VYTAUTO DIDŽIOJO UNIVERSITETAS
MCMXXII

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

HOW DOES THE PUBLIC'S INTEREST IN PARTICIPATING IN THE POLITICAL PROCESS INFLUENCE THE EQUILIBRIUM BETWEEN PRIVACY AND SECURITY IN CYBERSPACE?

Karolis Kubilevičius[1]
DOI: https://doi.org/10.7220/2029-4239.28.1

SUMMARY

E-democracy is becoming a prevalent factor in our daily lives. Whether knowingly (through utilising e-voting, e-petition systems, etc.) or unknowingly (by participating in discussion on social networks), citizens are beginning to exploit the advantages of e-democracy. Nevertheless, a comprehensive analysis of e-democracy from a purely legal perspective remains largely untouched. This article seeks to contribute to the ongoing discourse on e-democracy, with the specific focus on the delicate balance between security and privacy in the context of cybersecurity. Furthermore, the author introduces a third element to this intricate discussion – the public's interest in participating in the political process. Understanding and analysing the interplay between these three elements is crucial for the regulation of e-democracy.

KEY WORDS

E-democracy, cybersecurity, data protection, right privacy.

[1] Author is a PhD candidate at the Faculty of Law at Vytautas Magnus University in Kaunas, Lithuania. Being a practitioner of law, Karolis also specializes in civil law. Karolis is an author and co-author to various scientific articles, lecturer as well as participant of various research initiatives.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

INTRODUCTION

One of the most complex conundrums in the contemporary world pertains to striking a balance between security and privacy. On the one hand, the right to privacy is a foundational tenet of European Convention on Human Rights (hereinafter – **ECHR**). With the introduction of the General Data Protection Regulation (hereinafter – **GDPR**) in the European Union (hereinafter – the **EU**), the emphasis on the protection of the abovementioned right is more pronounced than ever before.

On the other hand, security is a critical component of a functioning society. In the era of the 4.0 Industrial Revolution (and even prior to it), security is no longer viewed merely as a defence against conventional warfare or physical threats. Cyberattacks have supplanted these traditional forms of threats and conflicts. Even terrorism has evolved into cyberterrorism. According to latest data, "cyber-attacks against organizations worldwide increased by an average of 50% in 2021, compared to 2020"[2]. Additionally, cyberattack campaigns are becoming "increasingly sophisticated and automated, targeting exposed attack surfaces that keep expanding and quickly exploiting vulnerabilities"[3]. In fact, due to a variety of cyberattacks, the EU's cybersecurity agency has assembled a list of the top 15 cyber threats[4]. The COVID-19 pandemic[5] and the Russia-Ukraine conflict[6] have undoubtedly escalated the number of cyberattacks occurring worldwide. The rise in expenditures on cybersecurity[7] also underscores the increasing threat of cyberattacks.

This illustrates the paradox between cybersecurity and privacy. To ensure security within cyberspace, states must ideally have access to as much data (private or otherwise) as possible. With access to private data, states can detect a cyberattack swiftly and neutralise it. Moreover, states can utilise the obtained data to bolster nationwide pre-emptive cybersecurity strategies and create countermeasures. Simultaneously, the greater the security (i. e., the more accessible the data becomes), the less privacy citizens have. While the conflict between privacy and security is not a novel issue, the context within which this issue will be analysed in this article is.

Electronic democracy (hereinafter – **E-democracy**) is a measure meant to strengthen or potentially transform traditional democracy through the use of information and communication

[2] S. Carlos, Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed, accessed January 10, 2023, https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed.

[3] Proposal for a regulation of the European parliament and of the council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, European Commission, 2022-03-22 OJ, COM/2022/122.

[4] European Union Agency for Cybersecurity, List of top 15 threats, accessed August 7, 2022, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-enisas-list-of-top-15-threats.

[5] European Union Agency for Cybersecurity, Cybersecurity in the healthcare sector during COVID-19 pandemic, accessed May 11, 2022, https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic.

[6] L. Cerulus, Cyber 'spillover' from Ukraine looms in the Baltics, accessed August 7, 2022, https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/.

[7] Spending on cybersecurity worldwide from 2017 to 2022, accessed August 7, 2022, https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

technologies (hereinafter – **ICT**). It empowers citizens to exercise their political rights electronically. While e-democracy brings a lot of benefits, such as streamlined public administration and simplified exercise of rights, it is also vulnerable to cyberattacks, like any other technology. In the context of e-democracy, if the instruments employed in the exercise of citizens' rights become compromised, the fundamental breach involves not merely citizens' privacy, but their rights, or in this case – political rights. The violation of citizens' rights undermines the sovereignty of a democratic state as well. Therefore, security is of paramount importance when devising, implementing and utilising e-democracy instruments. If states do not have complete access to the database of the aforementioned instruments (and their creation process), there is a real risk that the rights of citizens will be infringed. Moreover, the credibility of similar technologies will also be questioned, as citizens could lose trust in them. While it might be argued that privately created e-democracy instruments should be responsibility of the entity that created them, it remains the duty of the state to protect its citizens and their rights. Consequently, data gathered and used by e-democracy instruments, irrespective of who creates these instruments (i. e., public or private body), should also be managed by the state.

Due to peculiarity of this subject, there is a lack of literature that analyses this specific issue. Furthermore, numerous states tend to combine technologies related to democratic processes with other communication technologies, thereby applying similar priorities with respect to cybersecurity. Ultimately, the author will explore the balance between security and privacy within the cybersecurity context with the addition of a third element – the public interest in participating in the political process. This highlights the **novelty** of this topic.

At first glance, it might seem that the problem lacks relevance, because within the EU "privacy and data protection are not absolute rights and can be limited under certain conditions"[8]. Nevertheless, the topic of balance between security and privacy continues to stir heated debates. Moreover, e-democracy in general is not widely prevalent. Only a handful of countries even permit electronic voting[9], not to mention other forms of e-democracy. However, even if official institutions do not permit or support electronic voting or other forms of e-democracy, private individuals can create e-democracy instruments themselves (such as websites dedicated to e-petitions). Therefore, such instruments already exist. With scholars still debating over what is more important – privacy or security, e-democracy instruments are already falling victim to cyberattacks (e.g., Russian hackers gaining access to e-mails that swayed the public opinion of U.S. citizens thus affecting the outcome of the 2016 presidential elections[10]). Consequently, the analysed topic is **relevant.**

Finally, this article will contribute to the ongoing dialogue concerning e-democracy, cybersecurity and data protection. These fields intersect yet also conflict, particularly when discussing the principle of proportionality within the context of this article. The inherent interconnection of these discussed fields forms the basis of this article. Therefore, these three areas and their interrelation and balance thereof will be the focus of this article.

[8] European data protection supervisor, Data protection, accessed August 15, 2022, https://edps.europa.eu/data-protection/data-protection_en.

[9] The International Institute for Democracy and Electoral Assistance, Is e-voting currently used in any elections with EMB participation?, accessed August 15, 2022, https://www.idea.int/data-tools/question-view/742.

[10] U.S. Department of Justice, Report On The Investigation Into Russian Interference In The 2016 Presidential Election, accessed May 5, 2023, https://www.justice.gov/archives/sco/file/1373816/download.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

The article is composed of three primary sections. The first section scrutinises e-democracy and its distinct characteristics. The second section is centred on matters associated with cybersecurity. Lastly, the third section is devoted to addressing issues of data protection and privacy.

The *object* of this article is the interconnection between cybersecurity, personal data and public interest to participate in political process and balance thereof.

The following *research question* is addressed: should e-democracy technology (instruments) be subject to the GDPR?

Limitations. The legal reasoning presented in this article should be understood within the context of the legal systems of the EU and Lithuania.

Methodology. The author will undertake a comprehensive literature review. In order to dissect the topic at hand, a comparison of a broad spectrum of legal regulations, including but not limited to the European Convention on Human Rights, General Data Protection Regulation and Cybersecurity Act, will be executed. These legal regulations bear an intricate relationship as EU member states, although not mandatory for the EU itself, must comply with both the ECHR and EU regulations. However, this could potentially shift with the EU's accession to the ECHR[11].

