European Review of Digital Administration & Law – Erdal
2022, Volume 3, Issue 1, pp. 73-82
ISSN 2724-5969 – ISBN 979-12-218-0078-4 DOI 10.53136/9791221800784 06

*e-Governance and Good Administration: Examples from Estonia**

Katrin Nyman Metcalf
(Adjunct Professor of Communications Law at TalTech Law School, School of Business and Governance, Tallinn University of Technology and Senior Legal Expert at the Estonian e-Governance Academy eGA)

ABSTRACT The notion of good administration includes many different issues, both related to how the work of public officials is organised and how users of public services perceive these services. Technology supports a good administration in different ways and can help to protect rights of individuals, like better data protection, better access to services and so on. However, there are also challenges and it is important to take a total look on what e-governance means and how it should be designed. The article uses examples from Estonia, which has one of the most advanced e-governance systems in the world, to illustrate the key connecting points between e-governance and good administration. Estonia has a comprehensive interoperability system that enables the once-only principle and efficient administration. It is however essential that the increased technical possibilities to access data are not automatically translated into practical possibilities of data access, as any access needs a basis in law and must be proportional. The Estonian e-governance system uses technology to guarantee protection of rights and ensure a legal basis for data access. There are also legal tools to deal with other challenges, like access to services.

1. *Introduction*

Development of technology has affected the way public services are offered probably since carving in stone was replaced by clay tablets. The changes have been more rapid with a rapid development of technology during the past several decades, but in addition to this, what more recent technological developments have entailed is in many instances not just a possibility to do the same thing in a different way, but to actually do different things – a transformative effect of technology.[1] In the discussions about reforms of public administrations that are taking place in the 21st century, the extent and meaning of such transformation occupy a central place. It follows logically that the more transformative a technology use is, the more likely it is to raise questions that are quite unrelated to the technology as such – questions of good administration in a broad sense. In addition to having to understand whether and how people relate to the ways in which public services are offered and whether they have the physical possibility of accessing them, there may be ethical aspects linked to technology replacing the discretion of decision-makers, entirely new perceptions of administration, and so on.

The benefits of e-governance are often presented primarily as faster and more efficient administration. This already demonstrates how e-governance can benefit good administration, the definition of which tends to include many different issues, with speed and efficiency being among them.[2] At times these benefits are however set against risks for data protection or of increased divisions in society, with a need to weigh any potential benefits against risks that are presumed to be able to nullify the benefits. Is it worth sacrificing some data protection or inclusiveness in order to offer a faster and more professional service? However, such a question is based on a misconception: there is no need to make such choices if e-governance is properly planned. By having a transformative approach, technology can in fact provide many benefits for public administration, including better protection of data and easier access for all. Such benefits need to be properly integrated in the planning of e-governance, which cannot be a purely technical matter. Legal and social questions

* Article submitted to double blind peer review.

[1] "Noting that e-governance is about democratic governance and not about purely technical issues, and convinced therefore that the full potential of e-governance will be harnessed only if ICTs are introduced alongside changes in the structures, processes and ways that the work of public authorities is organised", see Council of Europe, Committee of Ministers, *Recommendation Rec(2004)15 of the Committee of Ministers to member states on electronic governance ("e-governance") and explanatory memorandum,* Strasbourg, 2004, Preamble. Available at www.coe.int.

[2] C.C. Hood and H. Z. Margetts, *The Tools of Government in the Digital Age*, London, Palgrave Macmillan, 2007, 207.

need to be integrated in the process of introducing or increasing e-governance or generally digitalising society. This should not mean that a lot of specific legislation is introduced for digital matters, but the challenge for regulators and legislators is to determine if, how and when, new and specific legal rules are needed for the new way to conduct administration. If it is just a question of doing things with new tools, existing laws will normally be sufficient as long as the key elements of digital identification and signature as well as data protection are properly addressed.[3]

This article does not deal with the aspect of use of technology to strengthen democratic processes. This is a very interesting topic that is rightly the subject of much practical and academic interest, that ranges from how technology can be physically used to support elections for example – something that became extra relevant during the Covid-19 pandemic and the restrictions on movement that this entailed –, to opportunities for more direct democracy, lobbying by a wider range of groups and of course the very question of access to trustworthy news and political information. Many of the general features mentioned in the article have a bearing also on the question of citizen participation and thus on democracy in the broad sense, but apart from this, so called e-democracy will not be specifically addressed.

