RUDN Journal of Sociology. ISSN 2313-2272 (print), ISSN 2408-8897 (online)
Вестник РУДН. Серия: СОЦИОЛОГИЯ
2023 Vol. 23 No. 4 851–865
http://journals.rudn.ru/sociology

СОЦИОЛОГИЧЕСКИЙ ЛЕКТОРИЙ

SOCIOLOGICAL LECTURES

DOI: 10.22363/2313-2272-2023-23-4-851-865
EDN: DLIPUS

Sociological study of cyber threats as an integrated part of the general data protection regulation*

M.A. Muqsith[1], V.L. Muzykant[2], R.R. Pratomo[1]

[1]Universitas Pembangunan Nasional Veteran Jakarta, Indonesia University,
R.S. Fatmawati Raya St., Depok city, West Java, Indonesia, 12450

[2]RUDN University, Moscow, Russia,
Miklukho-Maklaya St., 6, Moscow, 117198, Russia

(e-mail: munadhil@upnvj.ac.id; vmouzyka@mail.ru; rizkyridho0897@gmail.com)

Abstract. Sociology studies society and the patterns of its development, social processes, institutions, relations, structures, communities and certain cultural values which determine its development. Sociology also studies human behavior — how it affects society, and how people behave in social groups. There are many understandings of sovereignty in academic circles but mainly as absolute and hierarchical. As time passes, the concept of sovereignty, which prioritizes territory, has begun to lose relevance due to massive technological developments. In the context of technology and national security, territorial rules are irrelevant for three reasons: technology makes consistent and predictable territorial definitions difficult, data often moves in ways unrelated to the interests of users and legislators, and technology makes it easier for public and private actors to circumvent territorial rules, often without detection [12]. Another consequence of technological development is new actors with strong international influence due to globalization, free markets, and technological developments. Of all these actors, the most interesting are multinational companies. They do not operate on a territorial basis, which creates problems of jurisdictional asymmetry, overlap and control rather than of sovereignty in its formal sense [40]. Is sovereignty still relevant for the state? Since the advent of the Internet, the relevance of the nation-state concept has been questioned, and state actors have gradually lost their dominance. The Internet supports many international actors, and technology companies are the most significant. Their domination creates economic, legal, political, and social challenges; thereby, the state tries to regulate technology companies. The authors argue that the state sovereignty is still relevant despite many arguments saying otherwise. The paper

The article was submitted on 28.07.2023. The article was accepted on 16.10.2023.

explains the relevancy of the state sovereignty by presenting two cases: the General Data Protection Regulation (GDPR) and the New Media Bargaining Code (NMBC). The nation-state demonstrates its sovereignty by the law affecting national companies; thus, showing that the state can restrain the power of technology companies, i.e., state sovereignty is still relevant in the contemporary era.

Key words: cyber threats; data sovereignty; digital era; technology companies; General Data Protection Regulation (GDPR); New Media Bargaining Code (NMBC)

The principles of territoriality and state hierarchy appear at odds with the pervasive, flexible, and ever-changing constellation of global digital networks. Externally, sovereignty implies that each state is independent and is formally equal to others. Globalization erodes the meaning of state sovereignty due to new 'feudal lords' on a global scale. One thing that makes the multinational company's position unique is data. The saying 'data is the new oil' is true. When individuals search for information, they provide data for Google's algorithms to analyze. With patterns like this, algorithms can predict people's preferences according to their new data [54], which creates 'surveillance capitalism' [45]. There are several dominant technology companies (Alphabet, Meta, Amazon, Apple, and Microsoft), especially Alphabet and Meta: the former owns YouTube — the world's largest video streaming platform; Meta controls three social media platforms [47]. These platforms dominate public use and threaten the state authority and sovereignty. Therefore, several regulations were introduced to control the power of technology companies, such as the European Union's General Data Protection Regulation (GDPR) and the Australian government's News Media Bargaining Code (NMBC). For instance, GDPR encourages companies to develop information governance frameworks, use internal data, and keep humans in the loop in decision-making. Certainly, GDPR has side effects, but increases trust, standardization, and reputation of institutions [70]. GDPR manifests extraterritoriality, which can be legitimized by certain fundamental rights obligations [57].

