European Journal of Sustainable Development (2020), **9**, 3, 91-102 ISSN: 2239-5938
Doi: 10.14207/ejsd.2020.v9n3p91

Sustainable Digitalization in Public Institutions: Challenges for Human Rights

By Aurelija Pūraitė[1], Rūta Adamonienė[2], Audronė Žemeckė[3]

Abstract.
The modern world is bound not only by global flows of information, capital, services, and movement of goods and people but also by the wide range of opportunities to exert both positive and negative effects on these flows. Already, most of the aforementioned global flows, stationary and variable objects are protected (organized, coordinated, controlled) by digital technology and in the foreseeable future digitization will encompass the most diverse aspects and processes of existence. Access to the development, deployment, management and use of relevant digital technologies has expanded to such an extent that it has become virtually difficult and even impossible to provide timely protection against a wide range of actors, ranging from unauthorized specialized gathering to varying degrees of security. The development of information technology, which increasingly embraces various aspects of the existence of different security entities, calls for a new rethink of the philosophical - ideological, political, economic, social and cultural foundations of public security. In recent decades human rights have dominated in the discourse of legal and political systems. Now the balance between protection of human rights and public safety in the context of digitalization imposes necessity to reflect the concept of fundamental rights once again.

Keywords: Sustainable digitalization, public and private security, human rights

1. Introduction

It is not disputable, that nowadays anew era has come - economies and societies are being fundamentally transformed by digitalization, which essentially changes almost all aspects of modern lifestyle, including, but not limited by new models of business and work, public services, leisure and even democratic participation. Governments and all public sector are facing a demand to tackle the risks imposed by digitalization. Research shows that digital immersion is faster and more profound than the wider public, and even professionals internalize or even reflect upon (Franko & Gundhus 2015). Whole industries work in the field of digitalization, and digitization is generally considered positive. There is a lack of research on possible impacts and consequences of digitization on professions, professionals, and the social fabric, including public security, and on human life at large, including respect and enhancement of human rights. Digitization (digital transformation) is going faster than the reflection on its impacts on society, security, and rights; this in itself represents a potential threat to society. There is,

[1]Doctor of Social Sciences (Law), Associate Professor, Vice-Dean for Science at the Academy of Public Security, Mykolas Romeris University (Lithuania).
[2]Doctor of Social Sciences (Management), Habilitated doctor, Professor in the Departments of Humanities, the Academy of Public Security, Mykolas Romeris University (Lithuania).
[3]Doctor of Social Sciences (Law), Lecturer at the Academy of Public Security, Mykolas Romeris University (Lithuania).

therefore, an urgent need to analyse the process carefully to avoid the unforeseen, un-modelled and potentially detrimental consequences.

The use of technology has also exposed individuals to new risks to their human rights. Digitization and the development and enhancement of human rights are profoundly different regarding at least two criteria. Firstly, digitization is at its core an effectiveness-oriented product focused on immediate to short-time impact and as timely as the possible return of investments, and as such driven by the logic of quantification and monetarization; whilst orientation towards human rights is none of those. Development, enhancement and protection of human rights are costly, time-consuming, involve long-term modelling and investment, do not involve monetarization or quantification. Human rights are mostly about the expansion of the qualities of life that make life worth living, whilst digitization is about living life comfortably. Moreover, the development and enhancement of human rights and digitization are performed by a very different range of professions: human rights are at the focus of legal, education, social work professionals, philosophers, sociologists, while digitization is implemented by the IT and management professionals. Hence, there is a risk that those two processes will not always share the same understanding, rationale and priorities. Human rights abuses can be one possible effect of rapid and unchecked digitization. Interdisciplinary research has the potential to alter these negative future scenarios. Delivering public security through digitization of public institutions has already raised concerns regarding human rights in certain regions of the world. Digital nature of public institutions may also determine the levels of public trust, which is often controversial, opaque, especially due to recent trends to introduce more and more intrusive public governance and surveillance tools.