In this article, examples from Estonia will be used to illustrate what e-governance means and what the potential benefits for good administration may be – while not forgetting to highlight possible risks. Estonia is one of the countries in the world with the most advanced e-governance.[4] This is based on such matters as a universal digital identity with a much used digital signature attached to it, as well as a system of interoperability of databases, which permits the seamless provision of public services from what to citizens appears as one (virtual) location. Estonia used to be known for being the first country in the world with many digital solutions – the government went paperless in 2000 and the valid form of legislation is the digital form since 2002 to mention some examples – but today, what sets Estonian e-governance apart from other countries is rather the fact that it is very comprehensive as well as used to a great extent. In this article, the Estonian examples serve as examples to illustrate the discussion rather than study-objects for a deep analysis per se. The aim of the article is to offer a perspective on what e-governance means for good administration and how to ensure the maximum positive impact with the minimum of risks.

2. *Terminology and setting the scene*

The terms e-governance and e-government are often used interchangeably, even if they do not mean exactly the same thing. E-governance is broader as it encompasses not just public governance. Neither of the terms have any authoritative, single interpretation, set out in a generally accepted convention or similar. At the same time, usually neither the slightly different understanding of the terms, nor the difference in which words that are employed, leads to practical difficulties, as the contexts will provide the necessary interpretation. Actually, it may even be beneficial that there is no very specific definition, as e-governance should be something that touches upon most areas of governance and administration, in a manner which evolves with time and place.[5]

The absence of a clear definition, however, means that different ranking tables for the status of e-governance around the world are not always very relevant, as the comparisons may include things that are not valid everywhere or that have lost their relevance with time. In some comparisons, for example,

[3] K. Nyman Metcalf, *E-governance in law and by law*, in T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*, Heidelberg, Springer, 2014, 37.

[4] Comprehensive information on what the Estonian e-governance consist of and how it works is found on https://e-estonia.com.

[5] The Council of Europe in *Recommendation Rec(2004)15* refers to Electronic Governance or e-governance without a definition, but with an understanding that the term is self-explanatory. The World Bank links the benefits of e-governance to the definition: "E-Government refers to the use by government agencies of information technologies […] that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions". See The World Bank's brief at https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government.

the ability to upload signed Pdf files was included, whereas in an advanced e-governance system (like Estonia) this was never necessary, as it was possible to sign directly online regardless of file format. One element which is often included in e-governance rankings is the access to internet. On the one hand, in countries that have e-services, this is hugely important, as without internet there will be no point to have electronic, on-line services. On the other hand, if a country has excellent internet access but does not offer online services, it does not mean that there is advanced e-governance. This is the case in many rich and developed countries (like not least the USA, which has very limited e-governance). The existence of good internet access is clearly very relevant to measure the state of digitalisation of a society broadly, but e-governance presupposes that technology is used for the benefit of governance – not just that the technical potential for doing so exists.

The position of one or other state in rankings may appear to be irrelevant other than as a PR tool for diplomats and those seeking foreign investments, but the reason for this brief discussion about such rankings and how they are made is to point to the multifaceted nature of the phenomenon of e-governance. This is pertinent if we wish to understand whether or not it is good for administration. There has been a tendency in the past few decades, increasing across various disciplines when digital technologies become more ubiquitous, to measure most things quantitatively. Indeed, the word “digital” has brought with it a tendency to reduce everything to digits. Even if it is relevant to have criteria for comparison and benchmarks for progress, something as complex as e-governance is a good example of why it is nevertheless necessary to ensure also qualitative evaluations and narratives to explain progress or problems. It is not possible to determine in a relevant manner that a certain percentage of people became so many percent less corrupt because of a specific measure, or that so many people of a certain age are happier since a service became available in a new manner. Statistics support analysis but should not replace it. The evaluation of what is “good” remains a soft value, a subjective point that may be supported by, but cannot be replaced by, quantitatively measurable criteria.