Most studies prove the significant impact of the GDPR and NMBC regulations. However, one thing not discussed is what such regulations imply for the state sovereignty, how countries assert their sovereignty and compete to change and adapt [38]. The state still strives to prove its territorial sovereignty over technology companies, which is why today sovereignty includes digital one, and states have the right to assert their control in virtual worlds as based on physical constructs [44]. The article considers the state's efforts to demonstrate its sovereignty, focusing on GDPR in the European Union and NMBC in Australia: GDPR demands significant data protection safeguards, poses new challenges and opens new opportunities for organizations worldwide; NMBC brought regulation in rulemaking, changing it from reactive to systematic [6].

It seems that technology companies and the state fight for dominance and control of data. According to Antonio Gramsci, hegemony is a concept that

can explain two things: how the state apparatus or political society can force (with law, police, army, and prisons) to agree with the status quo; and how the dominant economic group uses the state apparatus to maintain the status quo [32]. Globalization questions the state's status quo as the sole owner of sovereignty, which is still trapped in the territorial paradigm. Globalization and technological developments bring new challenges: dematerialization (everything is paperless), de-temporalization (instant communication), and deterritorialization (not boundaries and geographical distances) of online activities and interactions [1]. Even if sovereignty encompasses the digital and there are physical factors such as ownership of company data banks [44], this does not prevent the state hegemony from eroding in international politics, in which technology companies become dominant actors.

The way for technology companies to achieve their hegemony is through normal means. According to Gramsci, "the exercise of 'normal' hegemony… is characterized by a combination of power and consent, which balance each other reciprocally without overly dominating power over consent. Indeed, efforts are always made to ensure that coercion will appear to be based on majority consent" [31]. When the Internet was invented, the world started to change — the power paradigm is evolving for data, especially personal data, becomes a new source of hegemony providing multi-faceted benefits. The processing of personal information became the newest form of bioprospecting, as entities of all sizes compete to discover new patterns and extract their market value [14]. For instance, Alphabet and Meta, two leading technology companies, have huge data stores — the data from billions of users cannot be managed by the traditional systems of physical and legal control; its constitutive differences render the state power, which animates them impotent, if not obsolete [36].

Dominant position of technology companies

Technology companies have a broad impact on society — their services make people's lives easier. For instance, social media allows to communicate, interact, share knowledge and moments with many people beyond time or distance. It is also easier for us to search for information due to the developed search engines. Meta and Google are the two most dominant technology companies. Meta has three social media platforms that are still people's favorites (Fig. 1) — Meta holds more than five billion people's data that can be used for market purposes.

Google is the largest search engine platform in terms of market: until August 2023, 91.85 % of the market was controlled by Google, i.e., people depend on the Google search engine to find information, and it would be difficult for them to switch to other platforms. Moreover, Google make things easier, thus, holding a very strong bargaining position in society: Google has YouTube, which is the main platform for free training, developing knowledge or watch various funny videos. There are 2.562 billion active YouTube users.

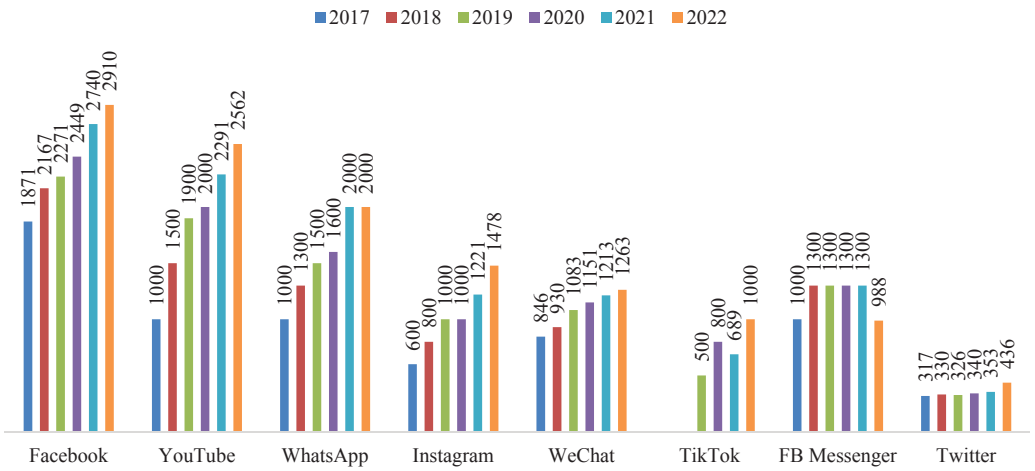

Figure 1. Social media users (2017–2022); WeAreSocial.org

The growth graph of the social media and Internet users is also in line with the population growth (Fig. 2). From 2017 to 2022, the world population increases by more than 400 million; however, the growth of Internet and social media users was much more significant due to benefitting the global society: develop knowledge of political issues [7], represent social revolutions [62], and promote goods and services [18]. Based on the data about social media users, Facebook and Instagram[1], WhatsApp and YouTube are the four largest platforms owned by Meta[2] and Alphabet, thus, holding and using most of the world's population data.