The legal, ethical and regulatory challenges in respect to digital algorithms in public governance and decision-making are already becoming a significant topic of debate across Europe (Babuta, Oswald, & Rinik 2018). However, the assessment of risks in this context is typically limited to issues of privacy, bias and accountability, and the solutions that are being proposed are equally limited to calls for transparency, accountability, ethics, oversight, fairness, and intelligibility (Ananny & Crawford 2018; Kemper & Kolkman 2018; Ferguson 2017, 2018). This research focuses on the issues of finding the balance between the protection of human rights and public security in the context of digitalization in public governmental institutions. The pervasive nature of technology creates new multidisciplinary realities for human rights research. The researched issues are interdisciplinary and require the systematic approach, therefore legal, managemental, economic aspects will be analysed. The research methods reflect this diversity of disciplinary approaches and include legal analysis, policy and document analysis, critical discourse analysis. Critical, comparative and systemic analysis of the previously conducted studies in the field, and the existing legal acts nationally and internationally will be carried out in order to construct main theoretical/conceptual constructs and frameworks regard the digitization of the public sector, development and enhancement of human rights. The focus was concentrated on understanding how the implementation of digital tools to the public sector and public services correlate with human rights and how possible harm to human rights is understood by the public sector.

2. Research Context and Literature Review

Digitalization has been a leading topic during the past decade. In 2015, the United Nations General Assembly approved the 2030 Agenda for Sustainable Development (United Nations, 2015), where, among other goals, Goal No 9 aims to "build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation", bearing in mind digital transformation in all sectors. European Digital Single Market (DSM) strategy, adopted in 2015, underlines the significant impact of digitalisation on growth and job creation within the economy (European Commission, 2015). In 2017 European Commission has launched the working document "Digital4Development: mainstreaming digital technologies and services into EU Development Policy" (European Commission 2017), in which admitted, that digital technologies and services enable sustainable development and inclusive growth. Digital technologies should be deployed at all levels of activity in both the private and public sectors, but to this end, the promotion of accessibility and secure broadband and digital access should be the key EU objectives; among other necessary measures, it is particularly important to develop the appropriate infrastructure, as well as to increase the digital literacy and skills of all sections of society; to promote the use of digital technologies as a factor in sustainable development. Digitalization has not only been instrumental in implementing these goals, but it presented itself as the very solution to these increased pressures while promising efficiency and knowledge-based and intelligence-led data-driven policing (Fyfe, Gundhus, & Rønn 2018).

It is clear, that digitalization imposes challenges on national governments first of all, as well as on the EU level institutions. Some mainstreamed challenges to be addressed are infrastructure and networks, creativity and cultural diversity in the digital environment, policy harmonisation, aiming to create the appropriate frameworks with independent national regulators, ethics and human rights protection in a diverse environment of digital reality. The role of government support is crucial for digital perspectives of a particular state. Though at the household level the digital transformations are unprecedented (as surveys indicate, there are more households in developing countries that own a mobile phone compared to having access to electricity or clean water (International Telecommunications Union 2016), access to information and communication technologies is still not available to 3.9 billion people. On the second had, on the public sector level the transformation is not as rapid as it could be expected, the public sector has deep cultural, legacy and bureaucratic habits, and the most difficult to replace is the mentality, which makes it complex to succeed with digital transformation projects. Speaking about public section the European Union, it is important to mention, that digitalization here is not only an option but recently it is being seen as both a necessity and a possibility to improve public service. Most of the Member States have developed digital strategies which contain high ambitions for modernising, simplifying and improving the public sector. However, there is a risk of those policies being only declarative instead of being a tool of good administration. The public sector needs to transform into a future digitized state, and the goal of the digitalization is to deliver better outcomes getting more from less and making resources more productive (Ruud 2017).

The research shows, that the transformation in the public sector organizations only superficially may seem to be about technologies and finances. When processes of public administration and public services are digitized, models to describe procedural knowledge are needed, and such models consist of algorithms, work processes and capacities of public authorities (Gray and Rumpe 2015). With no doubt, public sector depends on state financing policies and mechanisms, political will and even demands from the citizenry, but the main factors determining ability to make changes in management and workstyle are people and their competences, processes and inner procedures, organizational structure and leadership (Sundberg 2019; Söderström 2019; Reascos, Carvalho, and Bossano 2019). As analysed by Ruud, in a survey from 2015 two out of three top managers in public sector stated that lack of digital competence is a barrier to succeeding with digitalization (Ruud 2017). According to Berman, Korsten, and Marshall (2016), for traditional public sector organizations, digital reinvention involves a fundamental reconception of strategy, operations, technology, and management of human resources, and to succeed organizations should pursue a new strategic focus, build digital competence with a holistic view of products, services, processes, redefine customer/user experience, establish new ways of working (identity, retain, and develop the right talent to create and sustain a digital organization). Digitization in the public sector requires an integrated approach to technology, process, and people to manage the availability and sustainability of processes (Alhaqbani et. al 2016).