Although there is as mentioned no unified definition of e-governance, the features of interactivity and interoperability can be used to describe key elements that sets e-governance apart from just basic use of information and communication technology (ICT). Such basic uses include presenting public information on-line or providing downloadable forms. These may be important first steps, but are not enough to merit being called e-governance. Interactivity means that it is possible to complete transactions on-line; to declare or demand something or access data that is not public. To enable this, a digital identity is necessary and it is indeed not possible to go beyond a certain point in e-governance without a digital identity that is at least as secure as a traditional one. Interoperability means that databases can communicate with one-another, which makes it possible to access information from one location and which enables the once-only principle, in that once certain information exists in the system, everyone who needs this information will be able to access it and people do not have to provide the same information more than once. Interoperability is also the tool that permits transformative speed of administrative transactions.

3. *Interactivity and interoperability*

When considering interactivity and interoperability from a legal perspective and more particularly from a human rights viewpoint, several issues come to mind. Concerns for data protection[6] appear legitimate, but also questions of access to public services as this requires additional elements, not present for traditional services, namely an access to internet (and the knowledge of how to use it) and a digital identity. While it is correct that these questions should arise in the minds of those who deal with reforms to introduce or enhance e-governance, if the matters are properly addressed, there are no obstacles to the digital

[6] The best known instrument in this context is the 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 (GDPR), in force since May 2018, that has attracted global attention. It is not necessary for the purposes of this article to discuss the instrument in any detail, as so much literature exists and as it is sufficient for our purposes to note the existence of a data protection framework.

way of performing governance. One of the key suggestions to mitigate risks for data protection is the simple albeit essential advice to make sure that the question of who should have access to data is always addressed separately from the question of what access the technology enables. This will be further explained below. As for the access to services, improving access to internet on reasonable conditions and, perhaps, adding specific access possibilities for disadvantaged groups as well as development of a secure digital identity, are questions that need to be addressed together or in parallel with the establishment of interoperability and on-line services.

Let us start with a few words about digital identities and signatures. As these topics are not very new, but various examples exist worldwide, it is generally by now understood that such identities and signatures may indeed normally be more secure than traditional ones.[7] On the one hand, we all know that it is easy to copy a handwritten signature and relatively easy to pretend to be someone else of about the same age and general appearance. The way to abuse a digital identity and signature is different, with a certain mastery of technology and additional effort being necessary. On the other hand, such pretence can be made from the other side of the world, which of course vastly enlarges the potential circle of imposters. Thus, we are faced with features that per se can both better ensure identification or make it more vulnerable. In addition to this, we also need to keep in mind that the traditional legal system was well aware of the mentioned ways it was relatively easy to fake or assume identities in the traditional system, which is why we have measures such as the need to have witnesses to a signature, to be present in person with a photo ID, to do certain transactions in front of a notary or similar. In the digital system, there is a need to determine which of such means that are still relevant and, in that case, how to move them to the digital world. It should not be ignored that in some cases the result of the consideration may be that some transactions are not suitable for the digital environment – not because it would be impossible to create technological solutions, but because there are reasons to add an extra layer of security in the shape of requirements that need extra time and effort, to allow also for reflection. When Estonians present the Estonian e-governance system, it is often said in a joking manner (although it is true) that almost the only transaction you cannot do digitally in Estonia is to get married! This is not because there is some inherent feature of marriage that it would be impossible to do on-line in a country where everyone possesses a digital identity and a means to sign digitally. The reasons for requiring personal presence may of course be described as the traditional importance of the act and other "soft" reasons, but if we like, we can also explain it more pragmatically by pointing to the enforced extra time for reflection that results from having to go to a specific location and interact directly with an official. For some acts, it may be better to have to think twice, even if technology itself does not require this! This is the first of many examples that we will see in this article of non-technical considerations that need to be an integral part of creating essentially technical systems.

