https://doi.org/10.22364/iscflul.8.2.11

Irena Kucina, *Dr. iur., Associate Professor*
Faculty of Law, University of Latvia, Latvia
Head of the Office of the Presidential Advisers, Latvia
Adviser to the President of the State on Rule of Law and EU Legal Policy, Latvia

EFFECTIVE MEASURES AGAINST HARMFUL DISINFORMATION IN THE EU IN DIGITAL COMMUNICATION

Keywords: disinformation, digitalization, European Union, big data, rights to privacy, freedom of speech

Summary

Digitalisation has opened new technological horizons before society in terms of creating a better physical world and personal life. Impact of technologies on medicine, reduction of environmental pollution, resource savings and other areas is obvious. Digital technologies kept Latvian parliament (*Saeima*), government, public institutions, schools and business open or working remotely during pandemic to ensure running of the state, economy and society under restrictions and preventing close contact. Pandemic would have made our lives significantly harder 30 years ago.

Digital revolution is on the rise. Global data output is doubling every year. Just picture hundreds of thousands of *Google* searches and *Facebook* entries we generate every minute. They convey valuable information about what we think and experience.

It has also become apparent that technological euphoria has clouded our vision and we have failed to spot the threats to democracy, human rights and freedoms. Digitalisation come with great opportunities, but it also poses enormous risks, especially for democracy and rule of law.

On 15 December 2020, European Commission announced two new legislative proposals (proposals for regulation) – Digital Services Act[1] and Digital Markets Act[2]. Their main objective is to make internet safer for people who use it, in particular, for buying goods and services, and for the first time ever these regulations also contain provisions regarding reduction of threats to democracy and rule of law emanating from digital tools.

---

[1] Available: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0825&from=LV [viewed 24.01.2022.].

[2] Available: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0842&from=LV [viewed 24.01.2022.].

This paper analyses two significant legal risks associated with digitalisation that need to be mentioned: Big Data threats to fundamental human rights such as privacy (I) and threats to freedom of speech on social media (II), which are then evaluated from the perspective of interconnected legislative proposals announced by the Commission on 15 December 2020 (Digital Services Act and Digital Markets Act), followed by an assessment of how well they address (or not) the aforementioned risks (III). In conclusion, paper offers several proposals on how Latvia should address these issues during consultation process (IV).

1. Big Data and privacy risks

1.1. Big Data

Digitalisation generates Big Data.[3] Big Data comes from two main sources. Firstly, it is collected, and harvesting happens at an ever-increasing pace. And it is also generated by conflating the data – by stringing the data together to multiply its informational value.[4]

Big Data is characterised by three Vs: the enormous volume (*Volume*), enormous speed at which data is collected and processed (*Velocity*), and diversity (*Variety*).[5]

Big Data is primarily about the volume**.** Within the Social Media space, for example, *Volume* refers to the amount of data generated through websites, portals and online applications. *Volume* encompasses the available data that are out there and need to be assessed for relevance. *Facebook* has 2 billion users, *YouTube* 1 billion users, *Twitter* 350 million users and *Instagram* 700 million users. Every day, these users contribute to billions of images, posts, videos, tweets etc., thus generating huge volumes of data. It all becomes part of these large data sets.[6]

Collecting and processing speed (*Velocity*) reflects the rate at which data is produced. Staying with our social media example, every day 900 million photos are uploaded on *Facebook*, 500 million tweets are posted on *Twitter*, 0.4 million hours of video are uploaded on *YouTube* and 3.5 billion searches are performed in *Google*. Big Data helps these companies accept the incoming flow of data and at the same time process it fast, so that it does not create bottlenecks.[7]

Variety in Big Data refers to all data that has the possibility of getting generated either by humans or by machines (computers, gadgets, etc.). The most commonly added data are structured – texts, tweets, pictures & videos. However, unstructured data like emails, voicemails, hand-written text, audio recordings etc,

---

[3] Pääkkönen P., Pakkala D. Architecture and Classification of Technologies, Products and Services for Big Data Systems, Big Data Research. Vol. 2, Issue 4, December 2015, pp. 166–186. Available: https://www.sciencedirect.com/science/article/pii/S2214579615000027 [viewed 24.01.2022.].