Lithuania's example in digital governance could be presented as a good practice. Lithuania is recognized as a country of technologies in different meanings: Lithuania has got world's fastest download Internet and second fastest upload Internet in 2011 (in 2020 it is in the 22nd place as recent test results by Ookla, the global leader in broadband testing and web-based network diagnostic applications, show) (Speedtest 2020). As it is obvious, that the technical solutions for digitalization are present, and Lithuania is among the countries with the best digitisation infrastructure, maybe it is not surprising that in Lithuania, more than 90 % of public services are accessible on the internet, and more than 80 % of citizens use e-government services. It could be stated, that Lithuania's public sector is both active in the digitising services and is searching for ways to further boost innovation. As an example of relevant initiatives could be mentioned the fact that Lithuania has become an official partner of Smart Country Convention in 2019 and had the opportunity to present itself exclusively in Berlin on October 22-24, 2019. This event was dedicated to presenting the latest digitization solution to the public sector, cities and municipalities (Lithuanian Ministry of Economy and Innovations 2020). The spheres in which public governance is digitalized in Lithuania are very diverse (Electronic Election Information System and Services, Electronic System for Job seekers and Employers, Security Operational Centers (SOC) Services; Mandatory Health Insurance Information System; Electronic Service for Registration of Legal Entities; Electronic Declaration System; Platform for Mobile ID and E-Signature; Taxpayers Electronic Education, Counselling and Information Service system, Insurance Accidents Regulation System; Integrated Information System of Penal Process (IISPP); Virtual Electronic Heritage System; a "single-window" information systems City Municipalities; and many others), some of those systems are developed better and more effective than

the others. However, the main criticism could be posed not on the systems, but on their management, as the analysis of those institutions and their competences made by the authors of this research indicates, that there is lack of coordination, which leads to a huge fragmentation of instruments, programmes, institutions and infrastructures, as a result, the various institutions play (or at least should play according to the definition of their functions) a similar role, there is a similar fragmentation of functions at the national agencies' level.

Another concept related to the digitalization of public institutions that should be here mentioned is a widely analysed "algorithmic governance" approach. Technology has both reflected and reorganised society (Bijker & Law 1992; Latour 2005). Public administration eliminates forms of incidental agreements that are undesirable because they do not allow for reliance on specific rules; rules and agreements in society are the minimum guarantees of stability and security. Thus, algorithmic governance is a form of public control based on rules and involves particularly complex computational epistemic procedures (Katzenbach & Ulbricht 2019), but the essential word remains "governance". However, yet the algorithmic governance potentially increases the effectiveness of public services, applying algorithmic measures often imply new forms of population monitoring, and raise human rights concerns (Mejias & Couldry 2019; Lyon 2014; Noble 2018). Privacy and data protection issues associated with the surveillance systems, lack of transparency that might be inherent in algorithmic governance, protection of governance system by a network of secrecy laws, rights to expression and opinion versus right not to dignity and protection from defamation – those are only a few issues that may be addressed through legal discourse in the project. Among the biggest challenges is the question, if predictive governance is in breach of existing laws and norms (Andrade 2012; Greengard 2012). Many scholars indicate, that recently deterioration of human rights online is more than often, despite clear declarations from the United Nations General Assembly and the Human Rights Council that offline rights established under international human rights law also are protected online (Kaye 2018).

3. Findings

The digitalization of all sectors of life is presumed as being a positive one. It is however clear, that the evolution of digital tools is a 21st-century opportunity, challenge and phenomenon that affects all dimensions of social life - philosophical, social, legal, administrative. Inevitably, human rights concerns are also affected. Usage of digital public governance may be considered as an advantage to society (for example, by facilitating more personalised education), but at the same time expansion of artificial intelligence tools and its inclusion in daily life may threaten certain rights, for example, the right to equality, the prohibition of discrimination, the right to privacy. On February 5th, 2020, a court in the Netherlands ruled that a government system that uses artificial intelligence to identify potential welfare fraudsters is illegal because it violates laws that shield human rights and privacy. The program uses an algorithm to predict a citizen's likelihood of committing fraud by tapping vast pools of personal data collected by the Dutch government like employment records, personal debt reports, education and housing history - information that was previously kept separately (Jacobson 2020). The

ongoing fight against coronavirus pandemia in the People's Republic of China has revealed the unprecedented use of different digital tools that could be attributed to the concept of artificial intelligence (AI) (facial recognition systems and high-end cameras, computerized systems that track ID cards), and numerous violation of human rights have been recorded. Due to the limited scope of this research, the authors will focus their attention on a few most often discussion areas of fundamental rights, interfered by the use of digital tools in public governance.