This article will not elaborate on different forms of digital identities or the various necessary features for their security, such as certification organisations. It is known that there are different available technological means to make secure identities and signatures and no doubt new ways will be developed. From a legal side, the area of digital identities and signatures is one in which the principle of technological neutrality of legislation has to be somewhat qualified in order to secure an important principle of a rule of law society, namely legal certainty. Theoretically, it would be possible to allow people to use various kinds of digital identities according to their preference, but as identifying oneself is such a key feature of most transactions in society, it has to be clear which identity system will be recognised in all contexts, including as evidence in court. The need to verify a signature may arise decades after it was given, in a completely different location and context. It must be possible to know that the way a transaction was performed was in accordance with law. This said, to put excessive technical detail in the law may cause problems as it would lock in the exact technical situation at a given moment in a manner that makes any

[7] Some years old, but still relevant, is M. Wang, *The Impact of Information Technology Development on the Legal Concept – A Particular Examination on the Legal concept of 'Signatures'*, in *International Journal of Law and Information Technology*, vol. 15, issue 3, 2006, 253.

technical development impossible. This can be solved by having details in regulations, decisions or other secondary legal acts, that can be amended more easily than laws, while establishing the outlines as well as the system of verification in the law.

A common obstacle to functioning e-governance is that the digital identification system is too complex and thus the uptake of it is limited. There will always be people who are enthusiastic about new technologies and make efforts to get anything new, but these people tend to be the minority in society as a whole and, furthermore, unevenly distributed among different populations groups. If the digital identity is automatically given to everyone, it is much more likely that a broader range of people will use it. In Estonia, we do not have the same difference between age groups regarding the use of electronic services. One reason is to be found in that our e-governance is already about 25 years old and thus people who were in their prime working age when many solutions came are now elderly, but it is also important that the digital identity is automatic and, as services are generally user-friendly, it is more likely that people familiarise themselves with this new way of doing things. It is not compulsory to use the digital identity, but it is automatically given to everyone and the possibility to sign is linked with the same ID-card that can be used for travelling in the EU, for identifying oneself physically, as a shop loyalty card and so on. Thus, there is no extra action needed from citizens to get the possibility to use digital identity and signature.

To achieve benefits for good administration it is essential to get away from the tendency to use new technologies to do the same thing slightly differently, instead of embracing the transformative potential of the technology. Maybe the days when people used computers only as somewhat more comfortable typewriters are quite long passed, but when it comes to data handling, we see similar tendencies. Interoperability can eliminate the need to ask someone for data and reduce the need to update databases to the minimum, but a fully interoperable system remains the exception several decades after the technology started to be used in Estonia. What an interoperable system means is that different organisations and authorities can use databases regardless of where these are located, meaning that you use the database you need for your work directly from your workstation, even if it is held by a different organisation. There is no need to ask for data to be transferred, thus eliminating risks of data leakage, as well as the risk that different people working with the same data have different versions of it. It has been mentioned above that the technical possibilities to access data and the legal possibilities to do so are different things, so the system does not provide more data access – quite the contrary. It is namely essential that questions of how the access is legally given and how it practically takes place are integrated in the design of the system. The Estonian interoperability system is called the X-road – a name given to illustrate the connection between databases, avoiding any centralisation of data. The way the need to look separately at technical possibilities and legal possibilities for data access is handled is that any data access requires that persons identify themselves. It is only when the system determines who it is who attempts to access data that this becomes accessible to the extent intended. Such intentions are set out in agreements between the organisation that possesses the database and the one that needs to (and has a basis in law to) use the data. The agreements are specific and do not give access to organisations, but to individuals – there are no "ministry computers", but regardless of device, it is through identification that access is provided. As an extra guarantee, the access leaves a "footprint", showing who accessed which data and when. Individuals can see on their pages – in the one on-line location for all public services and data[8] – which authority accessed the data, but within the authority, it is also visible who it was.[9] Thus, in essence, the need to have a purpose and proportionality for data use is built into the system.