[4] Ibid.

[5] Ibid.

[6] Understanding the 3 vs of Big Data – Volume, Velocity and Variety. 8 September 2017. Available: https://www.whishworks.com/blog/data-analytics/understanding-the-3-vs-of-big-data-volume-velocity-and-variety/ [viewed 24.01.2022.].

[7] Ibid.

are also important elements under *Variety*. *Variety* is all about the ability to classify the incoming data into various categories.[8] All this enormous diversity of data contributes to the *Variety* of Big Data.

The three Vs describe the data to be analysed. Analytics is the process of deriving value from that data for the user.[9]

1.2. Data sources

Big Data have significant impact on our social processes and personal life, and this influence is bound to increase even further. The question is: what do we want to extract or get from such data?

Data sources can be broadly attributed to two groups in terms of origin: data generated technologically, and data linked to humans. For example, modern supercomputers, and soon also quantum computers, are able to detect magnetic waves from distant galaxies, trace COVID-19 mutations or test strength of materials, and such data, which is technologically generated, collected and processed, is less sensitive from societal and legal point of view than non-anonymised data linked to humans. And that is as far as technologically-generated and anonymised human data will be analysed here.

However, when non-anonymised data about a particular person is being collected, stored and processed to identify their behaviour, location, contacts with others, or biological features, that is an entirely different case. It is no longer a concern from scientific and technological perspective, it becomes a concern for the society, democracy, politics and law.

1.3. Rights to privacy

Democratic countries that uphold the rule of law have created privacy safeguards.

These rights were first described by Louis Brandeis, associate justice on the Supreme Court of the United States, in his 1890 article "Right to Privacy" for the Harvard Law Review.[10] "The right to be left alone", coined by Brandeis, is a perfect representation of the purpose and intent of these rights. They are about the right to be left alone, to be yourself.

Although this article was published 130 years ago and, while the practical and theoretical scope of privacy laws has significantly broadened and deepened, their content, purpose and mission has remained unchanged. These rights, which are closely connected with human dignity and subjectivity, give you an opportunity

---

[8] Understanding the 3 vs of Big Data – Volume, Velocity and Variety. 8 September 2017. Available: https://www.whishworks.com/blog/data-analytics/understanding-the-3-vs-of-big-data-volumevelocity-and-variety/ [viewed 24.01.2022.].

[9] Volume, velocity, and variety: Understanding the three V's of big data, 2018. Available: https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/ [viewed 24.01.2022.].

[10] Warren S., Brandeis L. The Right to Privacy. Harvard Law Review, 4, 193, 15 Dec. 1890.

to be yourself, have personal space where you can be free from outside influences or can independently form your beliefs, identity and be treated with respect as a subjective individual and equal member of society who interacts with public domain and is part of a public discourse.[11]

In Latvia, such rights are guaranteed by Art. 96 of the constitution, *Satversme*. Without these rights, democracy, which is essentially meant to provide any person a chance to establish themselves in the public domain, will simply not work. Any undue restrictions of such rights may undermine the constitution, government and social processes of democratic countries, which uphold the rule of law.

1.4. Threats to privacy rights

Digital surveillance of humans or *tracking*, or as one might describe it spying, which allows compiling and aggregating huge Big Data sets, human profiling[12], which makes use of algorithms to predict human behaviour in different information contexts (*prediction*) and uses such predictions about human response to create custom information contexts or filter bubbles to trigger the desired human reactions (micro-targeting) are at the core of the business model employed by big well-known global online platforms.[13]

Threats to privacy rights in digital domain come from such business models. In today's world, once you go online, you are constantly monitored and profiled. It is virtually unavoidable[14], unless you are ready to significantly limit your online opportunities, which means that you are actually excluded from social interactions. Surveillance, conducted against your rights to privacy, serves a very clear purpose from the perspective of global online platforms, their business and other entities. The purpose is to label you, or micro-target you into specific behaviour.

---

[11] Benn S. Privacy, freedom, and respect for persons. In: Schoeman F. (ed.). Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, 1984, p. 223.

[12] Definition of 'profiling' in Art. 4(4) of the General Data Protection Regulation: 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

[13] Zubov S. The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power. New York, Public Affairs, 2019.

