnership between the (private) banks and the government, with each side agreeing to accept the same identification and signature system. In practice, this meant that at first people accessed also public services with their bank identity, developed by the private banks but accepted also by the public sector. Gradually, as most people got the ID-card with the digital signature possibility linked to it, people started using this – public – ID [15] also for banking transactions. Not only is it efficient from a technology viewpoint to pool resources to develop and maintain a secure identity but having one multi-purpose identity also helps to make people familiar with it and more comfortable using it. This is essential, not only as a service to be nice to people and make their life easier (which of course is a nice aim in itself!) but also as there is often a vicious circle when it comes to developing e-services: few people use them as they find it complicated – this means that there is less interest in developing new service as so few people use them – this means that few people bother to find out how to use the services as there are only so few – and so on.

Another way, in addition to facilitating the use of one universal digital identity, that Estonia showed concern for the actual possibility for people to use digital governance solutions was a legal provision that still exists but now gets little attention in Estonia: namely a provision that there must be free access to internet for all residents, meaning a computer with free-of-charge internet access in different locations, wherever people live, both in villages and in towns. The provision is found in the Public libraries act [16], and that is also where such computers are normally found: in the library. The provision is still there but as most Estonians now have other means of accessing internet, it is less relevant. The provision reflects regard for the fact that in the 1990s, when e-governance in Estonia was developed, very many people lacked the means to get their own internet access, at their own cost. Nevertheless, the state wanted to show that this new way to govern and administer the country was not just something for an elite in the cities, but something everyone should be able to profit from. Such a measure – even if nowadays more symbolic – can still have an important signal effect, for showing concern for inclusiveness of governance.

These mentioned factors illustrate one of the core aspects of e-governance: interactivity – the way to actually "do something" on-line and not just access public information. The other important component of e-governance is interoperability – that databases and authorities can communicate seamlessly. This is something enabled by technology in ways which are not possible with traditional paper-based data. It is technically possible for anyone who needs to access certain information to do so directly from one source, without the need to somehow send information between authorities or other organs. If such a system is well designed, it can support not only greater efficiency (as it considerably reduces time of transactions) but also greater security, as data is accessed from one place, directly, with no additional needs to transfer it between people and institutions. Each such transfer – regardless of whether by sending data electronically, on paper, giving information over the telephone or in person – means that there is a risk it may get somehow corrupted, altered, not updated and so on. These risks are reduced or eliminated totally if everyone who has a legitimate right to have access to the data in question can get this access from the original database. It is prohibited in Estonia to make a database with data that already exists in another database – the "once only" principle actually works [17]. Technically, such a system is possible thanks to technology that allows databases to communicate, that allows different organisations to access databases. This idea is what is called X-road in Estonia. The name was given to illustrate that the system means creating a connection between databases (a road – although nowadays more often illustrated as a cloud) and not a gigantic, centralised database.

An important term in the description of the X-road above is that the access to data is given to those who have a *legitimate* right to access it. The technology should not mean that more people can access personal data. In fact, as the data access can be made more specific, it is possible to reduce the number of persons with access. There are no "ministry computers" or similar, where anyone who gets access to the device can access certain data, but any data access is based on the person identifying him- or herself before they get to the data. The identification is made with the same digital identity that is used by citizens to perform public services, as various levels of access can be linked to the card. Ordinary citizens can only see data about themselves, while persons working in authorities may after they have identified themselves also access personal data of others – if there is a legitimate need for them to do so, based on their work tasks and the fundamental rules of data protection. Personal data should be used for a specific purpose and in proportion to that purpose. Who gets what access is set out in agreements between those authorities who have data and those who need to use it, so called service level agreements. These are specific, meaning that the access is given to individuals, based on their work positions, and not by giving the same access to anyone in an organisation. Private companies can also join the X-road system and through this get for example information about addresses of their clients or other relevant information. However, it is important to recall that according to data protection rules, access to personal data by private organisations is given almost only based on consent of the data subject. Thus, private firms cannot get access to personal data through any "back door" via X-road, but this is just a technical tool to facilitate the access if the data subjects' consent to their data being used [18].

One of the very important elements of the X-road system that helps to protect rights is that every access of personal data leaves a "footprint" – it can be seen who it was who at a certain moment accessed a certain amount of personal data [19, p. 77–80]. As mentioned, all data access has to be preceded by identification of the person who is doing the accessing so it is possible to see not just which authority but even which individual who did this. Individuals can easily see on-line[5] if and when their data has been used. Authorities must always be prepared to answer what the purpose of the data use was. Within the authority, it is possible to see which individual it was who looked at the data, so it is pretty much impossible that people out of carelessness or curiosity access personal data without a proper reason. This is a very practical way to use technology to support a principle of rule of law and good governance.