4. *Legal obstacles?*

When working in different countries on e-governance matters, it is not unusual to hear the argument that there are legal obstacles to e-governance in general or to specific e-services. It is possible to meet this with the statement that there is no such thing as legal

[8] In this regard, see www.eesti.ee/et.

[9] A. Rull, E. Täks and A. Norta, *Towards Software-Agent Enhanced Privacy Protection*, in T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*, Heidelberg, Springer, 2014, 77.

obstacles to e-governance! This is a statement that is on purpose somewhat provocative. Evidently, like with most legal questions, the issue depends on exactly what you mean by the question or statement. Most lawyers work with application of existing laws in specific jurisdictions, to concrete circumstances at a given point in time. In such a case, there may be various legal obstacles to doing things in a new format, whether that is the digital format or some other new way of doing things. However, the process of introducing e-governance in a country or increasing the situations in which it can be used is a process of reform and should include also legal reform. It is only in recent years that it has fortunately become more common to take a comprehensive look on what e-governance means for society and thus include a wide range of persons in the teams working on related reforms. It was until recently not unusual that the process of digitalising society was led by technical specialists and thus to a large extent shaped almost exclusively by technology. This was a way in which legal obstacles could easily be created; if a technical solution was more or less completed and up-and-running, before any attention was paid to whether it was in compliance with legal requirements, what could have been dealt with through a minor adjustment to law and procedure became a serious obstacle to the validity of transactions.

Such situations are best explained by giving some examples of what kind of obstacles may arise, illustrating how this normally means quite simple and straight-forward matters, rather than legal intricacies. If a law speaks about delivering one original and so many copies, in a world of electronic data, such a requirement normally makes no sense. The law may state that certain decisions should be issued on grey paper or that an application shall be signed in blue ink – or indeed, that applications can be made during office hours. Such form requirements are common in legislation around the world and can exist in various types of laws: in procedural codes, in general administrative acts, in sector-specific legislation or in regulations, decrees and decisions issued at different levels of an administration. Some such requirements may be ignored in practice, if it is evident that they play no role in a digital administration, but there is always a risk to legal certainty if provisions exist on paper but are differently applied in practice. Thus, there is work for lawyers in relation to e-governance, but this work does not consist mainly of drafting specific laws or other rules on all matters digital, but instead of analysing existing legislation, "vacuuming" the laws for any language that does not fit with a digital world.[10] When such provisions are found, there are different options regarding what should be done. The first question to ask should however always be: what purpose is served by the requirement?

Form requirements may well have a purpose in that the format represents a specific value: we will know that a grey paper decision is different from other decisions, or we will know that from the moment someone applied for something, they need a response within so many hours, so we need to be able to determine that applications are made so that there is sufficient time for officials to deal with them. However, there are also many form requirements that exist mainly due to tradition and perhaps never fulfilled a specific, necessary role or otherwise that role has very clearly disappeared (like the need to sign with a special ink, which may have been needed to be visible on photocopies). It is only when the purpose of a requirement is understood that the next step should be taken: should such a requirement be somehow replicated in the digital world? If the answer is yes, this is an example of the need for cooperation between law and technology: technical people need to be given the task to create something that serves the same purpose in the new environment. If on the other hand it is clear that the requirements are not needed, they should be eliminated from law. This is not a technical question and needs to be addressed by people with different expertise and roles. The introduction or increase of e-governance is a good opportunity to get rid of unnecessary requirements and consequently a simplification of law becomes a useful "by-product" of the process. Legal changes as well as the need for any new, specifically "digital" laws need to be carefully considered, as there should not be too much legislation that focuses on the form of transactions.[11] For all

[10] K. Nyman Metcalf, *How to build e-governance in a digital society: the case of Estonia*, in *Revista Catalana de Dret Public*, issue 58, 2019, 1.