There are many efforts to develop new principles within the existing human rights framework, to refine existing ones to apply to the digital context, and to extend regulation to new actors (Guberek & Silva 2014). Speaking about the *freedom of speech*, it is paradoxical to say, but when it comes to the freedom of expression, the digitization of public institutions and the state's position as regards the protection of fundamental rights, the limitations and restrictions imposed by the state are observed more often than it could be expected. This issue may seem not related to the digitalization of the public sector, but in fact, the situation, on the contrary, is directly determined by the digitalization level of the governmental section - the government must have infrastructure, mechanisms, tools and capacities to impose restrictions. The research shows that a "chilling effect" on free speech, where citizens in certain countries feel less safe to assert their opinions, knowing that their personal data are monitored or archived (Donahoe 2014). The other indicator of the restricted right to freedom of speech is the internet restrictions imposed by governments on their own populaces, and this practice is surprisingly popular, only in 2017 more than 60 documented shutdowns are inspected (for example, in Bangladesh, Brazil, Burundi, Tajikistan, India, Ethiopia, Algeria, Congo, Pakistan, Syria, Iraq, and others), compared with 213 documented shutdowns in 2019 (with new countries, such as Benin, Zimbabwe, Eritrea, Gabon, and Liberia). Out of the 213 network disruptions documented in 2019, at least 196 were shutdowns (Taye & Anthonio 2019). For example, Chad cut access to social media platforms, for a staggering 472 days between 2018 and 2019. The government attempted to justify the social media blackout, stating that it was necessary for "security reasons." However, it was observed that authorities blocked access just as President Idriss Deby, who has been president of Chad since the 1990s, was making efforts to stay in power until the year 2033 (Woodhams 2019). Another example is related to not only the ability of the state to impose restrictions, but also to the intentions of the government to model the opinions of the people on governmental activities. In Iraq, after a massive protest against the government, in October 2019 the Iraqi government shut down the internet for more than 50 days (Al Jazeera, 2019). Sometimes the shutdowns may be justified by security reasons, and this is the positive outcome of the state public sector being digitalized – the predictive cyber policing must not be underestimated. For example, the United Kingdom cut Wi-Fi access in some of the city's stations of the underground transportation system in an attempt to "*prevent and deter serious disruption*" by climate change protesters, and this action was considered as preventive measures legally imposed by the UK police, to stop climate protestors from coordinating (Vincent 2019).

Thus, it is obvious that there are more and more situations when people face denial of their right to access information and freely express themselves. The danger and difficulty of opposing such state actions lie in the most often reason presented by the governments

– the state security issues. In cases when governments try to justify their restriction on the freedom of speech by the means of digital tools, the most often official justification was in one or other way connected to security reasons. As Taye & Anthonio (2019) research shows, the most often reasons indicated by governments, were the prevention of fake news/hate speeches, and precautionary measures.