Concluding remarks

Technology has become an integral part of most aspects of our everyday life. Most probably, there will be more and more uses of technology that are not even invented yet, that may affect different aspects of our lives. This has consequences for the legal system, with new questions of liability when a complex machine, perhaps including artificial intelligence, performs various functions, and with different considerations for communication when electronic channels are used for public services. Technology is not good or bad – it depends on how it is used. In this article we have not discussed the many different practical legal questions that arise, but instead focused on the more fundamental question of whether technology affects basic ethical and legal principles, including protection of human rights and fundamental freedoms. In response to the question of whether there is an influence or not, it can clearly be stated that technology indeed does affect the legal situation at all levels: from the fundamental to the mundane. When we look at what these effects are and whether they are positive or negative the picture is less clear. We see again how it is the way technology is used that is decisive. This may appear to indicate that technology use should be clearly regulated, to ensure that the use and its consequences are positive. However, in a fast-moving reality, trying to spell out rules for how something should be done is not easy: the rules may become obsolete quickly, be easy to bypass or act as obstacles to development and innovation.

So how to deal with the question of human rights perspectives of law and technology? First, it can be admitted that this article raises more questions than it answers. This is not by accident, but because one of the ways to deal with the complex and ever-changing issues is to discuss them, involving people from different backgrounds. Many of the changes to society that need to be reflected also by changes to the legal system have to do with organisational matters, the changing role of different actors, the elimination of borders in different context and so on – not so much with the actual technology. New and more flexible means of rulemaking can be an important step to realistic regulation. Sometimes technology itself can be used to implement rights, like by making transparency automatic or access to information realistic. For sure, we do not need to be afraid of technology as something that only presents risks.

In order to move from the fundamental and principled level to a more practical one, showing how technology can support goals of good governance and implementation of rights, we looked at the e-governance system of Estonia. This is one of the most advanced such systems in the world and it uses means by which good aims of transparency for example are directly supported by the technical solutions. It cannot solve all questions, not has it basically altered the traditional structure of the state, but it has meant that a citizen-centric government is practically possible. As one young Estonian, not herself involved neither in the governmental, nor in the technology sphere, so clearly put it: the Estonian e-governance system shows that government works for the people and not the other way around – it is not people who need to go to a time and place that suit the authorities, but the authorities come to you, at a time and place that suits you.

[5] At the same portal where it is possible to see all data the public sector holds on individuals plus access various services (www.eesti.ee).

References

1. 1865 England locomotive act [Internet; cited 2020 March 2]. Available from: https://archive.org/stream/statutesunitedk30britgoog#page/n246/mode/2up.

2. The case C-131/12 Google Spain SL, Google Inc v. Agencia Española de Protección de Datos (Mario Costeja González) [Internet; cited 2020 March 2]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

3. 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 (General data protection regulation) [Internet; cited 2020 March 2]. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

4. Nyman Metcalf K. The role of research for secure digitalisation. In: Holm C., editor. *Secure digitalisation. Nordic yearbook of law and informatics 2016–2018*. Stockholm: Poseidon; 2019. p. 65–76.

5. White paper on artificial intelligence – a European approach to excellence and trust [Internet; cited 2020 March 2]. Available from: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

6. Unboxing artificial intelligence: 10 steps to protect human rights [Internet; cited 2020 March 2]. Available from: https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights.

7. Wang M. The impact of information technology development on the legal concept – a particular examination on the legal concept of signatures. *International Journal of Law and Information Technology*. 2016;15(3):253–274.

8. Like the freedom online coalition [Internet; cited 2020 March 2]. Available from: https://www.freedomonlinecoalition.com.

9. Morgan B, Yeung K. *An introduction to law and regulation*. Cambridge: Cambridge University Press*;* 2007. p. 320–321.

10. Duvivier K. K. E-legislating. *Oregon Law Review.* 2013;92(9):10–76.

11. Dutt P, Kerikmäe T. Concepts and problems associated with democracy. In: Kerikmäe T. *Regulating etechnologies in the European Union.* Berlin: Springer; 2014. p. 285–324.

12. Hood CC, Margetts HZ. *The tools of government in the digital age.* Basingstoke: Palgrave Macmillan; 2007. 232 p.

13. Voting methods in Estonia [Internet; cited 2020 March 2]. Available from: http://www.vvk.ee/voting-methods-in-estonia/engindex/.

14. Madise Ü, Vinkel P. Internet voting in Estonia: from constitutional debate to evaluation of experience over six elections. In: Kerikmäe T, editor. *Regulating technologies in the European Union*. Heidelberg: Springer; 2014. p. 53–72.

15. Electronic ID-cards in Estonia [Internet; cited 2020 March 2]. Available from: https://e-estonia.com/component/electronic-id-card.

16. Public libraries act [Internet; cited 2020 March 2]. Available from: https://www.riigiteataja.ee/en/eli/525062014001/consolide.

17. Public information act [Internet; cited 2020 March 2]. Available from: https://www.riigiteataja.ee/en/eli/514112013001/consolide.

18. Nyman Metcalf K. Drafting e-governance: a new reality for legislative drafting. *International Journal of Legislative Drafting and Law Reform*. 2017;5(1):39–51.

19. Rull A, Täks E, Norta A. Towards software-agent enhanced privacy protection: In T Kerikmäe, editor. *Regulating etechnologies in the European union*. Heidelberg: Springer; 2014. p. 73–94.

Received by editorial board 30.03.2020.