Therefore, norms contained within both the ECHR, GDPR and other relevant legal frameworks, which address the protection of privacy, are crucial in analysing this subject. Consequently, one of the ways to safeguard privacy is by ensuring suitable security. This leads us to another key topic of this article. The responsibility for ensuring security predominantly rests on the shoulders of member states. Consequently, both privacy and security, along with the norms governing these two subjects, are pertinent and warrant analysis.

E-DEMOCRACY AND ITS IMPACT

What is E-democracy?

Conceptually, the definition of e-democracy might seem straightforward, but literature presents a different reality. When e-democracy, the idea of harnessing information and communication technologies (hereinafter – **ICT**) for political purposes, was in its infancy, it was referred to by various terms such as "digital democracy"[12], "teledemocracy"[13], virtual democracy and cyberdemocracy. Even after the e-democracy concept somewhat crystallized, many scholars continue to use the term "e-democracy" interchangeably with e-government, e-governance, e-participation, etc., though these concepts, while overlapping, are distinct.

Although scholars continue to grapple with a universally agreed-upon definition, the concept of e-democracy has remained fairly stable, with the difference primarily lying in its scope. Some

[11] Press and information team of the Delegation to the COUNCIL OF EUROPE in Strasbourg, Major progress on the path to EU accession to the ECHR: Negotiations concluded at technical level in Strasbourg, accessed July 10, 2023, https://www.eeas.europa.eu/delegations/council-europe/major-progress-path-eu-accession-echr-negotiations-concluded-technical-level-strasbourg_en?s=51.

[12] B. N. Hague and B. D. Loader, Digital democracy: Discourse and decision making in the information age (NY: Routledge, 1999).

[13] T. Becker, "Teledemocracy: Bringing power back to the people" Futurist 15, No. 6 (1981), 6-9.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

researchers view e-democracy as a broader concept[14], while others narrow it down to citizen participation.[15] Hacker and van Dijk define digital democracy as "the use of information and communication technology (ICT) and computer-mediated communication (CMC) in all kinds of media (e.g. the internet, interactive broadcasting and digital telephony) for purposes of enhancing political democracy or the participation of citizens in democratic communication"[16]. The definition here underscores the supplementary nature of e-democracy as an instrument for existing democratic processes.

However, the view of e-democracy merely as an auxiliary instrument hardly does justice to its transformative potential. For instance, Coleman and Norris suggest that "[a] common thread <…> is the assumption that e-democracy has something to do with the use of information and communication technologies (ICT) to enhance democratic structures and processes <…> E-democracy is both top-down and bottom-up; it is both about the institutional processes of hierarchies and the more fluid arrangements of networks"[17]. Despite e-democracy eventually enriching democratic processes, Coleman and Norris contend that it is not merely an instrument to improve existing systems.

With digitalization, e-democracy (namely, the citizen media) has already altered power dynamics[18]. Digital/social media now wield unprecedented power to not only connect representatives with the represented but also influence public opinion or even affect voting results. Moreover, emerging social networks (e. g., Facebook) have proven to be potent tools for rallying like-minded individuals or influencing their opinions.

Consequently, e-democracy has transcended traditional democratic boundaries and hastened the engagement of citizens through a plethora of ICT platforms. This trend could potentially birth new forms of democracy – internet democracy, liquid democracy, peer-to-peer democracy, blockchain democracy, decentralized autonomous democracy, wiki-democracy[19], etc. It can be concluded that e-democracy can impact the traditional methods of how citizens exercise their rights, extending beyond merely enhancing existing democratic processes.

In the present context, given that e-democracy is not extensively utilised as an "official" instrument, the author will define e-democracy as instruments, used to enhance existing democratic processes. More precisely, the author will adopt the definition provided by the European Parliament, which states that e-democracy is "the support and enhancement of traditional democracy by means of ICT, and which can complement and reinforce democratic processes by adding elements of citizens' empowerment through different online activities that

[14] Supra note 12.

[15] A. Manoharan and M. Holzer, Active Citizen Participation in E-government: A Global perspective (Hershley: IGI Global, 2012), 129.

[16] K. L. Hacker and J. A. G. M. van Dijk, „What is Digital Democracy?", in Digital Democracy : Issues of Theory and Practice (London: SAGE Publications, Limited, 2021), 1.

[17] S. Coleman and D. F. Norris, A New Agenda for e-Democracy, (OII Forum Discussion Paper, No. 1, 2005), 1-36.

[18] S. Meraz, "Is There an Elite Hold? Traditional Media to Social Media Agenda Setting Influence in Blog Networks", Journal of Computer-Mediated Communication 14, No. 3 (2009), 701, doi: doi.10.1111/j.1083-6101.2009.01458.x.

[19] Z. Bastick, "Digital Limits of Government: The Failure of E-Democracy", in Beyond Bureaucracy: Towards Sustainable Governance Informatisation (Springer International Publishing, 2017), 13.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

include, amongst others, e-government, e-governance, e-deliberation, e-participation and e-voting"[20].

While the definition provided by the European Parliament could encompass social media platforms, the author, in discussing e-democracy instruments, will primarily refer to platforms that enable users to vote electronically, file a petition or referendum, consult with representatives, etc. The challenges surrounding social media platforms as an instrument of e-democracy are not the subject of this article and therefore will not be discussed.

Implementation of E-democracy and its Use in Practice

The benefits of employing e-democracy are indisputable. According to Grigorios Spirakis and others, (i) "local citizens and communities have more power and responsibility for local and public affairs as they have the possibility to tell their opinion and make their political choice"[21], (ii) "local councils can listen to citizens' opinion and represent citizens through ICTs"[22], (iii) citizens acquire the skill of attentive listening to one another, engage in public discourse and community-level conversations, and foster mutual tolerance[23], (iv) local and national affairs can witness a heightened level of citizen and community engagement for greater effectiveness[24]. Another significant advantage is that e-democracy reduces regional isolation.

It is clear that the primary benefit of e-democracy is to amplify citizens' capacity to participate in the political process, which can be attributed to the supplementary nature of e-democracy. However, heightened citizen participation is not the sole advantage of e-democracy. Enhanced e-literacy and cyber-awareness constitute another key benefit, which not only complements the aforementioned advantages of e-democracy bus also fosters trust in technologies.

Despite the plethora of benefits, the usage of e-democracy's technology varies. The following examples summarise the use of e-voting systems worldwide:

[20] European parliament, European Parliament resolution of 16 March 2017 on e-democracy in the European Union: potential and challenges (2016/2008(INI)), accessed August 20, 2022, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0095_EN.html.

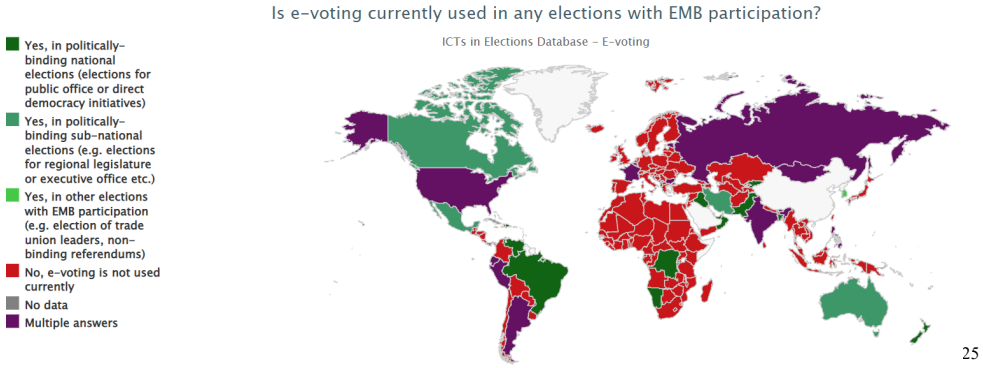
[21] G. Spirakis, C. Spiraki and K. Nikolopoulos, "The impact of electronic government on democracy: e-democracy through e-participation", *Electronic Government an International Journal* 7, No. 1 (2010), 82, doi: 10.1504/EG.2010.029892.