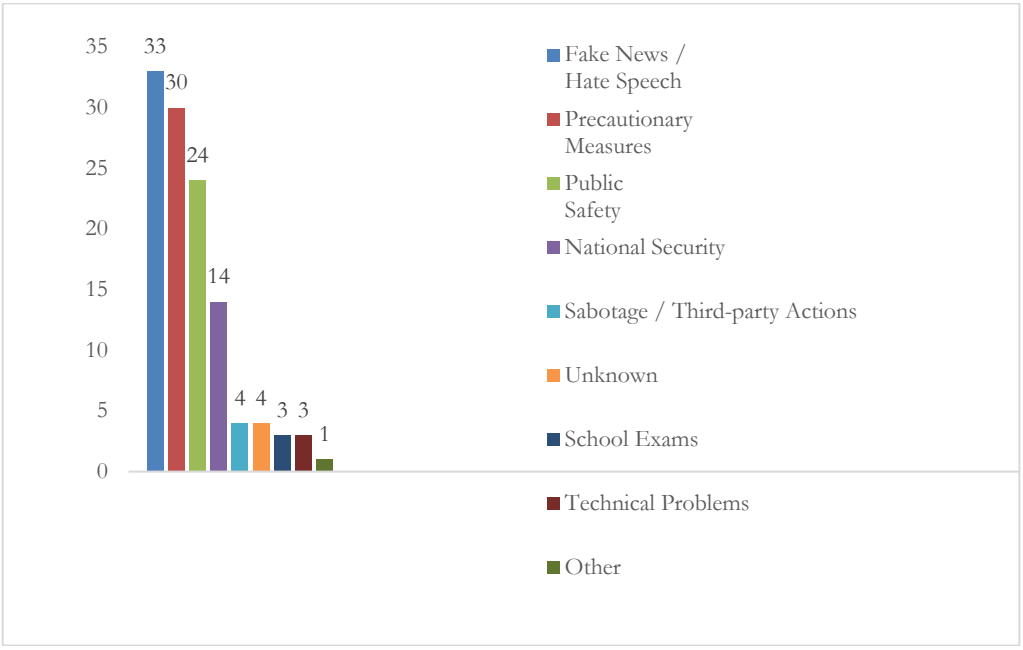

Figure 1. Justifications used by governments that ordered shutdowns in 2019
Source: Taye & Anthonio (2019), a table created by the authors

However, the real reasons based on information presented by observers were restraining of protests, attempts to hide state military actions, communal violence or political instability. Though sometimes seeming reasonable and justifiable, used not only by autocratic but also by the states that are considered as democratic ones, the attempts of the to control the access to information my have opposite than expected measures – to raise panic, uncertainty and distrust in the government among the population. It is also should be stressed, that such practice may impair democratic governance through the suppression of free speech and normal government functions (Policy Brief, 2015). The main challenge is that there is a lack of effective regulatory or oversight mechanisms, imposed on the states by adopted legal regulation. Legislative processes are catching up with digital change, and even more difficult is to find common legal standards at the international level. However, in 2014 forefront activity of adopting laws and codes of conduct to protect citizens' online rights was implemented, the Tallinn Agenda for Freedom Online was established, in which the members of the Freedom Online Coalition (delegates from over 60 countries) raised the intention to protect and strengthen freedom online in the face of new challenges and the complex and hotly debated subject of Internet governance (Freedom Online Coalition 2014a).Concerns

were raised over the growing wave of censorship of freedom of expression, attempts to establish state sovereignty over the Internet and deepening government involvement in restricting online freedoms in numerous countries around the world (Freedom Online Coalition 2014b). The Council of Europe also has adopted the Internet Governance Strategy for 2016-2019, aiming to strengthen democracy online, protecting human rights, and ensuring online safety and security (Council of Europe, 2016). The aim of the future legislation should not be the norms making impossible for the governments to restrict some fundamental rights, but creating a sustainable legal regulation enabling states to properly act applying security measures using very clear, transparent and not extensive legal norms. "It is imperative that governmental actions do not take a narrow view of security in which national security, counterterrorism, and sovereignty are held above all else" (Piccone 2018).

The other most sensitive aspect of digitalization of public institutions that may result in the breach of fundamental rights is digital tracking and surveillance, the collection of personal data for the purposes of profiling – this may pose *a threat to privacy* and the general enjoyment of human rights. Last few years many states and their public institutions have upgraded their capacity to use more advanced digital tools not only for censorship, that may infringe with breach of expression, but also surveillance, that often is on a thin and sharp line with the right to privacy. Speaking about surveillance techniques used by public institutions (most often those are law enforcement institutions in the broad sense of the meaning), there must be a distinction made between targeted and mass surveillance. Targeted surveillance focuses on a specific individual, set of individuals or regions and is thus at least potentially compliant with international human rights law (La Rue 2013). Mass surveillance, on the other hand, focuses on collecting all information possible from the digital sources, an indiscriminate practice that is likely in breach of International Covenant on Civil and Political Rights Article 17 ("*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation*") (ICCPR 1966). What should be mentioned here is that governments are not the only subject involved in implications of surveillance mechanisms, it is a common practice that surveillance tools are developed by private companies and later on sold to different states. A common legal standard for digital surveillance is the approach of allowance of surveillance while imposing the responsibility on governments to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. However, and it is correctly noted, "*no laws or guidelines can address all the challenges created by digital developments, in order to adequately protect digital rights, countries need to cooperate and develop comprehensive and smart policies to fulfil their obligations set out in internationally agreed laws and standards*" (Wagner et. al 2015). The European Union, in recognition of these challenges, issued the European Union Ethics Guidelines for Trustworthy AI (European Commission 2019), wherein it urged relevant stakeholders to voluntarily commit to these guidelines, and implement relevant audit systems, transparency and data and privacy protection measures – an instance of "soft law" (Abbott & Snidal 2000; Jackson 2010). Even bearing in mind current fundamental legislation (the General Data Protection Regulation) public institutions still have many possibilities to claim that national security justifies infringements on privacy.