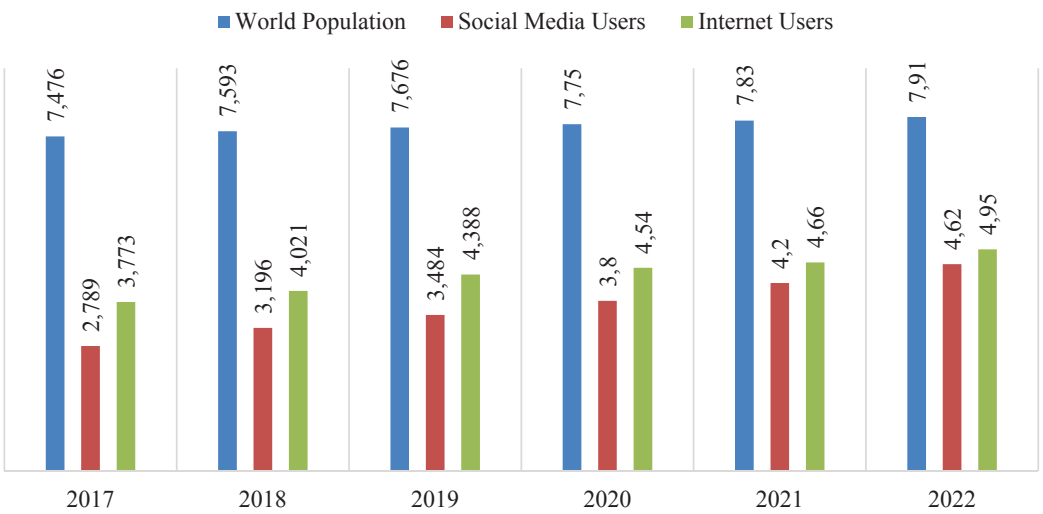

Figure 2. World population, Internet, and social media users (2017–2022)

[1] Both forbidden in the Russian Federation
[2] Forbidden in the Russian Federation

Service users became a rich source of data for technology companies, and markets with a high reliance on data can win: the more data the company has, the better its products are [49]; network externalities and the rise of social media allow technology companies to monopolize [22]; large databases (Big Data) enable them to get business benefits [68]. Technology companies can exercise monopoly because of data-driven network effects: companies provide their services for free in exchange for data to use for their benefit; process the data they get to create new services or more personalized advertising, based on the real-time data from their users. Thus, large technology companies serve as nodes of the digital economy and future technology infrastructure. The power of individual and collective technology companies manifests itself in their capacity to privatize information, act as indispensable platform gatekeepers, set and maintain technological and social standards. Suppose business success is based on collecting as much data as possible to feed algorithms based on the most representative data — then Google, or Amazon are the most successful when all potential users exclusively use their platforms [20].

However, their monopoly is offset by their huge impact on society. As more and more of our activities are digitized, the resulting Big Data proves to be a powerful tool for curing diseases, feeding the hungry, reducing gender inequality, strengthening national security, and improving environmental and disaster response [49]. The social media platforms owned by Meta and Google have provided benefits to MSMEs who sell their wares on the social media; the rural SMEs that are members of the social media business networks tend to show higher turnover and sales compared to rural and urban SMEs that are not members [63]. Google and Meta change the world in various perspectives — economic, political, social, and cultural. People become dependent on the above-mentioned services, especially on advertising, social media and information. Over time, technology companies have become more powerful, for instance, in terms of the GDP: in 2021, Meta's market cap was $939 billion, which exceeds the GDP of the Netherlands, Saudi Arabia, Turkey, and other countries [66]; Apple, Microsoft, Alphabet, Amazon, and Meta earned $1.4 trillion in revenue, on par with Brazil and ahead of Spain and Indonesia. Most of technology companies' income comes from advertising: Google dominates search advertising, and Facebook has a dominant and still growing share of online display advertising, especially mobile [5]. In 2019, Google and Facebook accounted for over 60 % of all US digital advertising spending and 33 % of all US advertising spending [52], i.e., businesses rely on advertising from Google and Facebook to gain visibility for their products.