[22] Id..

[23] S. Wright, "Electrifying democracy? 10 years of policy and practice", *Parliamentary Affairs* 59, No. 2 (2006), 236–249, doi: 10.1093/pa/gsl002.

[24] D. R. Insua, "Introduction to the special issue on e-democracy", *Group Decision and Negotiation* 17 (2008), 175-177, doi: 10.1007/s10726-007-9077-7.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27



25

Upon observation, it is apparent that many states are hesitant to fully implement any kind of e-voting system, or to implement such a system at all. In contrast, the scenario with e-petitions is somewhat different. Largely, even if a state does not officially support or possess an e-petition system, individuals often develop specialized websites that citizens can utilise to submit their online petitions.

In lieu of a graphical representation, the author will present statistical data for a few e-petition systems. To illustrate, a total of 33,181 e-petitions were submitted to the "House of Commons and Government system" over the period from 2017 to 2019. Total number of unique users – 16 166,387[26].

Meanwhile, another well-known e-petition system, www.change.org, received a total of 791,896 e-petitions in the United States of America alone, amassing "more than 463,883,172 signatures in total"[27]. The disparity in availability and popularity between e-voting and e-petition systems leads to the conclusion that the accessibility of e-democracy instruments largely depend on their impact. For instance, while e-petitions may be more prevalent and accessible, it does not imply that a majority (if any) of petitions will succeed. Conversely, e-voting systems, albeit less frequently used, may exert a greater influence on the local populace.

The accessibility and use of e-democracy instruments, while undoubtedly dependent on available technologies, are profoundly influenced by the risks inherent in cyberspace.

Risks Possessed by E-democracy

The European Parliament has encapsulated the primary risks of e-democracy: "whereas further progress on cybersecurity and data protection is essential if we wish to make greater use of new technologies in institutional and political life and thereby enhance citizen participation in decision-making"[28]. An obvious conclusion can be made that the current advancement of cybersecurity technologies is insufficient to protect e-democracy technologies from cyber threats.

[25] *Supra* note 9.

[26] UK Parliament, House of Commons trends: E-petitions, accessed January 11, 2023, https://commonslibrary.parliament.uk/house-of-commons-trends-e-petitions/.

[27] A. Mustafic, Change.org Releases Top Ten Petitions that Changed 2021, accessed January 11, 2023, https://www.change.org/l/us/change-org-releases-top-ten-petitions-that-changed-2021.

[28] *Supra* note 20.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

While the importance of cybersecurity is recognized across all sectors that have adopted or seek to adopt technological solutions, a breach in e-democracy, its instruments, could lead to the violation of citizens' rights. Inevitably, such a violation could infringe upon the sovereignty of a democratic nation (since, democratic countries, sovereignty typically rests with its citizens).

Another risk involves the sensitivity of data. While cybersecurity encompasses all forms of security systems that protect users from cyberthreats, data protection technologies primarily focus on information directly related to individuals. In the context of e-democracy, this type of data could include information related to the citizen (defined as personal data under GDPR), as well as aspects of their identity (economic, cultural, social or even political).

Even a vote cast in an election could, to a certain extent, be considered personal data (as defined in the GDPR), because in the event of a security breach, this information could be used to target a specific citizen, or citizens, in an attempt to manipulate their voting behaviour. In other words, when a person casts their vote, they do so based on their beliefs and views. This is valuable personal information. In fact, some states have enshrined the secrecy of voting in their constitutions, e. g. the Republic of Lithuania, article 55, 78, 119[29].

While cyber threats and data breaches are arguably the two main risks of e-democracy, they are not the only ones. The over-representation "of a small cross-section of the population"[30] is another risk that may lead to misleading results. Despite the era of technology, a digital divide still exists[31]. Without appropriate measures, this could result in policies being accepted by only a handful of the population who have access to various ICTs.

Another risk is the danger for normalising the applicability of e-democracy to the offline world. As Zach Bastic has argued, the application of electronic technologies to existing, age-old, ideas serves to reinforce the current status quo[32]. The concept of democracy is thousands of years old, and established democratic principles have largely remained unchanged throughout the ages. Indeed, even with the introduction of e-democracy and the internet in general, no "internet revolution" has occurred in states. Instead, new instruments provided by the internet are used to further consolidate and maintain political power. This undermines the core concept behind e-democracy, i. e., restoring political power to the citizens. Despite this, it is not all negative; there are states that do make extensive use of electronic technologies to encourage citizen participation (e. g., the Republic of Estonia). However, often the full potential of these technologies is not realised.

The concept of democracy itself must evolve. The previously mentioned examples represent just a few of the different types of democracy that warrant exploration. Without such evolution, we risk a situation where outdated norms, originally adapted for traditional forms of democracy, may fail to safeguard citizens' rights within cyberspace.

Upon analysing the key characteristics of e-democracy, this article will now delve into the concepts and peculiarities of the right to security and privacy. The presence or absence of these rights may significantly influence the implementation of e-democracy instruments.

---

[29] Constitution of the Republic of Lithuania, Official Gazette (1992, No. 220-0).

[30] The Organisation for Economic Co-operation and Development, *Promise and Problems of E-Democracy: Challenges of Online Citizen Engagement* (Paris: OECD PUBLICATIONS, 2003), 16, https://www.oecd.org/governance/35176328.pdf.

[31] M. Negreiro, Bridging the digital divide in the EU, accessed August 15, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/573884/EPRS_BRI(2015)573884_EN.pdf.

[32] *Supra* note 19, p. 10.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

CYBERSECURITY

Risks Possessed by E-democracy

Prior to discussing the right to cybersecurity, it is crucial to establish the parameters and peculiarities of cyberspace. Despite the existence of myriad definition, this article will adhere to the following – cyberspace is a "global domain within the information environment consisting of the interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[33]. The term "global" serves as the defining characteristic of this definition. In essence, cyberspace is boundless, devoid of physical borders, and as such, allows subjects, irrespective of nationality or residency, to navigate foreign cyberspace freely and virtually (e. g., the ability to virtually explore foreign museums).

With the acknowledgment that cyberspace is, in fact, devoid of physical boundaries, a question arises wherein individual states struggle to apply their respective legal norms to incidents transpiring within or because of cyberspace. In this context, one might posit that cyberspace is essentially a lawless domain. To ascertain the validity of this assertion, it becomes necessary to analyse the definition of sovereignty, as sovereignty underpins the state's prerogative and capacity to enforce its legal norms.

Sovereignty "signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[34] While sovereignty is conventionally understood as something associated with physical land, "the principle of State sovereignty applies in cyberspace"[35] as well. Therefore, regardless of whether it pertains to physical space or cyberspace, foreign nations "must not conduct cyber operations that violate the sovereignty of another State"[36].

Given the aforementioned arguments, the protection of cyberspace may be deemed state's responsibility. In fact, the author argues that cybersecurity ought to be the responsibility of a state, akin to how the state bears the responsibility for overall security. This could be either individually or in cooperation with other states, as suggested by Article 73 of the Treaty on the EU (hereinafter – **TEU**).

As such, much like security, cybersecurity should also be guaranteed by the state. Upon defining cyberspace and sovereignty, it becomes possible to define cybersecurity. The author will refer to the definition provided in the Cybersecurity Act (hereinafter – the **CA**), which describe cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"[37]. Since networks and information

[33] National Institute of Standards and Technology, Guide for Conducting Risk Assessments, accessed January 17, 2023, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[34] *The Netherlands v. U.S.A.*, Permanent Court of Arbitration (1928, II RIAA 829).

[35] M. N. Schmitt, "Sovereignty", in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Newport: Cambridge University Press, 2017), 11.

[36] Id.

[37] Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

systems, despite their physical manifestations, primarily operate in the same cyberspace, a state indeed bears an obligation to protect its cyberspace. Consequently, cybersecurity also signifies the security of one's own cyberspace to a certain degree.