[14] Following the adoption of EU General Data Protection Regulation and CJEU judgement (of 1 October 2019 in the Case C-673/17, Planet 49), online websites visited by users are now required to ask for visitor's consent for cookies that trace online activities of users. Definition of 'consent' in Art. 4(11) of the General Data Protection Regulation: 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. It is debatable from the human rights perspective, whether consent without an actual alternative is legally a real choice, especially when there are sites that you can actually visit only when *clicking* 'agree' (for example, public institutions or private monopolies). Anyhow, this should be subject to 'meaningful consent' from the user and pushing 'agree' should not be considered adequate consent. Collection, Targeting and Profiling of Consumers Online. BEUC Discussion paper, 2020. Available: https://www.beuc.eu/publications/2010-00101-01-e.pdf [viewed 24.01.2022.].

People are usually oblivious or unaware of such manipulation. It can be used to trigger particular financial behaviour, but it becomes very dangerous once it is used to influence personal or collective political beliefs and corresponding political action. It raises questions about compatibility of such business models with democratic governments and rule of law.[15] It is a major data protection challenge, which prevents us from finding an efficient solution.[16]

2. Social media threats to freedom of speech

Global digital space has created numerous new opportunities at the local, national, regional and global level. This includes all types of political activism, cultural exchanges and human rights advocacy. Global online conglomerates have created human communication platforms. Most people, public bodies and private businesses prefer to communicate mostly online. Until now, there has been very little regard for the fact that global communication platforms created by these global conglomerates are run according to house rules defined by their owners.

This has led to potential abuse of global communication platforms: to spread hate speech or child pornography, incitement to violence, and other activities that are prohibited in the real world. Authorities can apply fines and even criminal penalties for such violations. However, when it comes to digital domain, the lines between freedom of speech, expression and privacy are less distinct, more blurred and subject to great many interpretations.

Democratic countries that maintain the rule of law do guarantee freedom of speech and expression. In the case of Latvia, it is the Art. 100 of *Satversme*. It is one of the fundamental rights available to citizens. Respect for it is a precondition for efficient democracy as a form of government. Notably, like many other human rights, this freedom is not absolute. Its scope is defined in Art. 116 of *Satversme*. It may be restricted to achieve legal balance with the rights of others and alleviate real and direct threats to public safety.[17]

Eradication of hate speech serves public interests, but it is equally as important to ensure that digital domain does not restrict freedom of speech. Any such restrictions should only be applied as the last resort. As European Court of Human Rights indicates in one of its judgements, freedom of speech also applies to information and ideas "that offend, shock or disturb the State or any sector of

---

[15] Cf.: Bennett C. J., Smith O.-M. Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities. 2019. Available: https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf [viewed 24.01.2022.].

[16] Witzleb N., Paterson M. Micro-targeting in Political Campaigns: Political Promise and Democratic Risk. Available: https://www.researchgate.net/publication/344839124_Micro-targeting_in_Political_Campaigns_Political_Promise_and_Democratic_Risk [viewed 24.01.2022.].

[17] Constitutional Court judgement in Case 2003-05-01, (22).

the population".[18] This means that any attempts to restrict free speech that does not violate rights of other persons are to be considered a violation of people's right to freedom of expression.

Large online platforms, global digital conglomerates are part of private businesses mostly headquartered in the US and governed by American laws, which allow them to **control** and delete content uploaded by users when they *suspect* that such content contains, for instance, false medical facts, hate speech or incitement to violence.

However, user-generated content uploaded to these websites is also part of Latvia's public discourse, i.e., part of democratic and political process.[19] Any lines between legal and illegal content can only be defined by legislature democratically elected by people. Furthermore, such lines may differ from one country to another. Given its past experience, Latvian society is extremely sensitive to any freedom of speech issues.

Global online giants have created digital communication platforms that have become the main communication media for people. Without them our civic participation is almost impossible. These companies "govern" our online social lives.[20] The extent to which a democratic state can restrict its citizens' rights to free speech is expressly defined in constitution. Any such restrictions are an exclusion and impact determination should remain a prerogative of independent courts,[21] whereas private companies, these enormous global internet giants, are unrestricted in their choice of how to limit freedom of speech because they operate in an unregulated or grey area. Their direct, and more importantly, indirect influence on humans, political discourse in a democratic society and personal communication is immense. Global online giants have amassed huge power. Power, which is beyond the reach and control of democratic institutions.