There are many examples of public institutions exceeding their powers and infringing the privacy of private persons. For example, in 2017 Mexican government using the Pegasus software performed surveillance on human rights defenders, journalists and anti-corruption activists. In this specific case of government sponsored cyberattacks, the WhatsApp feed of the son of a prominent lawyer and civil right journalist was the target of intrusion and privacy infringement (Ahmed & Perlroth 2017). The biggest danger that most of the scholars indicate is that a serious potential exists for big data mining to be used to repress minorities, which consequently may broaden disproportionate incarceration of already marginalized groups. For example, China implemented a "Police Cloud" project, which enables law enforcement institutions to track social and ethnic groups (Human Rights Watch 2017). It is clear that it is necessary to oblige on governments that carry out reckless mass surveillance to limit their ability to collect and use private information about individuals. Most probably the national legislation here would not be a solution, therefore the international organizations must be proactive and interfere using their reputation and influence to adequately foster privacy-enhancing technologies that would protect all individuals equally. However, it should be also stressed that while governments are demonized as infiltrators of the privacy of their citizens, they are also guarantors of the digital human rights and have the powers to apply liability for those who violate those rights. As Goldstein and others (2018) state, "*legislation that safeguards sensitive data is important, and many countries are struggling to keep pace with innovations in information technology that have expanded the realm of digital rights*". Governments must both protect privacy and promote transparency (Gutwirth & De Hert 2008), it may be challenging, but that is most probably the only way how the balance between digitalized public governmental institutions and trust of the society may be achieved.

Conclusions

This research aimed to present the policies and examples of usage of digital tools by public institutions that may affect certain human rights, but at the same time, it attempted to demonstrate a link between offensive practices and the broader set of human rights. The main challenge in a very near future for the European Union in general, its member states separately in national levels, and other states around the world are to refine the definitions of all human rights in the online context. There is a sense of urgency to enhance the adequate regulation on protection of fundamental rights in digital space and, what is the most important, to balance interference by the state with a demand of new perception of fundamental rights. That would not only raise the concept of human rights to another level, but also would benefit for state institutions while building trust between government and the population, and introducing new capacities among their human potential. The research approach presented in this article emphasizes a human rights lens, which includes promoting and defending universal rights and freedoms in both the physical and the digital space. Without underestimation of new technologies and their impact on political, legal, social, economic development of all world, acknowledging the digitalization of the whole environment of human life as a key factor, it must be stressed that at the end of the day the main goal is human rights, and

not technologies, as technologies *per se* are not the problem nor the solution. The main goal is to determine how individuals, public and private institutions and social context are going to interact with digitalization, that most obviously is going to increase even more. This study is planned as a theoretical basis for further empirical research, which will include interviews with managers at the level of the heads of the relevant public sector institutions in order to determine the readiness of the institutions to work in the digital environment, to assess the legal framework on which these institutions apply digital solutions, and to identify factors leading to misuse of digital tools and further on to potential human rights violations.

References

1. Abbot, K.W. & Snidal, D. (2000) "Hard and Soft Law in International Governance", in *International Organization*. Vol. 54, No. 3, pp. 421-456, available at https://www.jstor.org/stable/pdf/2601340.pdf?refreqid=excelsior%3A966cd02500dfabcc8e8d2cd929c4b8ca Accessed 2020-04-18.
2. Ahmed, A. & Perlroth, N. (20170 "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families", in *New York Times*, published June 19, 2017, available at https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html , Accessed 2020-04-18.
3. Alhaqbani, A., et. al (2016) „The impact of middle management commitment improvement initiatives in public organisations", *Business Process Management Journal*, 22(5), pp. 924–938. DOI: 10.1108/BPMJ-01-2016-0018.
4. Al Jazeera (2019). Iraq protests: Death toll rises to 20 as unrest spreads. Published October 3, 2019, available at https://www.aljazeera.com/news/2019/10/iraq-imposes-curfew-baghdad-deadly-protests-191003060238724.html Accessed 2020-04-18.
5. Ananny, M., K. Crawford (2018). „Seeing without Knowing: Limitations of the transparency ideal and its application to algorithmic accountability". *New Media & Society* 20 (3), pp. 973-989.
6. Andrade, N.N.G. (2012). The application of future-oriented technology analysis (FTA) to law: the cases of legal research, legislative drafting and law enforcement. *Foresight* 14 (4), http://dx.doi.org/10.1108/14636681211256116 Accessed 2020-04-18
7. Babuta, A., M. Oswald, & C. Rinik (2018). „Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges". *RUSI Whitehall Report 3/18, September 2018*, pp. 1-37.
8. Berman, S. J., Korsten, P. J., & Marshall, A. (2016) „A four-step blueprint for digital reinvention", *Strategy & Leadership*, 44(4), pp. 18–25. DOI: 10.1108/SL-06-2016-0042.
9. Bijker, W. E., & Law, J. (Eds.). (1992). *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: The MIT Press.
10. Council of Europe (2016). "*Internet Governance – Council of Europe Strategy 2016-2019. Democracy, human rights and the rule of law in the digital world*". Adopted March 30, 2016. Available at https://edoc.coe.int/en/internet/7128-internet-governance-council-of-europe-strategy-2016-2019.html, Accessed 2020-04-18.
11. Donahoe, E. (2014) "Human Rights in the Digital Age." In *Just Security*, pp. 1-5, Published December 23, 2014, available at https://www.justsecurity.org/18651/human-rights-digital-age/ Accessed 2020-04-18.
12. European Commission (2019). "*Ethics Guidelines for Trustworthy AI*", available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Accessed 2020-04-18.
13. European Commission (2017). "*Digital4Development: mainstreaming digital technologies and services into EU Development Policy*", doc. SWD(2017)157, available at https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-157-F1-EN-MAIN-PART-1.PDF Accessed 2020-04-16