[11] R. H. Weber, *A Legal Lens into Internet Governance*, in L. DeNardis, D. Cogburn, N. Levinson and F. Musiani (eds.), *Researching Internet Governance –*

its advanced e-governance, Estonia does not have any specific "e-governance" or digital legislation. Instead, the focus is on the word "governance", electronic is just the means and not the end.[12]

As access to internet is needed to use electronic services, the availability of good and inexpensive access has also meant that most people have a real possibility to try electronic channels. In this context, the legal provision that there must be computers with free internet access available to the population all over the country is important. This was introduced into the Public Information Act and Public Libraries Act in 2000 and meant that Estonian public libraries were all equipped with internet-connected computers. Today the rule is less important as most people in Estonia have other ways of accessing internet; in addition to most people having some form of subscription, there are many free wi-fi spots in the country, but the psychological importance of the rule must also not be underestimated, as it indicated that the novel ideas about governance were not just of interest for a small elite in the capital. For this reason alone, such ideas could be considered in countries that come to widespread e-governance later, especially if the socio-economic conditions of the country are diverse. The public computers are still used and not infrequently for use of public services (although there is no rule that restricts them only to that purpose) by those who very infrequently need to use a service, as the people then also often ask for help from librarians.

Even if on-line services are easy to use and everyone has the necessary identity and access to internet to use them, a good e-governance system does not mean abolishing any possibility of a personal service from a human being. This does not mean that it is necessary to retain a paper-based service, but it should be possible to go to an office and deal with administrative matters, which in practice may mean that an official makes the computer entries or assists with it. This is essential not just for those who feel uncomfortable with using computers, but also for all those situations that may "fall between chairs" or for some reason not fit with the standard digital system. The fact that most transactions can be handled by people directly on-line means that the staff in different authorities will have more time to deal with direct contacts and specific requests. To add a personal note, this author has lived in several different countries and worked in even more and can attest to the fact that getting in touch with Estonian authorities is a lot less stressful than in most countries! Very limited hours for calling or waiting in phone queues is almost unheard of in Estonia.

5. *Challenges*

The various benefits of e-governance that contribute to good administration more than just by providing faster and cheaper public services have been outlined above. However, it must not be forgotten that there are also challenges. The use of more ICT in administration does not automatically and necessarily lead to a better administration. The new tools must be used in the most appropriate manner and specific risks related to technologies must not be overlooked. We are not here thinking primarily of data protection risks, which are perhaps the most commonly mentioned legal risks related to e-governance. As has been explained, technology can be used to protect data better than in a traditional paper-based world, so it is not correct to assume greater data protection risks just because the data is in digital format. Nevertheless, one of the reasons why data protection is so commonly brought up as a reason for hesitancy about using more e-governance is a good illustration of one of the challenges that needs to be addressed when transitioning to more technology use: namely, the perception of risks. Digital data like digital transactions and "documents" are intangible, which affects the image people have of them to a great extent. Protecting a document can be very physical, like locking a safe. Delivering an application on paper is also physical and we can see that the document in question has reached its destination, that it looks fine with signatures and stamps. Assets that we can touch are easier to relate to than those that only exist virtually.

The reason to focus on how people feel about new formats is not only an expression of

Methods, Frameworks, Futures, Cambridge, MA, London, MIT Press, 2020, 107.

[12] On adapting rather than making fundamental changes to legal rules, see K. K. Duvivier, *E-Legislating*, in *Oregon Law Review*, vol. 92, issue 9, 2013, 48; P. Dutt and T. Kerikmäe, *Concepts and Problems Associated with eDemocracy*, in T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*, Cham, Springer, 286.

a "soft" outlook, to be nice to people. If inhabitants of a country that introduces more and more e-governance do not trust the new way to do things, they will not use digital solutions and there will thus not be any gains of efficiency or lower costs, as the state will have to maintain other ways of accessing services or alternatively – but hardly likely in democratic societies – use resources to force people to use digital methods. The lack of popular uptake can lead to a vicious circle, when those who are tasked with designing and allocating resources to digital services see that very few people actually use them, so there is less interest in making services available, while those who may show some interest and investigate what kind of services could be accessed in the new manner will see that there is not much and consequently it is not very relevant to learn how to operate in the new environment.