Hence, the very fact that global internet giants are controlling key democratic discourse platforms by deleting, preventing or otherwise limiting free speech on their privately owned websites that are designed for profit purposes is quite alarming.[22] It is a threat to common fundamental values and democracy and rule of law as a form of government.

President of Latvia Egils Levits has noted that social media algorithms or unknown anonymous individuals should not be allowed to decide how to limit the free speech provided by *Satversme* of Latvia. In a democratic country governed

---

[18] ECtHR judgement in Handyside v. United Kingdom, C-5493/72, (49).

[19] Comp.: Levits E. National information and democratic discourse space as an element of democratic government. Jurista Vārds, Issue 9, 1 March 2016.

[20] Suzor N. P. Lawless: the secret rules that govern our digital lives and why we need new digital constitutions that protect our rights. Cambridge University Press, 2019. Available: file:///C:/Users/konto-2/Downloads/Suzor%202019%20Lawless-2018-11-19T13_55_25.098Z.pdf [viewed 24.01.2022.].

[21] See: Šņepste I. Default restrictions on free speech online: concept and legitimacy. Jurista Vārds, Issue 1, 5 January 2021.

[22] Comp.: Stjernfelt F., Lauritzen A. M. Your Post has been Removed. Springer Open., 2020, p. 83. Available: https://link.springer.com/content/pdf/10.1007%2F978-3-030-25968-6.pdf [viewed 24.01.2022.].

by the rule of law, legal boundaries of free speech are defined by legislature, whereas courts decide whether such boundaries have been overstepped.[23]

That is why Europe has moved from a debate on necessity to regulate[24] internet business, and especially global online conglomerates or the big online platforms, to action. It has become rather apparent that traditional data protection paradigms, including the most sophisticated forms of data protection such as the General Data Protection Regulation, are falling short of protecting privacy, free speech and thus also the democracy itself.

3. Digital Services Act and Digital Market Act packages

European Commission announced these two proposals for regulation, the Digital Services Act and Digital Market Act, on 15 December 2020.

Digital Services Act package defines basic requirements and principles applicable to online platforms and how they publish and distribute content. In addition to offering a framework for holding platforms liable for inappropriate content posted by their users, it also defines the main features of content moderation (a term substituting the less appealing censorship[25]) policies and their enforcement.[26] Proposal, *inter alia*, provides:

- actions against illegal content posted by users, including mechanisms allowing users to notify presence of such content and platforms to cooperate with trusted flaggers;
- protection of recipients of the service and their right to appeal content blocking;
- partial algorithm transparency obligation for online platforms.

---

[23] President of Latvia: we must prevent attempts to appropriate freedom of speech. Available: https://www.president.lv/lv/jaunumi/zinas/valsts-prezidents-varda-un-makslas-briviba-nedrikst-tikt-sasaurinata-26622#gsc.tab=0 [viewed 24.01.2022.].

[24] Dobber T., Ó Fathaigh R., Zuiderveen Borgesius F. J. The regulation of online political micro-targeting in Europe. Internet Policy Review. Vol. 8, Issue 4, 31 December 2019. Available: https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe [viewed 24.01.2022.].
Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020. Available: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0825&from=en [viewed 24.01.2022.].
Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020. Available: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0842&from=en [viewed 24.01.2022.].
Dobber, T., Ó Fathaigh, R., Zuiderveen Borgesius, F. J 2019.

[25] See also: Stjernefelt F., Lauritzen A. M. *Facebook* and *Google* as Offices of Censorship. 2020. Available: file:///C:/Users/konto-2/Downloads/Facebook_and_Google_as_Offices_of_Censorship.pdf [viewed 24.01.2022.].

[26] Barata J. The Digital Services Act and the Reproduction of Old Confusions. 2 March 2021. Available: https://verfassungsblog.de/dsa-confusions/ [viewed 24.01.2022.].

Notably, Regulation offers specific and more stringent requirements for big online platforms, as opposed to online business of other sizes, because these huge platforms are the biggest *users* of tracking, profiling, prediction and micro-targeting tools. They are defined as very large online platforms "that provide services to at least 10% of the Union's population" (Art. 25).