14. European Commission (2015) COM (2015)192 final. *A Digital Single Market Strategy for Europe*, available at https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-157-F1-EN-MAIN-PART-1.PDF Accessed 2020-04-16
15. European Parliament and Council (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*), OJ L 119, 4.5.2016, p. 1–88.
16. Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.
17. Ferguson, A. G. (2018). "Illuminating Black Data Policing." *Ohio State Journal of Criminal Law* 15, pp. 503-525.
18. Freedom Online Coalition (2014a), *Tallin Agenda For Freedom Online*, available at http://www.freedomonline.ee/foc-recommendations, Accessed 2020-04-10.
19. Freedom Online Coalition (2014b), available at https://freedomonlinecoalition.com/annual-conference/tallinn/ Accessed 2020-04-18.
20. Fyfe, N., H. Gundhus, K. V. Rønn, eds. (2018). *Moral Issues in Intelligence-led Policing*. London: Routledge.
21. Gray, J. and Rumpe, B. (2015) „Models for digitalization", *Software & Systems Modeling*, 14(4), pp. 1319–1320. DOI: 10.1007/s10270-015-0494-9.
22. Goldstein, K., Ohad, S, & Prazeres, D.T. (2018) "The Right to Privacy in the Digital Age", in Report of the High Commissioner for Human Rights, United Nations, available at https://www.researchgate.net/publication/328789396_The_Right_to_Privacy_in_the_Digital_Age , Accessed 20250-04-18.
23. Greengard, S. (2012). Policing the future. Communications ACM Vol 55, No 3, http://dx.doi.org/10.1145/2093548.2093555 Accessed 2020-04-18.
24. Guberek, T., & Silva, R. (2014) "Human Rights and Technology": Mapping the Landscape to Support Grantmaking, Ford Foundation, available at https://www.fordfoundation.org/media/2541/prima-hr-tech-report.pdf
Accessed 2020-04-18
25. Gutwirth, S. & De Hert, P. (2008). Regulating profiling in a democratic constitutional state. In *Profiling the European citizen*, pp. 271-302, Springer, Dordrecht.
26. (12) (PDF) The Right to Privacy in the Digital Age. Available from: https://www.researchgate.net/publication/328789396_The_Right_to_Privacy_in_the_Digital_Age [accessed Apr 18 2020].
27. Human Rights Watch (2017) "*China: Police 'Big Data' Systems Violate Privacy, Target Dissent*", published November 19, 2017, available at https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent Accessed 2020-04-18
28. International Telecommunications Union (2016), *Press Release: ITU releases 2016 ICT figures*, available at http://www.itu.int/en/mediacentre/pages/2016-PR30.aspx Accessed 2020-04-16
29. Jackson, K.T. (2010) "Global Corporate Governance: Soft Law and Reputational Accountability", in *Brooklyn Journal of International Law*, 2010, Volume 35, No 1, pp. 41-107. Available at https://heinonline.org/HOL/Page?handle=hein.journals/bjil35&id=43&collection=journals&index= , Accessed 2020-04-18.
30. Jacobson, D. (2020) "Dutch anti-fraud system violates human rights, court rules", in *UPI*, published February 5, 2020, available at https://www.upi.com/Top_News/World-News/2020/02/05/Dutch-anti-fraud-system-violates-human-rights-court-rules/6051580914081/ Accessed 2020-04-18.
31. Katzenbach, C. & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review*, 8(4). DOI: 10.14763/2019.4.1424
32. David Kaye, "*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*." United Nations General Assembly, A/71/373, September 6, 2016, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc Accessed 2020-04-18
33. Kemper, J., Kolkman, D. (2018). „Transparent to Whom? No Algorithmic Accountability without Critical Audience." *Information, Communication & Society*: 1-17. https://doi.org/https://doi.org/10.1080/1369118X.2018.1477967. Accessed 2020-04-16.