The news media is one of many relying on advertising in Google and Facebook to generate audience traffic. They place advertisements at a certain price, hoping that many netizens will visit their website or page. One study found that 24 % of news companies get their traffic from the social media, whereas another 67 % come directly or from searches to their websites [55]. Nevertheless, the news media organizations have begun diversifying their distribution strategies and associated business models

in response to the Facebook's algorithm changes [51]. There were 10 million active advertisers on Facebook in the third quarter of 2020, which explains why Google and Meta dominate the digital landscape. The winner-takes-all principle makes technology companies ambitious to dominate various economic lines to increase profits. Their strategies typically include the creation of proprietary standards and platforms; collection and use of large amounts of users' data; product bundle; building large-scale infrastructure, parts of which are leased to other companies; strategic acquisitions; trademark and intellectual property litigation (trademarks and patents); regulatory and tax arbitrage; political lobbying [5]. Google's business unit YouTube accounted for $15 billion in 2019 (roughly 10 % of Google's revenue). Meta's social media platforms WhatsApp and Instagram provide about $20 billion in annual revenue for Facebook, nearly a quarter of Facebook's sales [53].

The bargaining power that Meta and Google have is so great that it can influence the state policy. According to Schwarz, interactions on Facebook are so intense that they leverage the data they collect to maximum advantage and influence the core political decisions; Facebook can discipline its users if they break the rules; digital platforms move towards decentralized governance — intensive legislation, administration of justice and punishment, eclectic instruments of government and legitimacy consisting of algorithms, proletarian judicial work, and government documents. Google and Meta have a lot of data that can be used for any purposes. It could be said that they can create their own cyber rules with this power, and this power will continue to grow, especially with the development of artificial intelligence [41].

GDPR: Reaffirming state sovereignty

This is why the state must do something so that technology companies do not become dominant actors. Today national governments are no longer relevant, because other actors make them share power — international organizations, transnational companies and non-governmental organizations, which erode the Westphalian system. However, if we talk about sovereignty, the state still has the power to enforce its sovereignty as long as it operates within its jurisdiction, including the digital realm. Digital sovereignty means governing citizens and foreigners, usually companies offering services worldwide [11]. The Internet is not a certain place removed from our world — like the telephone, telegraph and smoke signals, it is a medium of communication [25]. Because states naturally have jurisdiction, they use laws to demonstrate their sovereignty. Any country is sovereign if recognized as a holder of 'equal legal status' in the international community [23].

Today sovereignty is eroded by globalization and the Internet. Indeed, globalization has succeeded in questioning the concept of sovereignty as centralized in the state. Economic, technological and cultural changes have significantly affected governmental activities, the cumulative effect of which is a reduced efficiency of those levers of command and control that have been a common feature of the

modern nation-state [46]. Now we live in a globalized world, and state control is not as extensive as it was hundreds of years ago: users have control over what they can and cannot do with their smartphones and their data.

Some say that sovereignty, globalization, and democracy overlap. The ongoing expansion of democracy and globalization within the sovereign state system has placed tensions and pressures on all three [59]. This makes sovereignty more fluid as it seeks to find a certain formula in an increasingly contested world. As a result, sovereignty has become obsolete in its descriptive capacity and is rarely applied to denote anything tangible [15]. However, in recent years, states have sought to redefine sovereignty with a strong position, particularly in regulation. The Cambridge Analytica case is a significant warning for the state to regulate systematically: it helped Donald Trump to win as Facebook submitted personally identifiable information of more than 87 million users to Cambridge Analytica [35]. Even though Cambridge Analytica had purchased tens of millions of Americans' data without their knowledge [42], this was a turning point for the state to start protecting people's data from misuse. In many cases, states have taken strong steps to regulate technology companies. The US government through the Federal Trade Commission (FTC) voted to approve a fine of Facebook of approximately $5 billion to resolve an investigation of the company's privacy violations [69].