Digital Market Act, *inter alia*, stipulates criteria for designating very large online platforms as gatekeepers who control access:

- dominant market position, significant impact on internal market and presence in several Member States;
- strong intermediary power, i.e., wide reach to masses of users;
- it has (or is likely to acquire) entrenched and durable position on the market, i.e., secure long-term position.

Providers (mainly global internet giants) designated as gatekeepers are required to ensure fair conditions for all, especially small and medium size enterprises and start-ups. For example, to prevent online search engines like *Google* from 'pushing up' its products or products marketed by its affiliated companies and partners in the search results.

Commission's proposals are currently being debated in a number of European countries. Latvia is not yet among them. There is a considerable number of critical voices. According to them, there are two major conceptual weaknesses:

Firstly, Digital Services Act is focused on removing illegal content, with online providers having primary responsibility for such removal. In other words, providers are responsible for detecting illegal content posted by their users. Other users may flag such content for provider. They are called trusted flaggers. Companies can search for it themselves, which raises an immediate question: are these companies now allowed in fact to censor the content they upload? Is it compatible with free speech, which in democratic countries upholding the rule of law is regulated by democratically elected legislature? It must be considered that almost any decision to label content illegal and delete it may be contested on the grounds of legitimacy of such assessment. Should we really let algorithms make such legal determination?[27] And how would appeal procedures be set up considering the huge volume of potential protests? How does the rule of thumb or the existing list of banned words, which is not publicly available anywhere and is being used by algorithms of these platforms, fit into the concept of rule of law, given that it may lead to self-censorship undesirable in free and democratic society?[28]

---

[27] Use of algorithms in AI-assisted adjudication, comp: Kucina I. Algorithms in Courts and Predictive Justice. In: Iliopoulos-Strangas J., Levits E., Potacs M., Ziller J. (Hrsg.): Die Herausforderungen der digitalen Kommunikation für den Staat und seine demokratische Staatsform [The Challenges of Digital Communication for the State and its Democratic State Form]. Nomos, Baden-Baden; Stämpfli, Bern; Sakkoulas, Athens, 2021.

[28] Comp.: Benesch S. But *Facebook*'s Not a Country. How to Interpret Human Rights Law for Social Media Companies. Yale Journal on Regulation Online Bulletin, 2020. Available: https://digitalcommons.law.yale.edu/jregonline/3/ [viewed 24.01.2022.].

Secondly, European Commission failed to muster sufficient courage (with a little nudge from lobbyists, most probably) to impose any serious restrictions, or better yet, ban, on profiling and micro-targeting.[29] As argued previously, digital human surveillance infrastructure with tracking and profiling that feed into micro-targeting is designed to infringe upon our privacy and find better handles for manipulating our behaviour. The very foundations of democracy are attacked, whenever these tools are directly or indirectly applied to achieve political influence.

However, one of the main achievements of the Digital Market Act is that it, albeit carefully, does address the issues surrounding surveillance, profiling and micro-targeting systems for the first time ever. Art. 29 of the Act stipulates a specific obligation in case of very large online platforms to specify in their terms and conditions the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters that they may have made available, including at least one option which is not based on profiling. Users would benefit from greater transparency and opportunities to determine the extent of influence that very large internet platforms have over their choices. That is a large step forward in solving this rather complex problem.

The scope of the Digital Services Act is also raising some issues. Articles 5 and 14 apply to all kinds of services offered by platforms – not only social media, but also e-mails, cloud services, and so on. Does that mean censorship will also apply to private e-mails and information stored by users on cloud servers?[30]

Neither of the new legislative initiatives talks about accountability of very large internet platforms towards users for leakage of data. User information of 533 million *Facebook* users, including personal data and phone numbers, was leaked online in early April of 2021.[31] How was *Facebook* held liable? Did it have to notify its users about data leakage? Can users claim from *Facebook* a compensation for moral and material damage?

4. What should Latvia do?

Like any other European Union Member State, Latvia is about to embark on a digital transformation. European Union is planning to invest major funds into digital transformation of Member State economies, work environments, communications and other systems.

What should Latvia do in this regard?