While the CA does lay the groundwork for cybersecurity-specific regulations, the right to cybersecurity as such is not formally acknowledged. Nonetheless, despite the absence of formal recognition, it is irrefutable that cybersecurity holds significant importance for states, private entities and even citizens to function effectively in the era of the fourth industrial revolution, given that cyber threats are only becoming increasingly prevalent[38].

Hence, while the right to cybersecurity may not be formally guaranteed, the member states of EU are obliged to ensure security (including cybersecurity) within their jurisdiction. Article 4(2) of the Treaty on EU, stipulates that "[the Union] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security"[39]. As stipulated by the aforementioned article, safeguarding national security is considered one of the essential duties that a state possesses. In this context, cyber threats can compromise national security, and there have been numerous instances in practice where they have done so[40]. Therefore, in the era of the Fourth Industrial Revolution, states must remain steadfast in protecting their cyberspace.

Having established that the right to cybersecurity ought to be guaranteed, the author will further delve into the legal landscape of cybersecurity and the issues associated with it.

Legal Regulation of Cybersecurity and Related Issues

The CA constitutes the primary specialized legal framework in the EU concerning the regulation of cybersecurity. According to article 1(b), the CA established "a framework for the creation of European cybersecurity certification schemes with the aim of assuring an adequate level of cybersecurity for ICT products, ICT services, and ICT processes in the Union <…>"[41].

The author contends that this article is crucial within the context of the topic discussed within, as it empowers the European Union Agency for Cybersecurity (hereinafter – the **ENISA**) to formulate an ICT certification scheme. In compliance with Article 51 (1) of the CA, cybersecurity certification schemes should encompass elements like rules for monitoring adherence with ICT products, extra prerequisites to which conformity assessment bodies are subject, and so forth. However, up to the present time, there have been only a few certification schemes (as per ENISA), signalling that this entire process is relatively new. Moreover, it suggests that the EU is heading in the right direction, as it implicitly recognises the different ICT

certification and repealing Regulation (EU) No 526/2013, 2019-06-07, Official Journal of the European Union, L 151.

[38] M. Hill and D. Swinhoe, The 15 biggest data breaches of the 21st century, accessed April 6, 2023, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html#tk.rss_dataprotection.

[39] Consolidated version of the Treaty on European Union, 2012-10-26, Official Journal of the European Union, No. 326/01.

[40] Significant Cyber Incidents, accessed September 20, 2023, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[41] *Supra* note 37, art. 1(b).

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

products should be regulated by different legal stipulations, the specifics of which are ultimately determined by the field that will utilise the ICT.

Another EU legislative act set to address cyber threats is the Cybersecurity Resilience Act. However, the author will refrain from delving into further detail, as the abovementioned legislation is currently in its proposal phase and awaits approval from the appropriate EU bodies.

Lastly, the Regulation on electronic identification and trust services for electronic transactions in the internal market (hereinafter – the **EITS**) holds relevance to this article as well. Trust services, as defined in the aforementioned directive, include services that can assure the cybersecurity of ICT. The security of e-democracy instruments may be partially outsourced, for example, by implementing a high-quality electronic signature that safeguards against certain types of cyberattacks. Moreover, the regulation itself established requirements for service providers to ensure proper security measures[42].

Despite the aforementioned points, incidents related to cybercrime continue to escalate[43]. Moreover, according to Microsoft, 24% of reported attacks occur in the public sector[44]. Consequently, with the deployment of e-democracy technology, the risk perseveres. This statement is further corroborated by authors such as Haugen, who contends that "technology to improve services to citizens also increases exposure to cyber-crime and cyber-terrorism"[45].

Conversely, some authors contend that technology aimed at improving services for citizens "does not increase citizen participation since only a handful of people are using the information, and the information might facilitate terrorist attacks"[46]. Despite these observations being made in 2005, they still remain applicable to e-democracy instruments as such technology is not widespread.

Leif Sundberg in his analysis of e-government has outlined four risks: (1) IT security; (2) user adoption; (3) implementation barriers; (4) policy and democracy[47]. The author posits that some of these risks are relevant in the context of this topic. The security of IT is closely tied to cybersecurity. ICT must be secure. The security threshold is set even higher for technology utilised in the public sector. As previously argued, one of the primary challenges of using ICT in democratic processes is in fact that cyberattacks may not only compromise the integrity of these systems but also infringe on citizens' rights.

States, private companies and individuals must be obligated to ensure the highest possible security of e-democracy instruments, as such technology will be processing highly sensitive personal data. The risk factor should not merely limit itself to appropriate reaction to the

---

[42] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014-08-28, Official Journal of the European Union, L 257.

[43] F. Pennings, Cyber Resilience Act: A step towards safe and secure digital products in Europe, accessed April 6, 2023, https://blogs.microsoft.com/eupolicy/2023/02/16/cyber-resilience-act-cybersecurity-skills/.

[44] Id.

[45] S. Haugen, "E-government, cyber-crime and cyber-terrorism: a population at risk", *Electronic Government an International Journal* 2, No. 4 (2005), doi: 10.1504/EG.2005.008331.

[46] L. Sundberg, "Electronic government: Towards e-democracy or democracy at risk?", *Electronic government: Towards e-democracy or democracy at risk?* 118 (2019), 28, doi: 10.1016/j.ssci.2019.04.030; A. J. Meijer, "Risk maps on the Internet: Transparency and the management of risks", *Information Polity* 10, No. 1 (2005), 105-113, doi: 10.3233/IP-2005-0062.

[47] Id., 25.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

prevailing dangers but must also take into account the nature of technology. That is, the technology used in cyberattacks will persistently be refined, thus heightening the sophistication of cyberattacks.

Another risk pertains to policy and democracy. As previously discussed, the state must adopt suitable laws that would ensure all parties involved in the chain bear responsibility for cybersecurity. This includes entities that manufacture these systems or components thereof (for instance, if the technology of electronic signature is outsourced). It also includes those who provide the network needed for these systems to operate remotely, those who administer these systems and finally, the individuals who use these systems.

One method to ensure cybersecurity is through the adoption of suitable policies, which would apply to the aforementioned parties. However, the reality is not as straightforward. Regardless of the stringency of policies, there must ultimately be a mechanism in place to continuously monitor whether a particular system is under a cyberattack. To respond in a timely manner, the appropriate institutions must have access to a private individual's internet activity. Without this access, there is a chance that the individual may not be equipped to handle the cyberattack or may not even realise that they are a victim of such attack[48].

Understandably, institutions have restricted access to an individual's internet activity due to prevailing privacy laws, a topic that will be explored in the subsequent chapter.

PRIVACY

Right to Privacy

The primary legal document that governs data protection in the EU is Regulation 2016/679, concerning the protection of natural persons with regard to the processing of personal data and on the free movement of such data, otherwise known as the GDPR. A key objective of the GDPR is the protection of "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"[49]. The GDPR ensures that the personal data of natural persons are processed in accordance with stringent rules, and it provides individuals with the ability, albeit with limitations, to freely dictate how their personal data should be processed and whether it should be processed at all.

While there are exceptions, specified in Article 2(2) of the GDPR, where the regulation does not apply, the GDPR primarily governs all sectors where the personal data of natural persons (EU citizens) are processed. In the context of this article, a question arises as to whether internet (online) activity could be categorised as personal data. According to the definition provided by the GDPR, if this personal data could be used to identify a natural person, then internet (online) activity is treated as personal data. Moreover, in line with recommendations of CM/Rec (2014)6,

[48] D. Štitilis, „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos", *Socialinės technologijos* 3, No. 1 (2013), 203, doi:10.13165/ST-13-3-1-13.

[49] 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 process, 2016-05-04, Official Journal of the European Union, L 119.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

privacy on the internet, including the protection of personal data, is indeed safeguarded[50]. Therefore, it can be concluded that general surveillance of internet (online) activity is only permissible if one of the criteria stated in Article 2(2) of the GDPR is met (e. g., for the purpose of preventing, investigating, or detecting criminal offences, etc.)