One may argue that these statements are obsolete, as the on-line world is hardly new anymore. However, even before coming to the different perceptions of different groups in society, we may note that the online world still often copies the offline one to make its users understand what is what – from small things like deleting virtual documents by placing them in a virtual wastepaper basket to more significant symbolism. In fact, the tendency to replicate the "real world" look and feel of things is something that may slow down digitalisation in some contexts. This does not mean that it is necessarily a bad thing and this statement leads on to a very relevant aspect of challenges with digitalisation of administration: that of perceptions of different people. It is popular to refer to older people as being the group that is uncomfortable with online solutions, which to some extent is true in most countries but may also be a simplification. The avid social media users of today are not all young. Yes, it tends to be the case that younger people go along with new things quicker and indeed physically can handle devices faster, so older people will keep legacy digital solutions alive longer, but at the same time, the question of what different categories feel comfortable with is more complex than just related to age. It is essential to identify which groups in society that may feel less confident in the digital world and why – with such knowledge, the necessary tools can be designed to deal with this.[13]

One of the risks with introducing e-governance is that the process is led primarily by the technology. Indeed, we need to know what technology exists and it is the technology that needs to be able to address the issues that lawyers and public officials highlight, like the need for secure identification, the need to give access to only some of the data in a specific database, the need to differentiate between different people who may access the same website for different things, and so on. However, it is not the technology that should determine why and when someone needs to identify themselves or who shall have access to what data or which services, on what conditions. These are practical reasons for including different categories of people in the process of e-governance reforms. Among the necessary skills is also the ability to understand how different categories of people perceive contacts with authorities or different organisations. A service aimed at businesses, which will mainly be used by professionals can look very different from one which is aimed at those who rarely need to contact authorities. This is very obvious as a statement, but unfortunately much less obviously reflected in digital public services. Fortunately, the situation is improving in most countries and governments are learning from the private sector, where friendly-looking chatbots may help people or websites generally are inviting also for those who are not used to navigating electronically. For tech experts it will be counter-intuitive to not employ the most advanced technology, but for "ordinary people" being able to use something familiar will be valuable. Finding the balance is something that can only be done if different competences are included in the process.

To conclude the section on challenges, it is necessary to mention the specific digital challenges and risks that do exist. This is on purpose left to the last section, not because these risks may not be significant, but as discussions on challenges of e-governance or digitalisation more broadly tend to pay a lot of attention to these features and they are thus well discussed both in practice and in

[13] Inequality or even the perception of it serves to undermine trust, as discussed by E. Menéndez Sebastián and J. Ballina Diaz, *Digital citizenship: Fighting the Digital Divide*, in *European Review of Digital Administration & Law*, vol. 2, issue 1, 2021, 149.

academic literature. Data protection was mentioned above. In addition to risks related to careless handling of data, there are risks of external attacks to steal or modify data. Many of the tools described above, used in Estonia, serve to eliminate risks in the daily, regular data handling and the GDPR also primarily addresses such risks. For external, ill-intentioned attacks, other methods are needed. This does however not mean that the protection systems introduced for the regular data processing would not serve any role in the broader context. If risks due to carelessness, lack of proper competence and oversight or over-eager data collection without systems for evaluating purpose and proportionality can be eliminated, illegal and illegitimate data uses can be more easily spotted and resources can be directed to these unpredictable risks. These kinds of actions should serve as complements to technical means such as decryption.