---

[29] At a Glance: Does the EU Digital Services Act protect freedom of expression? Available: https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/ [viewed 24.01.2022.].

[30] Ibid.

[31] 533 million *Facebook* users' phone numbers and personal data have been leaked online. Business Insider, 3 April 2021. Available: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 [viewed 24.01.2022.].

First of all, it should keep in mind that digitalisation is not just a technical exercise, there is also the social and legal dimension to it. Legal scientists should ensure that transformation positively benefits society and protects it from any adverse effects.

Secondly, investment decisions linked to digitalisation should consider the existing and growing trend of regulating digital environment in a way which safeguards individual rights to privacy from eroding and protects independent, autonomous decision-making. Current business models that are based on user tracking and conditioning through micro-targeting will most probably have to be discontinued in near future, although the above acts of the EU have been rather sparing towards existing practices.

Thirdly, instead of just waiting for 'things to happen', going with the flow, Latvia can become a key stakeholder in this discussion and contribute through very clear position and being vocal about proposals of the European Commission. The author of the current article believes Latvia should take the position that protects users and their fundamental rights and freedoms, while online businesses must adopt, and European Union legislation should support business models that respect these rights and freedoms.

Fourthly, Latvia should find its own innovative national-level legal tools that clearly define the line between desired and undesired effects of the digital transformation. Legal environment and legal infrastructure are just as important in the economy as capital, labour and other financial factors. Latvia is well positioned to create a sustainable legal environment and ensure that digital transformation happens faster and offers better opportunities, thus also boosting the economy.

Conclusion

1. Digital revolution is on the rise. Global online giants which are mostly private companies have created digital communication platforms that have become the main communication media for people.
2. These enormous global internet giants are controlling key democratic discourse platforms by deleting, preventing or otherwise limiting free speech. And it is a threat to common fundamental values and democracy and rule of law as a form of government. Indeed, digitalisation comes with great opportunities, but it also poses enormous risks, especially for democracy and rule of law.
3. Considering the significance of these packages for the future European digital space, and rights and opportunities of users in this space, there is still a lengthy and scrupulous debate on various levels ahead of the adoption of these acts. Interests of the global online conglomerates and other internet players will certainly clash with individuals' interests. Citizens expect their privacy and freedom of speech to be regulated by national laws, which define the scope of these rights. They do not expect these matters to be governed by corporate interest and understanding of what is and what is not acceptable.

4. Latvia's and Europe's opportunity is to create an innovative legal approach towards accountability to platforms and make sure regulations protect their users instead of leaving them and their business models to their 'own devices' and creating regulatory framework around such *modus operandi*.
5. This is also a good time to lay down the fundamental constitutional elements, which will form the common European social fabric in the digital age. Debate on the digital constitutionalism is growing stronger by day. Rule of law and good governance are the basic elements of a new constitutional concept for managing and doing business online. These companies and their risks should be subject to a democratically legitimate scrutiny.

BIBLIOGRAPHY

Literature

1. Barata J. The Digital Services Act and the Reproduction of Old Confusions. 2 March 2021. Available: https://verfassungsblog.de/dsa-confusions/ [viewed 24.01.2022.].
2. Benesch S. But *Facebook*'s Not a Country. How to Interpret Human Rights Law for Social Media Companies. Yale Journal on Regulation Online Bulletin, 2020. Available: https://digitalcommons.law.yale.edu/jregonline/3/ [viewed 24.01.2022.].
3. Benn S. Privacy, freedom, and respect for persons. In: Schoeman f. (ed.). Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, 1984.
4. Bennett C. J., Smith O.-M. Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities. 2019. Available: https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf [viewed 24.01.2022.].
5. Dobber T., Ó Fathaigh R., Zuiderveen Borgesius F. J. The regulation of online political micro-targeting in Europe. Internet Policy Review. Vol. 8, Issue 4, 31 December 2019.
6. Kucina I. Algorithms in Courts and Predictive Justice. In: Iliopoulos-Strangas J., Levits E., Potacs M., Ziller J. (Hrsg.): Die Herausforderungen der digitalen Kommunikation für den Staat und seine demokratische Staatsform [The Challenges of Digital Communication for the State and its Democratic State Form]. Nomos, Baden-Baden; Stämpfli, Bern; Sakkoulas, Athens, 2021.
7. Levits E. National information and democratic discourse space as an element of democratic government. Jurista Vārds, Issue 9, 1 March 2016.
8. Pääkkönen P., Pakkala D. Architecture and Classification of Technologies, Products and Services for Big Data Systems, Big Data Research. Vol. 2, Issue 4, December 2015. Available: https://www.sciencedirect.com/science/article/pii/S2214579615000027 [viewed 24.01.2022.].
9. Stjernfelt F., Lauritzen A. M. Your Post has been Removed. Springer Open. 2020. Available: https://link.springer.com/content/pdf/10.1007%2F978-3-030-25968-6.pdf [viewed 24.01.2022.].
10. Stjernefelt F., Lauritzen A. M. *Facebook* and *Google* as Offices of Censorship. 2020. Available: file:///C:/Users/konto2/Downloads/Facebook_and_Google_as_Offices_of_Censorship.pdf [viewed 24.01.2022.].
11. Suzor N. P. Lawless: the secret rules that govern our digital lives and why we need new digital constitutions that protect our rights. Cambridge University Press, 2019.