Simultaneously, one could observe that institutions do not have the right to continuously monitor citizens' internet activity. The only way an institution could legally justify their surveillance of a natural person is by providing that the surveillance is conducted in order to protect the public interest. Apart from that, if there is no evident crime in process, or there is no evidence that the person will be a victim of a targeted crime, or there is no existing agreement, a person's private data should be respected. Therefore, a peculiar situation arises, where the state, to the best of its ability, cannot guarantee the cybersecurity of its citizens, because it cannot freely monitor citizens' activity in cyberspace.

The inability to guarantee cybersecurity does not arise solely from the fact that the state cannot continuously monitor the internet activity of private persons without a substantiated reason. Another significant reason is the clandestine nature of cyberattacks. Usually, citizens do not even realise that they have fallen victim to a cyberattack. A cyberattack does not always result in data loss. The purpose of a cyberattack could be to slow down a private person's electronic device, or it could simply be a display of prowess. Furthermore, even if the goal of the cybercriminal is data theft, the private person may not even be aware that their data has been stolen.

Moreover, if a company falls victim to a cyberattack, revealing the incident may not be in the company's best interest due to potential harm to its reputation. Therefore, companies often choose to conceal information about cyberattacks. This tendency makes it more challenging for a state not only to monitor the overall cybersecurity within its jurisdiction but also to improve its cybersecurity strategy based on practical incidents.

Hence, the author posits that a state should be granted the permission to continuously monitor e-democracy instruments. An infringement of these instruments could lead to a violation of citizens' constitutional rights and their right to the governance of the respective state.

Nonetheless, the right to privacy extends beyond the EU. It constitutes a fundamental human right, enshrined in Article 8 of the European Convention on Human Rights (hereinafter – **ECHR**). Part 2 of the aforementioned article permits public authority to interfere with this right only if deemed necessary "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"[51] This exception is consistent with the exemption outlined in Article 2(2)(d) of the GDPR.

Article 8 of the ECHR is crucial in the context of this discussion. If a person is utilizing an e-democracy instrument from the comfort of their home and the system is continuously monitored by relevant authorities, it could be argued that their right to private and family life has been

[50] Council of Europe, "GUIDE TO HUMAN RIGHTS FOR INTERNET USERS", accessed April 1, 2023, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31.

[51] Convention for the Protection of Human Rights and Fundamental Freedoms, 1950-11-04, Official Gazette, No. 4.XI.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

violated. This could be directly associated with private data and its processing, which is protected by the GDPR.

In the case of *Rättvisa*, the European Court of Human Rights ruled that personal data may be collected, provided that the *measures* to do so have been approved by an independent body and that they are needed for a specific reason[52].

The risk of arbitrariness was also highlighted in the case of *Roman Zakharov*[53]. The court further confirmed that storing "clearly irrelevant data"[54] and the absence of procedures for the destruction of such data do not ensure that secret surveillance measures are only used when "necessary in a democratic society".[55]

A clear conclusion can be drawn: the right to privacy is one of the most protected rights in a democratic society. However, the discussed cases and legislation have defined the boundaries of this right. First, if constant monitoring of certain technologies is necessary to ensure national security, such surveillance should be considered an exception. Second, appropriate policies must be in place that explicitly detail the procedures for monitoring such technologies, gathering data and establishing a timeline for data deletion.

Despite the abovementioned points, some authors argue that there is a tendency "to place cybersecurity in the same legal category as privacy"[56]. The author further explains that "while privacy is focused on protecting communications and deidentifying personal information, cybersecurity relates to the confidentiality, integrity, and availability of computer systems and networks"[57]. In other words, constant surveillance of e-democracy instruments would not necessarily result in a breach of privacy. However, even if a state were to adopt the above definition of cybersecurity in relation to privacy, it remains unclear whether it is technologically feasible to monitor an e-democracy system without having access to user's private information and whether all e-democracy instruments should be monitored, or only those managed by the state.

In the subsequent chapter, the author will examine how the balance between cybersecurity and privacy has shifted within the context of citizens' right to participate in the political process.

SHIFT OF BALANCE BETWEEN CYBERSECURITY AND PRIVACY

Public Interest to Participate in Political Process

In the initial section of this article, the author discussed in depth the concept and peculiarities of e-democracy. However, e-democracy itself pertains to electronic instruments, designed for use

[52] *Rättvisa v. Sweden*, ECHR (2018, No. 35252/08).
[53] *Roman Zakharov v. Russia*, ECHR (2015, No. 47143/06).
[54] Id.
[55] Id.
[56] A. M. Matwyshyn, "Cyber!", *Brigham Young University law review*, No. 5 (2017), 1109-1195, https://digitalcommons.law.byu.edu/lawreview/vol2017/iss5/6.
[57] Id.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

by citizens. The presence of e-democracy instruments does not inherently signify that a citizen has an irrefutable right to utilise these instruments.

Therefore, it is essential to analyse whether participation in the political process constitutes a public interest and whether the form through which participation occurs is absolute. Primarily, public interest is understood as the interests of a society or part of a society, which the state has an obligation to guarantee and fulfil[58]. In other words, it is a cherished expectation of an individual or individuals that exist in a legal state and exist objectively (i. e., irrespective of individual actions), exceeding the boundaries of private interests[59]. Consequently, public interest forms the foundation of citizens' rights. It is accepted that the recognition and realisation of public interest is crucial to the existence and development of the society itself[60].

That being said, there is no unanimous definition of public interest. Typically, it is determined on a case-by-case basis. For instance, various authors in the scientific literature define public interests as follows: under the principles of legitimacy theory, an organisation or profession can only gain societal approval and recognition when its value system aligns with the societal values of the community in which it functions.[61] There exists a mutual agreement, a form of social contract, between them.[62] Therefore, if a member of society infringed upon this agreement, it could be asserted that a violation of public interest has occurred. Naturally, this definition is more applicable to professions, where specific society members work not only for their private interests, but also for the public interests. It could be simplified to the point where working in accordance with public interest simply means working in alignment with the existing rule of law.

Other authors argue that public interest stems from the worth of public assets (public goods)[63]. In a particular article, the author presented an example of utilitarianism using a different context. For instance, consider a public good like a technological innovation. Utilitarians could argue that granting exclusive patent rights to a company or an individual is necessary - even though it restricts others from freely using that innovation - because what is crucial is that the innovation is developed and applied in a way that delivers the greatest benefit to society. In this instance, the public interest is tied to the value of that innovation, and proper development and application will extract the maximum societal benefit from it.

Finally, in some instances, current law outlines scenarios that could be categorised as public interest. Authors Lei Liu and Zhihang Xu postulate that these situations might encompass national defence, public utilities, social security and the "redevelopment of old urban areas"[64], among other things. Although the wording varies, all the aforementioned examples concur that the primary concern of public interest is the welfare of society. Whether a particular interest can be classified as a public interest is contingent upon the law (for instance, when the law expressly

[58] Decision of the Constitutional Court of the Republic of Lithuania (1997, No. 13/96).

[59] Id.

[60] Id.

[61] C. Deegan, "Introduction: The legitimizing effect of social and environmental disclosures – a theoretical foundation", *Accounting, Auditing & Accountability Journal*, No. 3 (2002), 282-31, doi:10.1108/09513570210435852.

[62] Id.

[63] A. Sheydayi and H. Dadashpoor, "The public interest- schools of thought in planning", *Progress in Planning* 165 (2022), 4, doi: 10.1016/j.progress.2022.100647.

[64] L. Liu and Z. Xu, 2018, "Collaborative governance: A potential approach to preventing violent demolition in China", *Cities* 79 (2018), 26-36, doi: 10.1016/j.cities.2018.02.019.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

identifies the public interest) or a specific circumstance. Moreover, there is a unanimous agreement that the responsibility of assuring this public interest lies with the state[65].

Having discussed the concept and definition of public interest, the author can determine whether the right to participate in political processes is a public interest. On the one hand, each public interest is rooted in fundamental societal values, which are enshrined and safeguarded in the constitution[66] or another principal legal act. In this instance, a simple review of the pertinent constitutions could answer this question. This is, if the right to participate is enshrined in the constitution, then it is indicative of a public interest. On the other hand, the matter is not that straightforward. Participation in the political process encompasses a broad range of activities. It could imply the right to vote, the right to submit a petition, the right to express one's opinion, or even include all administrative proceedings. Naturally, every individual case will not be documented in the respective constitutions.