Law enforcement is not always systematic but rather reactive. Although the state makes visible efforts to regulate the use of technology companies' data, these efforts are still not sustainable and systematic. The EU was the first to introduce a systematic regulation called the General Data Protection Regulation (GDPR). GDPR is a comprehensive regulation that governs the data use and allows consumers to control their data. The basic idea for creating GDPR was that being data sovereign means controlling one's digital destiny, which includes individual rights in data management and control, and economic, political, and social motivations and concerns. The law would effectively create a 'right to explanation' — users can request explanations about algorithmic decisions made about them [26]. In other words, sovereignty is transferred from technology companies to individuals with the state's help. In short, individuals have sovereignty over their data provided to technology companies. GDPR also emphasizes the rule of law: state entities and institutions still have legal power/sovereignty as long as the entity operates on its territory, i.e., this is a legal entity and the state has legal sovereignty [23] as the effect of sovereign claims made (practices of sovereignty, such as adopting laws, punishing lawbreakers, social exclusion, etc.) [21].

GDPR shows that the state sovereignty remains. There is a growing discourse that the government has no authority over cyberspace. When new technology emerges, its use is not regulated or is governed by old regulations. As more governments interact with this new technology, they seek to control it, and one of the powers only the state has is the legitimacy to use violence [67]. In other words, GDPR enables users, including the people of the EU, to question technology

companies about their use of data (so that to avoid its arbitrary use). Additionally, like multi-sided platforms, social networking business models rely on free or subsidized services for users [60]. However, the real purpose of GDPR relates to economy and power — to contain the concentrated market power and competitive distortions and to maintain consumers' trust [56]. With this new framework, GDPR will serve as a role model for other policy areas, in which the consequences of globalization and digitalization require new regulatory approaches to effectively protect values and standards [2].

What will happen when GDPR comes into effect? First, it will make tech companies rethink privacy and personal data. Many companies have already revised their data practices and taken a professional approach to handling personal data [33]. GDPR makes it more difficult for technology companies to do their usual things: from January 2021 to January 2022, the EU data protection authorities fined $1.2 billion for violations of the GDPR legislation [10]. After enacting GDPR in 2018, many companies have paid fines. As of August 20, 2023, GDPR issued 1,701 fines for about 4 billion euros, and of the five companies with the heftiest fines, Meta dominates. Second, the GDPR created a huge wave of similar regulations. The most common aspects of the globally replicated legislation are data subject rights, accountability requirements and data breaches, which have determined public interest and awareness about the use of personal data [8]. Many countries have more comprehensive regulations of data protection and accountability (for instance, in Indonesia, the Personal Data Protection Law refers to GDPR). Third, the Data Protection Agency can provide consultation and law enforcement against technology companies that violate regulations [19; 28].

Thus, GDPR fulfils the mission of limiting the arbitrariness of technology companies and defines the EU as the ultimate holder of sovereignty, which applies to companies and citizens within its sphere of influence. "GDPR is a fantastic start on really treating privacy as a human right" [29]. Regulation is needed, and the state has authority to ensure it with GDPR which sets clear standards for the world's largest market — no data controller can ignore them, and other governments are under pressure to improve their data protection standards so that to get access to the EU's digital market. GDPR broadens the scope of data protection so that it applies to any person or organization that collects and processes information related to the EU citizens, regardless of where they are located or where the data is stored [61].

NMBC: A more competitive market

The Australian government strives to regulate the dominance of technology companies with an approach different from the EU GDPR. Australia is more focused on ensuring healthy competition between two technology companies, Meta and Alphabet, and the media. In other words, the emphasis is put on how the media in Australia are compensated for news coverage on Google and Facebook. The Australian government drafted a law requiring that Google and Meta pay

royalties to the media for news broadcasts on their platforms [13], i.e., the Australian government wants to protect the rights of its citizens, which are eroded by the domination of technology companies. According to Meta, the proposed legislation fails to address the nature of agreements between publishers and platforms [64]. According to Google, this bill does not consider what Google has been doing and "diminishes the already significant value that Google provides to news publishers, including sending billions of clicks to Australian news publishers for free every year worth US $218 million" [13].

Another difference with GDPR is that technology companies fight for their interests. For instance, on February 17, 2021, Meta demonstrated its ability to influence lawmaking by removing all news links from Facebook, leaving the Facebook page of the country's largest media company empty [50]. In January, Google ran a so-called 'experiment' that removed or demoted breaking news in the search results available to Australian users [43]. Meta and Alphabet act like a state, trying to demonstrate superiority over tech-illiterate, benevolent and trustworthy governments to users [30] and to convince the public that they cannot survive without their platforms.