Just like e-governance cannot be seen as something for specialists only but must become an integrated tool for the administration as a whole, cybersecurity needs to be an integrated feature of the modern state.[14] Risks are very real and very multifaceted. It is instructive to look at the National Cyber Security Index[15] created by the Estonian e-Governance Academy and note the various matters that are measured. Protection just by technical means is not possible, but in addition to education and proper legislation, technology needs to be used when possible, as the nature of the cyber world is such that the measures taken in one country cannot be sufficient to eliminate all risks. Intrusions into the "territory" of other states are easier and more likely than ever before. When promoting e-services, it is important to be open about the fact that risks do exist and to explain how these are dealt with, rather than hoping to create trust by playing down risks or speaking about them in terms that "ordinary people" do not understand. This said, such a situation is hardly an argument against e-governance as in that case, the risk of hostile action by enemies would be a reason not to build up a good state at all – as it may be attacked. The likelihood of an attack causing serious damage must be reduced and the measures to ensure this explained to citizens. Estonia involuntarily got the chance to become an example also in this field, as the country was the first country to be the victim of a concerted cyber attack from another country, already in 2007. The very digital nature of the society opened it up to be potentially badly affected but the way the systems had been designed meant that the damage was limited in time and scope. Furthermore, the event led to public attention to cybersecurity[16] and various initiatives like a cyber "home guard" for example. The cybersecurity area develops constantly and rapidly, with international standards supporting the activities of states when they address the challenges.[17]

6. *Concluding remarks*

When discussing good administration and e-governance, the range of matters to consider is wide. We have the practical tools needed to benefit from electronic services. The technical aspects of security of identification represent only one of the matters in need of consideration. People must be able to use the identification mechanism. As mentioned above, to enable interactivity and allow people to complete transactions on-line is a key step to a transformative e-governance, to something that really changes the way administration works. It is with such a system that we can actually say that the administration has become citizen-centric in that it is the individual citizen or resident that decides where and when to use public services and communicate with authorities, instead of the authorities demanding people to come at a

[14] R. Geiss and H. Lahmann, *Freedom and Security in Cyberspace: The Focus away from Military Responses toward Non-Forcible Countermeasures and Collective Threat-Prevention*, in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2013, 621. Also E. Caliskan and R. Peterson, *Technical Defence Methods, Tools, Techniques and Effects*, in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, Tallinn, NATO Cyber Defence Centre of Excellence, 61.

[15] See http://ncsi.ega.ee.

[16] It is almost difficult to believe now that before the 2007 attacks on Estonia, no country in the world had a cybersecurity strategy (at least not an officially known one) and that even for a military alliance such as NATO, before this date the only cybersecurity tools were directly related to protecting NATO´s own communications networks and not to protecting member states from the cyber viewpoint.

[17] T. Tropin, *Cybercrime. Setting international standards*, in E. Tikk and M. Kerttunen (eds.), *Routledge Handbook of International Cybersecurity*, London, New York, NY, Routledge, 2020, 151.

time and place that suits the authority. This positive effect will not arise unless most people feel comfortable with using the digital channels and are able to do so properly.

As digital identities with a possibility to sign digitally are automatically given in Estonia, the hurdle of having to get people to be sufficiently interested to take action to procure themselves with the identity disappear. There are many possible ways to securely identify oneself digitally and this is one of the (relatively few) areas where e-governance requires specific legislation, as it must be clear not only how to get the identity, but also that it is recognised fully, if need be also as evidence in court. Another positive example from Estonia is the system of interoperable databases that not only provides faster administration, but also has data protection elements built in.

The fact that there are challenges to building a secure and efficient as well as citizen-friendly e-governance should not mean that the process is not undertaken. The gains for good administration can be very important. Technology is not a threat – it is rarely good or bad in itself, but it depends on how it is used. We have shown positive examples of increasing many different elements of administration with e-governance tools. This article does not try to push other countries to adopt exactly Estonian solutions – actually, quite the opposite in the sense that what makes e-governance successful is that it is integrated into society and administration and not seen as a separate, parallel system of governance. This is achieved only when the solution is adapted to the country in question. At the same time, not everyone needs to re-invent the wheel. Estonian solutions are more than a quarter of a century old, with many upgrades along the way, and can thus present examples of the process, challenges, and solutions that others can learn from.