However, as previously discussed, the right to exercise political rights is closely linked to sovereignty in a democratic state. This norm is also included in the constitutions of various states: Lithuania's (article 2), Latvia's (article 2), Estonia's (article), Finland's (section 2), etc. Therefore, the author posits that by enabling citizens to participate in political process, the public interest is preserved. If this was not the case, the fundamental source of a state's sovereignty, which constitutes the sovereignty both internally and externally, would be negated, thereby causing the state to lose its sovereignty. After all, in contemporary society, sovereignty is understood not as a control mechanism but as a set of obligations that the state must fulfil[67], primarily to its citizens and secondly to other parties.

This leads us to another query: should there be a limit on the form of participation or exercisability of political rights? Analogous to public interest, legal statues may also dictate the means by which citizens exercise their right to engage in the political process. However, without delving too profoundly into specific legal norms, it is crucial to understand that there are two primary modes of participating in the political process: either directly (verbally or in writing) or via a representative.

The author has previously established that the right to engage in the political process is an intrinsic right of every citizen and is deemed a public interest; therefore, it must be safeguarded. Consequently, if a state stipulates a procedure for citizens to exercise their rights in a variant of the two previously mentioned forms, for instance, electronically, it can be readily inferred that the right to exercise one's rights electronically is protected and guaranteed. This is because fundamentally, the ability to partake in the political process electronically mainly signifies that a citizen is employing electronic communication instruments to exercise his or her rights, either verbally (video conferences) or in writing (email, application submission through specialised websites). The form remains unchanged; only the exercisability of that form is modified.

Hence, it can be concluded that the right to engage in the political process constitutes a public interest and the method of participation is not absolute. Naturally, if an electronic system is designated as an instrument of e-democracy (provided no applicable legal rules specify otherwise), citizens should have an unassailable right to utilise these instruments. A question might arise regarding whether the right to develop such instruments should be exclusive to the

[65] Decision of the Constitutional Court of the Republic of Lithuania (2006, No. 35/03-11/06).

[66] Id.

[67] J. N. Maogoto, *Statal discipline and indiscipline: sovereignty as fealty of the independent state to international humanitarian normativity* (ElectronicPublications.Org Ltd, 2015).

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

state, or whether a private company could also produce similar e-democracy instruments. However, this question falls outside the scope of this article and will therefore not be further explored.

Moreover, if citizens have access to e-democracy instruments and can use them to participate in the political process, but these instruments are not governed by specific legal norms, the prevailing status of such a situation could lead to a violation of public interest.

The crucial point is that the state ultimately bears the responsibility for ensuring that forms of political participation, regardless of their variations, are safe, accessible and effective. If the state cannot guarantee this, it must prevent citizens from using unsafe e-democracy instruments. In the following sub-section, the author will elaborate on the state's obligation to safeguard citizens' right to participate in the political process.

The Duty of the State

Having established that states have obligations towards their citizens' welfare, including but not limited to, protecting the public interest often associated with citizens' rights (such as the right to housing, the right to vote, etc.), the author can proceed to answer the primary research question of this article.

Both privacy and security, or in the context of this article, cybersecurity, necessitate protection by the state. However, it is argued here that the compromise of private data, amassed when a citizen engages with an e-democracy instruments (for instance, inputting personal data to cast an online vote), would represent a far greater infringement.

In this context, it is crucial to distinguish between various scenarios. For instance, if a state persistently monitors an e-democracy instrument, thereby collecting and storing (either intentionally or unintentionally) private data associated with political participation, an argument could be put forth that the right to privacy or protection of personal data (in line with Article 8 of the EU Charter of Fundamental Rights) has been violated. This argument would stem from the fact that data related to political participation is generally confidential (for instance, Articles 55, 78, and 119 of Lithuania's Constitution explicitly state that voting is secret), and that, according to Article 6 of the GDPR, the state can process data only if there is an imminent or potential threat to the public interest. Even if the state requires citizens to sign temporary agreements to legally process their data, it is unclear how this would align with the principle of proportionality, as imposing additional legal obligations on every citizen is clearly excessive.

On the other hand, if the aforementioned data is compromised (leaked, stolen, deleted) by cybercriminals, it also represents an infringement of both the right to privacy and the protection of personal data. The question then arises, which of these scenarios causes greater harm to the public interest of state's citizens. Based on the prior discussion and arguments presented, the author contends that the latter example would constitute a more severe infringement of public interest. Although the former can also be seen as a violation of fundamental citizens' rights, or even nationally upheld citizens' rights, and might even be deemed an infringement of public interest (if we view maintaining public interest as simply respecting the basic constitutional and fundamental rights of citizens), the end effect is primarily on the individual citizen concerned.

Conversely, in the latter scenario, theft of personal data related to the political process could, in addition to the aforementioned repercussions, also infringe upon the state's sovereignty. While the state has an obligation to protect all relevant citizens' rights, it ultimately has to decide which

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

right is objectively more crucial and should be prioritized for protection. This aligns with Article 6(1)(e) of the GDPR, which stipulates that "[p]rocessing shall be lawful only if <…> processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."[68]

In this scenario, the public interest lies in citizens being able to exercise their political rights, thereby ensuring the state's sovereignty. Additionally, it is in the state's interest not only to protect these citizen rights, but also to safeguard the sanctity of its own sovereignty. Given the intertwined nature of sovereignty and citizens' political rights, they cannot be evaluated independently. Hence, in the context of e-democracy, priority should be accorded to cybersecurity. By ensuring robust cybersecurity, both the sovereignty of the state and the citizens' rights to participate in the political process are protected.

Shift of Balance or a New Reality?

Authors who have analysed the ongoing debate of security vs privacy argue that it's not a simple "black and white" issue[69]. David G. W. Birch posits that technology, designed for a specific purpose, does not necessarily need to contain personal and private information to fulfil its objective[70]. However, this does not apply to e-democracy instruments. The concern is not so much about the threat to private data *per se*, but rather the risk that this data might be compromised. Moreover, every action, whether casting a vote, submitting a petition, or signing a referendum, irrespective of additional personal data such as the user's name, age, and so on, is in itself private data. It not only serves a specific purpose (the expression of the citizen's will) but can also identify the citizens themselves. Therefore, in the case of the technologies in question, the state has an obligation to prioritise security, while treating privacy as a "desirable characteristic"[71].

Kevin Aquilina's stance on this issue also lends weight to the tilt towards security, as revealed in his attempt to strike a balance[72]. Aquilina recognises that the "scales of the balance are more often than not tilted in favour of public security to the detriment of individual privacy"[73], which aligns with the findings of this article. At the same time, he contends that public security is not absolute[74], and there should still be safeguards to protect privacy. Hence, it can be proposed that Aquilina, like the author, perceives security as the primary focus, with privacy as a secondary yet desirable trait. While Aquilina's analysis tackles a broader issue, the author of this article narrows down the problem to a specific type of technology – e-democracy instruments. To determine if exceptions should exist in this context, one must answer whether exceptions to preserving state sovereignty should be allowed. As previously argued in this article, the consensus

[68] *Supra* note article 49, art. 6(1)(e).

[69] D. G. W. Birch, "Victorian values: Politicians and the public incorrectly see security and privacy as opposites", *Information Security Technical Report* 14, No. 3 (2009), 144, doi: 10.1016/j.istr.2009.10.006.

[70] Id.

[71] Id., 12.

[72] K. Aquilina, "Public security versus privacy in technology law: A balancing act?", *Computer Law & Security Review* 26, No. 2 (2010), 142, doi: 10.1016/j.clsr.2010.01.002.

[73] Id.

[74] Id.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

is that there should be no exceptions when it comes to safeguarding state sovereignty and, by extension, citizens' rights to the political process.