However, the Australian government is not threatened by such Meta and Alphabet's steps and stresses that the government needs to make laws. First, cyberspace's political and technological meaning never rests on its non-territoriality: cyberspace consists of information networks that need networks of cables; political implications arise when physical objects merge with human rules and institutions. Second, the state does have the authority to regulate everything as long as the entity exists within its territory, including cyberspace. Additionally, there are complaints that the media suffers huge losses due to Meta and Alphabet. In mid–2020, News Corp Australia complained that "digital platforms have become the default conduit for many consumers", and snippets accompanying headlines in searches are more likely to result in users staying on the digital platform and not reading the publisher's content [27].

The state must ensure its citizens are happy and provide justice. The Australian government has no interest in allowing Meta and Alphabet to such great power as to disrupt stability. Regulation is a tool that technology companies use: "Australia makes rules for things you can do in Australia. That is done in our parliament. Our government does it" [64]. Australia has the authority and right to make fair regulations for its people. The laws are Australian, which means they can withstand the hegemony of Google and Facebook in this country.

Ultimately, the Australian government, Google and Facebook agreed to the NMBC Act, and each party believes to have won the battle, for instance, the Australian government claims this law is a victory for Australia as a fair deal. NMBC and similar reform agendas in other countries are just one example of a broader international push towards a more aggressive role for nation-states in the Internet regulation and platform governance [6]. However, one year after the law was enacted,

several parties protested and were dissatisfied with its implementation. Some media do not publish content on Facebook, and a group of mid-sized publishers explain this decision by the fact the Facebook and Google refused to pay for their work under the NMBC [39]. Apart from the debate about who benefits from this regulation, its implications could be useful for other countries as an example of a global movement from regulation that is ad hoc and relies on global platforms to do the 'right thing' towards a more interventionist approach with the formalized rules, policies, procedures, and sanctions for non-compliance.

The state hegemony as a dominant actor

Some authors believe that the concept and practice of sovereignty are no longer relevant, especially in the era of globalization which implies that sovereignty gets weaker, including in protecting itself [48]. Moreover, countries are dependent on other countries and investment of private companies, i.e., compromise their sovereignty to accelerate economic growth. It seems that in the long run, blockchain technology will undermine the sovereignty of nation-states and strengthen the transformation of global exchange and governance. Moreover, future sovereignty may become sovereignty not only of society but also of technology agents. Therefore, the state must treat technology companies as sovereign countries in the rapidly evolving world beyond the reach of regulators — the digital space [9].

Nevertheless, the state can still maintain its hegemony as the main actor in the international community by restraining the pace of technology companies with laws. As a result, sovereignty refers to having the authority and ability to make decisions about how people live and what things direct their lives (e.g., laws, policies, technology) [58]. Some things are the state's authority, such as making regulations that protect the interests of many parties. Sovereignty remains important because the only entity that has the right to introduce legal rules is the state. Moreover, the basic principle of sovereignty includes political notions of order inward (security, peace, hierarchy) and outward (equality of states, prohibition of interventions, etc.) [65]. Therefore, there is no room for corporations that transcend the state sovereignty, and only a few national companies operating in many countries can become truly transnational [3].

There has to be a strong reason for the state to do something, and states can justify their actions by a public threat. Privacy and monopoly issues is a threat to those affected: the state must act — make regulations and become a jury — so that people feel that the state exists and protects public interests [4]. However, this does not deny the fact that understanding sovereignty in a territorial context is a challenge in the digital era. But the state can adapt to current developments. Sovereignty in the digital world is more about the ability to act and apply Newton's third law: action equals reaction. Sovereignty associated with legal claims to autonomous governance from within and without outside interference is also evident in many cases of countries' dealing with technology companies. And territorial context

is still relevant [24] when considering where the technology company operates (In which state has offices and provides services). With the growth of power held by technology companies, there will be a struggle between the state and technology companies for control.