Available: file:///C:/Users/konto-2/Downloads/Suzor%202019%20Lawless-2018-11-19T13_55_25.098Z.pdf [viewed 24.01.2022.].
12. Warren S., Brandeis L. The Right to Privacy. Harward Law Review, 4, 193, 15 December 1890.
13. Witzleb N., Paterson M. Micro-targeting in Political Campaigns: Political Promise and Democratic Risk. Available: https://www.researchgate.net/publication/344839124_Micro-targeting_in_Political_Campaigns_Political_Promise_and_Democratic_Risk [viewed 24.01.2022.].
14. Zubov S. The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power. New York, Public Affairs, 2019.

Legal acts

15. Digital Services Act. Available: https://eurlex.europa.eu/legalcontent/LV/TXT/HTML/?uri=CELEX:52020PC0825&from=LV [viewed 24.01.2022.].
16. Digital Markets Act. Available: https://eurlex.europa.eu/legalcontent/LV/TXT/HTML/?uri=CELEX:52020PC0842&from=LV [viewed 24.01.2022.].

Court practice

17. Judgment of the European Court of Justice (Grand Chamber) of 1 October 2019. Case C-673/17. Planet49. (ECLI:EU:C:2019:801). Available: https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=40437623 [viewed 24.01.2022.].
18. Judgement of the European Court of Human Rights of 7 December 1976. Handyside v. United Kingdom. Application No. C5493/72. Available: https://www.bailii.org/eu/cases/ECHR/1976/5.html [viewed 24.01.2022.].
19. Judgment of Constitutional Court of Latvia of 29 October 2003. Case 2003-05-01. Available: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2003-05-01_Spriedums.pdf [viewed 24.01.2022.].

Other materials

20. Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020. Available: https://eurlex.europa.eu/legalcontent/LV/TXT/HTML/?uri=CELEX:52020PC0825&from=en [viewed 24.01.2022.].
21. Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020. Available: https://eurlex.europa.eu/legalcontent/LV/TXT/HTML/?uri=CELEX:52020PC0842&from=en [viewed 24.01.2022.].
22. At a Glance: Does the EU Digital Services Act protect freedom of expression? Available: https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/ [viewed 24.01.2022.].
23. President of Latvia: We must prevent attempts to appropriate freedom of speech. Available: https://www.president.lv/lv/jaunumi/zinas/valsts-prezidents-varda-un-makslas-brivibanedrikst-tikt-sasaurinata-26622#gsc.tab=0 [viewed 24.01.2022.].
24. Understanding the 3 vs of Big Data – Volume, Velocity and Variety. 8 September 2017. Available: https://www.whishworks.com/blog/data-analytics/understanding-the-3-vs-of-big-data-volume-velocity-and-variety/ [viewed 24.01.2022.].

25. Volume, velocity, and variety: Understanding the three vs of big data. 2018. Available: https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/ [viewed 24.01.2022.].
26. 533 million *Facebook* users' phone numbers and personal data have been leaked online. Business Insider. 3 April 2021. Available: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 [viewed 24.01.2022.].