V. Katos and C. Adams underscore the parallel existence of both security and privacy rights. Their position is that the use of technology (in their example - wireless technology) could lead to a "richer set" of information flow[75]. This concept could also be applied to e-democracy instruments as they process not only regular private information but data concerning political affiliations as well.

Katos and Adams contend that as a new form of technology is adopted, "both privacy and security landscapes change, requiring reassessment of how privacy and security levels can be maintained"[76]. However, till date, there has not been an in-depth examination of the potential shifts in the security and privacy landscapes specifically related to e-democracy instruments.

Admittedly, e-democracy instruments are yet to be widely adopted by states. Only in 2023 Estonia did achieve the milestone of conducting the "world's first mostly online national elections"[77]. Still, Estonia's success remains an exception rather than a standard as most other states have not implemented similar practices or have abandoned their initiatives altogether.

This situation exposes us to a whole new set of privacy and security concerns, which this article has sought to analyse. The establishment of a new type of policy is crucial if a state is to ensure the protection of citizens' rights concerning political participation.

Consequently, the integrity of e-democracy instruments becomes a pressing reality, as such technology empowers citizens to exercise their rights directly and more efficiently. As a result, their protection and security must be prioritised above all else.

CONCLUSIONS AND RECOMMENDATIONS

1. Taking into account the aforementioned discussion, it can be deduced that e-democracy instruments fall under the purview of the GDPR, but only on the condition that cybersecurity is assured. Within the context of e-democracy instruments, the right to privacy is considered a secondary right and should only be prioritised if cybersecurity is first ensured. This conclusion stems from the understanding that private data collected by e-democracy instruments is intrinsically linked to a state's sovereignty. Thus, any infringement on the right to privacy to guarantee the cybersecurity of such technology not only safeguards public interest but also facilitates the use of such instruments by citizens.
2. Indeed, if cybersecurity cannot be assured, e-democracy instruments should not be made available to the public. If such instruments are accessible without ensuring their safety, it becomes the state's responsibility to prevent their use. To maintain the principle of proportionality, the author suggests that e-democracy instruments could be managed, processed, or overseen by neutral entities. This would align with the previously

[75] V. Katos and C. Adams, "Modelling corporate wireless security and privacy", *The journal of strategic information systems* 14, No. 3 (2005), 307, doi: 10.1016/j.jsis.2005.07.006.

[76] Id., 319.

[77] E. Piirmets, "How did Estonia carry out the world's first mostly online national elections", accessed April 20, 2023, https://e-estonia.com/how-did-estonia-carry-out-the-worlds-first-mostly-online-national-elections/.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

mentioned cases, as even if priority is given to cybersecurity, the state would still be able to ensure sufficient protection of private data. If not, at the very least, the procedures to monitor these technologies could be approved by independent bodies.

3. Further research into this topic could delve into whether e-democracy instruments ought to be state-owned and developed, or whether private companies could also create and utilise such instruments. An ethical perspective could also be investigated. For example, it could be questioned whether private companies should be permitted to profit from such technology, given that the purpose of this technology is to aid citizens in exercising their rights. Similarly, determining the extent of a state's obligation to protect citizens' rights when using privately owned e-democracy instruments could also be probed. Or perhaps such technology could be regarded as "neutral", as argued by Lips and Koops[78]. Finally, in the context of e-democracy itself, it would be worthwhile to explore social media as an e-democracy instruments to examine how the balance between privacy and security shifts, if at all.

LEGAL REFERENCES

Special literature

1. Aquilina, K., "Public security versus privacy in technology law: A balancing act?", *Computer Law & Security Review* 26, No. 2 (2010), 142, doi: 10.1016/j.clsr.2010.01.002.
2. Bastick, Z., "Digital Limits of Government: The Failure of E-Democracy", in *Beyond Bureaucracy: Towards Sustainable Governance Informatisation* (Springer International Publishing, 2017).
3. Becker, T., "Teledemocracy: Bringing power back to the people" *Futurist* 15, No. 6 (1981).
4. Birch, W. G. D., "Victorian values: Politicians and the public incorrectly see security and privacy as opposites", *Information Security Technical Report* 14, No. 3 (2009), doi: 10.1016/j.istr.2009.10.006.
5. Coleman, S., and D. F. Norris, *A New Agenda for e-Democracy,* (OII Forum Discussion Paper, No. 1, 2005).
6. Deegan, C. 2002, "Introduction: The legitimizing effect of social and environmental disclosures – a theoretical foundation", *Accounting, Auditing & Accountability Journal*, No. 3 (2002), 282-31, doi:10.1108/09513570210435852.
7. Hacker, L. K., and Van Dijk, M. G. A. J, "What is Digital Democracy?", in *Digital Democracy: Issues of Theory and Practice* (London: SAGE Publications, Limited, 2021).

[78] Miriama Lips and Bert-Jaapa Koops, "Who regulates and manages the Internet infrastructure? Democratic and legal risks in shadow global governance", *Information Polity* 10, No. 1-2 (2005), 117-128, doi: 10.3233/IP-2005-0071.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

8. Hague N. B., and B. D. Loader, *Digital democracy: Discourse and decision making in the information age* (NY: Routledge, 1999).
9. Haugen, S., "E-government, cyber-crime and cyber-terrorism: a population at risk", *Electronic Government an International Journal* 2, No. 4 (2005), doi: 10.1504/EG.2005.008331.
10. Insua, R. D., "Introduction to the special issue on e-democracy", *Group Decision and Negotiation* 17 (2008), doi: 10.1007/s10726-007-9077-7.
11. Katos, V. and C. Adams, "Modelling corporate wireless security and privacy*", The journal of strategic information systems* 14, No. 3 (2005), doi: 10.1016/j.jsis.2005.07.006.
12. Liu, L. and Z. Xu, 2018, "Collaborative governance: A potential approach to preventing violent demolition in China", *Cities* 79 (2018), doi: 10.1016/j.cities.2018.02.019.
13. Maogoto, N. J., *Statal discipline and indiscipline: sovereignty as fealty of the independent state to international humanitarian normativity* (ElectronicPublications.Org Ltd, 2015).
14. Manoharan, A., and M. Holzer, *Active Citizen Participation in E-government: A Global perspective* (Hershley: IGI Global, 2012).
15. Matwyshyn A, M., "Cyber!", *Brigham Young University law review*, No. 5 (2017), https://digitalcommons.law.byu.edu/lawreview/vol2017/iss5/6.
16. Meijer, J. A., "Risk maps on the Internet: Transparency and the management of risks", *Information Polity* 10, No. 1 (2005), doi: 10.3233/IP-2005-0062.
17. Meraz, S., "Is There an Elite Hold? Traditional Media to Social Media Agenda Setting Influence in Blog Networks", *Journal of Computer-Mediated Communication* 14, No. 3 (2009), doi: doi.10.1111/j.1083-6101.2009.01458.x.
18. Schmitt, N. M., "Sovereignty", in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Newport: Cambridge University Press, 2017), 11.
19. Sheydayi, A. and H. Dadashpoor, "The public interest- schools of thought in planning", *Progress in Planning* 165 (2022), doi: 10.1016/j.progress.2022.100647.
20. Spirakis, G., C. Spiraki and K. Nikolopoulos, "The impact of electronic government on democracy: e-democracy through e-participation", *Electronic Government an International Journal* 7, No. 1 (2010), doi: 10.1504/EG.2010.029892.
21. Sundberg, L., "Electronic government: Towards e-democracy or democracy at risk?", *Electronic government: Towards e-democracy or democracy at risk?* 118 (2019), doi: 10.1016/j.ssci.2019.04.030.
22. Štitilis, D., „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos", *Socialinės technologijos* 3, No. 1 (2013), doi:10.13165/ST-13-3-1-13.
23. The Organisation for Economic Co-operation and Development, *Promise and Problems of E-Democracy: Challenges of Online Citizen Engagement* (Paris: OECD PUBLICATIONS, 2003), https://www.oecd.org/governance/35176328.pdf.
24. Wright, S., "Electrifying democracy? 10 years of policy and practice", *Parliamentary Affairs* 59, No. 2 (2006), doi: 10.1093/pa/gsl002.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

Legislation

25. Constitution of the Republic of Lithuania, Official Gazette (1992, No. 220-0).
26. Consolidated version of the Treaty on European Union, 2012-10-26, Official Journal of the European Union, No. 326/01.
27. Convention for the Protection of Human Rights and Fundamental Freedoms, 1950-11-04, Official Gazette, No. 4.XI.
28. Proposal for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, European Commission, 2022-03-22 OJ, COM/2022/122.
29. Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, 2019-06-07, Official Journal of the European Union, L 151.
30. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014-08-28, Official Journal of the European Union, L 257.
31. 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 process, 2016-05-04, Official Journal of the European Union, L 119.