Sociology studies social norms, values, roles, statuses, opinions and many other phenomena that make up what we call "social life", in which the state tries to play the key regulatory role so that technology companies cannot do as they please. It is no exaggeration to say that the speed of technological progress depends on technology companies and changes our social life, and the state should continue demonstrating its power. However, the state must be careful: as technology develops, the power of technology companies will become more outstanding based on artificial intelligence, quantum technology, biotechnology, etc. In the future, technology will be a game changer in people's lives, and technology companies will be at the forefront of the innovation race. Countries must look for creative ways to maintain their hegemony and sovereignty.

References

1. Adams J., Albakajai M. Cyberspace: A new threat to the sovereignty of the state. *Management Studies*. 2016; 4 (6).
2. Albrecht J.P. How the GDPR will change the world. *European Data Protection Law Review*. 2016; 2 (3).
3. Bakan J. The invisible hand of law: Private regulation and the rule of law. *Cornell International Law Journal*. 2015; 48 (2).
4. Balzacq T., Léonard S., Ruzicka J. 'Securitization' revisited: Theory and cases. *International Relations*. 2016; 30 (4).
5. Barwise T.P., Watkins L. The evolution of digital dominance: How and why we got to GAFA. M. Moore, T.D (Eds.). *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*. Oxford University Press; 2018.
6. Bossio D., Flew T., Meese J., Leaver T., Barnet B. Australia's News Media Bargaining Code and the global turn towards platform regulation. *Policy & Internet*. 2022; 14.
7. Boulianne S. Social media use and participation: A meta-analysis of current research. *Information, Communication & Society*. 2015; 18 (5).
8. Breitbarth P. The impact of GDPR one year on. *Network Security*. 2019; 7.
9. Bremmer I. The Technopolar moment: How digital powers will reshape the global order. *Foreign Affairs*. 2021; November.
10. Browne R. Fines for breaches of EU privacy law spike sevenfold to $1.2 billion, as Big Tech bears the brunt. *CNBC*. 2022; January 17.
11. Chander A., Sun H. *Sovereignty 2.0. J. Transnat'l*. London; 2022.
12. Clopton Z.D. Territoriality, technology, and national security. *University of Chicago Law Review*. 2016; 83.
13. CNN Indonesia: Kronologi Akhir Perseteruan Google-Facebook vs Australia. 2021; February 24.
14. Cohen J.E. The biopolitical public domain: The legal construction of the surveillance economy. *Philosophy & Technology*. 2018; 31.
15. Conversi D. Sovereignty in a changing world: From Westphalia to food sovereignty. *Globalization*. 2016; 13 (4).
16. Creswell J.W., Creswell J.D. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE; 2016.

17. Crowe S., Cresswell K., Robertson A., Huby G., Avery A., Sheikh A. The case study approach. *BMC Medical Research Methodology*. 2011; 11 (100).
18. Erlangga H., Sunarsi D., Pratama A., Nurjaya Sintesa N., Hindarsah I., Juhaeri Kasmad. Effect of digital marketing and social media on purchase intention of Smes food products. *Turkish Journal of Computer and Mathematics Education*. 2021; 12 (3).
19. Euronews: Meta hit with €265 million fine by Irish regulators for breaking Europe's data protection law. 2022; November 28.
20. Flyverbom M., Deibert R., Matten D. The governance of digital technology, big data, and the Internet: New roles and responsibilities for business. *Business & Society*. 2019; 58 (1).
21. Foucault M. *Society Must Be Defended: Lectures at the Collège de France 1975–76*. Picador; 2003.
22. Fukuyama F. 30 years of world politics: What has changed? *Journal of Democracy*. 2020; 31 (1).
23. Geenens R. Sovereignty as autonomy. *Law and Philosophy*. 2017; 36 (5).
24. Glasze G., Cattaruzza A., Douzet F. et al. Contested spatialities of digital sovereignty. *Geopolitics*. 2023; 28 (2).
25. Goldsmith J.L. The Internet and the abiding significance of territorial. *Indiana Journal of Global Legal Studies*. 1998; 5 (2).
26. Goodman B., Flaxman S. European Union regulations on algorithmic decision-making and a "right to explanation". *AI Magazine*. 2017; 38 (3).
27. Grueskin B. Australia pressured Google and Facebook to pay for journalism. Is America next? *CJR*. 2022; March 9.
28. Gupta S. Google hit with $222M fine from Indian regulators over anti-competitive practices. *CTV News*. 2022; October 21.
29. Hamilton I.A. Microsoft CEO Satya Nadella made a global call for countries to come together to create new GDPR-style data privacy laws. *Business Insider*. 2019; January 24.
30. Heylen K. Enforcing platform sovereignty: A case study of platform responses to Australia's News Media Bargaining Code. *New Media & Society*. 2023. https://doi.org/10.1177/14614448231166057.
31. Hoare Q., Smith G.N. *Selections from the Prison Notebooks of Antonio Gramsci*. Lawrence & Wishart; 1971.
32. Holub R. *Antonio Gramsci: Beyond Marxism and Postmodernism*. Routledge; 1992.
33. Hoofnagle C.J., van der Sloot B., Borgesius F.Z. The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*. 2019; 28 (1).
34. Hyett N., Kenny A., Dickson-Swift V. Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-Being*. 2014; 9 (1).
35. Isaak J., Hanna M.J. User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*. 2018; 51 (8).
36. Johnson A. The Mechanics of sovereignty: Autonomy and interdependence across three cables to I celand. *American Anthropologist*. 2021; 123 (3).
37. Johnston M.P. Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries*. 2014; 3 (3).
38. Kavanagh C. Cybersecurity, sovereignty, and U.S. foreign policy. *American Foreign Policy Interests*. 2015; 37 (2).
39. Ketchell M. Publishers take on Facebook and Google for failing to pay up under the News Media Bargaining Code. *Conversation*. 2022; March 23.
40. Kobrin S.J. Sovereignty@Bay: Globalization, multinational enterprise, and the international political system. A.M. Rugman (Ed.). *The Oxford Handbook of International Business*. Oxford University Press; 2009