34. La Rue, F. (2013). "*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*", (A/HRC/23/40), United Nations, Geneva. Available at https://www.right-docs.org/doc/a-hrc-23-40/ Accessed 2020-04-18.
35. Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford; New York: Oxford University Press.
36. Lithuanian Ministry of Economy and Innovations (2020) *Digital-Lithuania*, available at https://digital-lithuania.eu/digitalgovernment/ Accessed 2020-04-18
37. Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, 1(2). https://doi.org/10.1177/2053951714541861 Accessed 2020-04-16.
38. Mejias, U. & Couldry, N. (2019) *Datafication. Internet Policy Review*, 8(4). DOI:10.14763/2019.4.1428.
39. Piccone, T. (2018). "Democracy and Digital Technology", in *International Journal on Human Rights*, 2018, Vol 15, Issue 27, pp. 29-38, available at https://sur.conectas.org/en/democracy-and-digital-technology/ Accessed 2020-04-18.
40. "Policy Brief: Internet Governance and the Future of the NetMundial Initiative", in *Access Now*, available at https://www.accessnow.org/cms/assets/uploads/archive/docs/POLICYBRIEFInternetGovernanceandtheFutureoftheNetMundialInitiative.pdf , Accessed 2020-04-18
41. Reascos, I., Carvalho, J. A., Bossano, S. (2019) Implanting IT Applications in Government Institutions: A Process Model Emerging from a Case Study in a Medium-Sized Municipality, *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV'19)*, Melbourne, Australia, April 3-5, 2019, DOI: 10.1145/3326365.3326376
42. Ruud, O. (2017) *Successful digital transformation projects in public sector with focus on municipalities*, Conference Central and Eastern European e|Dem and e|Gov Days, 2017 available at https://www.researchgate.net/publication/316715943_Successful_digital_transformation_projects_in_public_sector_with_focus_on_municipalities_research_in_progress Accessed 2020-04-16
43. Söderström, F., Melin, U., (2019), *Creating Local Government Innovation: Lessons Learned From An Institutional Theory Perspective, Electronic Government*, pp 125-138. https://doi.org/10.1007/978-3-030-27325-5_10 Accessed 2020-04-16.
44. Speedtest Global Index (2020), *Global Speeds*, available at https://www.speedtest.net/global-index Accessed 2020-04-18.
45. Sundberg, L (2019) Value Positions and Relationships in the Swedish Digital Government, *Administrative Sciences*, DOI: 10.3390/admsci9010024
46. Taye, B, & Anthonio, F. (2019) *Targeted, Cut Off, and Left In the Dark. The #KeepItOn report on internet shutdowns in 2019*, available at https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf Accessed 2020-04-18.
47. United Nations (1966) *International Covenant on Civil and Political Rights*. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49, available at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx Accessed 2020-04-18.
48. United Nations (2015) "*2030 Agenda for Sustainable Development"*, available at https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E Accessed 2020-04-16
49. Vincent, J. (2019). UK police shut off Wi-Fi in London Tube stations to deter climate protesters, in *The Verge*, Published April 17, 2019, available at https://www.theverge.com/2019/4/17/18411820/london-underground-tube-wi-fi-down-shut-off-protests-extinction-rebellion, Accessed 2020-04-18.
50. Wagner, et. al (2015) "*Surveillance and censorship: The impact of technologies on human rights*", European Parliament available at https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf Accessed 2020-04-18.
51. Woodhams, S. (2019), Chad social media ban reaches one-year mark, in *African Arguments*, Published March 28, 2019, available at https://africanarguments.org/2019/03/28/chad-social-media-shutdown-has-now-lasted-a-whole-year/ Accessed 2020-04-18.