Case law

32. Decision of the Constitutional Court of the Republic of Lithuania (1997, No. 13/96).
33. Decision of the Constitutional Court of the Republic of Lithuania (2006, No. 35/03-11/06).
34. Rättvisa v. Sweden, ECHR (2018, No. 35252/08).
35. Roman Zakharov v. Russia, ECHR (2015, No. 47143/06).
36. The Netherlands v. U.S.A., Permanent Court of Arbitration (1928, II RIAA 829).

Other reference

37. Carlos, S., Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed, accessed January 10, 2023 https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed.
38. Cerulus, L., "Cyber 'spillover' from Ukraine looms in the Baltics", accessed August 7, 2022, https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/.
39. Council of Europe, "Guide to Human Rights for Internet Users", accessed April 1, 2023, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

40. European data protection supervisor, Data protection, accessed August 15, 2022, https://edps.europa.eu/data-protection/data-protection_en.
41. European parliament, European Parliament resolution of 16 March 2017 on e-democracy in the European Union: potential and challenges (2016/2008(INI)), accessed August 20, 2022, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0095_EN.html.
42. European Union Agency for Cybersecurity, List of top 15 threats, accessed August 7, 2022, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-enisas-list-of-top-15-threats.
43. European Union Agency for Cybersecurity, Cybersecurity in the healthcare sector during COVID-19 pandemic, accessed May 11, 2022, https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic.
44. Hill, M., and D. Swinhoe, The 15 biggest data breaches of the 21st century, accessed April 6, 2023, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html#tk.rss_dataprotection.
45. Mustafic, A., Change.org Releases Top Ten Petitions that Changed 2021, accessed January 11, 2023, https://www.change.org/l/us/change-org-releases-top-ten-petitions-that-changed-2021.
46. National Institute of Standards and Technology, Guide for Conducting Risk Assessments, accessed January 17, 2023, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
47. Negreiro, M., *Bridging the digital divide in the EU*, , accessed August 15, 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/573884/EPRS_BRI(2015)573884_EN.pdf.
48. Pennings, F., Cyber Resilience Act: A step towards safe and secure digital products in Europe, accessed April 6, 2023, https://blogs.microsoft.com/eupolicy/2023/02/16/cyber-resilience-act-cybersecurity-skills/.
49. Piirmets, E., "How did Estonia carry out the world's first mostly online national elections", accessed April 20, 2023, https://e-estonia.com/how-did-estonia-carry-out-the-worlds-first-mostly-online-national-elections/.
50. Press and information team of the Delegation to the COUNCIL OF EUROPE in Strasbourg, Major progress on the path to EU accession to the ECHR: Negotiations concluded at technical level in Strasbourg, accessed July 10, 2023, https://www.eeas.europa.eu/delegations/council-europe/major-progress-path-eu-accession-echr-negotiations-concluded-technical-level-strasbourg_en?s=51.
51. Significant Cyber Incidents, accessed September 20, 2023, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
52. Spending on cybersecurity worldwide from 2017 to 2022, accessed August 7, 2022, https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

53. The International Institute for Democracy and Electoral Assistance, Is e-voting currently used in any elections with EMB participation?, accessed August 15, 2022, https://www.idea.int/data-tools/question-view/742.
54. UK Parliament, House of Commons trends: E-petitions, accessed January 11, 2023, https://commonslibrary.parliament.uk/house-of-commons-trends-e-petitions/.
55. U.S. Department of Justice, Report On The Investigation Into Russian Interference In The 2016 Presidential Election, accessed May 5, 2023, https://www.justice.gov/archives/sco/file/1373816/download.

SANTRAUKA

KAIP VISUOMENĖS INTERESAS DALYVAUTI POLITINIAME PROCESE VEIKIA PUSIAUSVYRĄ TARP PRIVATUMO IR SAUGUMO KIBERNETINĖJE ERDVĖJE?

Elektroninė demokratija tampa vyraujančiu veiksniu mūsų kasdieniame gyvenime. Sąmoningai (naudodami elektroninio balsavimo, e-peticijų sistemas ir pan.) ar nežinodami (dalyvaudami diskusijoje socialiniuose tinkluose) piliečiai pradeda naudotis e. demokratijos privalumais. Nepaisant to, visapusiška e. demokratijos analizė grynai teisiniu požiūriu lieka beveik nepaliesta. Šiuo straipsniu siekiama prisidėti prie vykstančio diskurso apie e. demokratiją, ypatingą dėmesį skiriant subtiliai pusiausvyrai tarp saugumo ir privatumo kibernetinio saugumo kontekste. Be to, šioje sudėtingoje diskusijoje autorius įveda ir trečią elementą – visuomenės suinteresuotumą dalyvauti politiniame procese. Šių trijų elementų sąveikos supratimas ir analizavimas yra ypatingai svarbus e. demokratijos reglamentavimui.

Pirmoje šio straipsnio dalyje autorius didelį dėmesį skiria e. demokratijos ypatumams. E. demokratija, taip kaip ir demokratija, susiduria su sąvokos apibrėžimo problema. Mokslinėje literatūroje pastebima, jog įvairūs autoriai e. demokratijos sąvoką neatskiriamai naudoja su kitomis sąvokomis, kaip antai: virtuali demokratija, skaitmeninė demokratija ir pan. Be to, e. demokratijos sąvoka yra maišoma su kitomis, nors ir susijusiomis, sąvokomis, kaip e. vyriausybė, e. valdymas ir pan. Pačios e. demokratijos įdiegimas praktikoje priklauso iš esmės nuo e-demokratijos instrumentų poveikio. Kuo didesnis poveikis, tuo mažesnė tikimybė, jog bus sudarytos sąlygos tokios sistemos naudojimui. Pagrindinė rizika, su kuria susiduria e. demokratija yra kibernetinių incidentų pavojus. E. demokratijos instrumentų sutrikdymas sudarytų sąlygas tiek nutekinti piliečių duomenis, tiek pasikėsinti į valstybės suverenitetą, kadangi piliečiams būtų užkirsta (arba apribota) teisė į valstybės valdymą.

Antroje šio straipsnio dalyje autorius išanalizavo kibernetinio saugumo aspektus. Nors teisė į kibernetinį saugumą nėra visuotinai pripažinta teisė, valstybės, turėdamos pareigą apsaugoti savo piliečius nuo grėsmių, turi pareigą užtikrinti piliečių saugumą taip pat ir kibernetinėje erdvėje. Fizinių sienų nebuvimas nepanaikina šios valstybės pareigos ir pačiai valstybei tenka nuspręsti, kaip tai yra tikslingiausia padaryti. Vienas iš kibernetinio saugumo užtikrinimo veiksmingiausių būdų – nuolatinė prieiga prie piliečių elektroninių sistemų – susiduria su

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (28), 2023, p. 3-27

proporcingumo problema, t. y., balanso paieškos tarp visuomenės saugumo ir teisės į privatumą. Siekiant atsakyti į straipsnyje iškeltą klausimą, autorius išanalizavo visuomenės intereso dalyvauti valstybės valdyme svarbą; valstybės pareigą užtikrinti visuomenės intereso apsaugą bei tradicinių normų prisitaikymą prie naujos skaitmeninės realybės.

RAKTINIAI ŽODŽIAI

E. demokratija, kibernetinis saugumas, duomenų apsauga, teisė į privatumą.