41. Kuner C., Svantesson D.J.B., Cate F., Lynskey O., Millard C. The rise of cybersecurity and its impact on data protection. *International Data Privacy Law.* 2017; 7 (2).
42. Lapowsky I. How Cambridge Analytica sparked the great privacy awakening. *Wired*. 2019; March 17.
43. Leaver T. Going dark: How Google and Facebook fought the Australian News Media and Digital Platforms Mandatory Bargaining Code. *M/C Journal*. 2021; 24 (2).
44. Lewis J.A. Sovereignty and the role of government in cyberspace. *Brown Journal of World Affairs*. 2010; 16 (2).
45. Lomas N. Meta's behavioral ads will finally face GDPR privacy reckoning in January. *Tech Crunch*. 2022; December 6.
46. Loughlin M. The erosion of sovereignty. *Netherlands Journal of Legal Philosophy*. 2016; 45 (2).
47. Manjoo F. Tech's frightful five: They've got us. *New York Times*. 2017; May 10.
48. Marsonet M. National sovereignty vs. globalization. *Academicus International Scientific Journal*. 2017; 8 (15).
49. McIntosh D. We need to talk about data: How digital monopolies arise and why they have power and influence. *Journal of Technology Law & Policy*. 2019; 23 (2).
50. Meaker M. Australia's standoff against Google and Facebook worked — sort of. *Wired*. 2022; February 25.
51. Meese J., Hurcombe E. Facebook, news media and platform dependency: The institutional impacts of news distribution on social platforms. *New Media & Society*. 2021; 23 (8).
52. Moore D.J. Identity crisis: Why Google and Facebook dominate digital advertising. *Digital Content Next*. 2020; May 19.
53. Morris I. Letting Facebook buy WhatsApp and Instagram was dumb, FTC shows. *Light Reading*. 2021; August 20.
54. Muqsith M.A., Pratomo R.R. The development of fake news in the post-truth age. *SALAM: Jurnal Sosial Dan Budaya Syari*. 2021; 8 (5).
55. Myllylahti M. An attention economy trap? An empirical investigation into four news companies' Facebook traffic and social media revenue. *Journal of Media Business Studies*. 2018; 15 (4).
56. Niebel C. The impact of the general data protection regulation on innovation and the global political economy. *Computer Law & Security Review*. 2021; 40.
57. Ryngaert C., Taylor M. The GDPR as global data protection regulation? *AJIL Unbound*. 2020; 114.
58. Sadowski J. Who owns the future city? Phases of technological urbanism and shifts in sovereignty. *Urban Studies*. 2021; 58 (8).
59. Stein A.A. The great trilemma: Are globalization, democracy, and sovereignty compatible? *International Theory*. 2016; 8 (2).
60. Steinbaum M. Establishing market and monopoly power in tech platform antitrust cases. *Antitrust Bulletin*. 2022; 67 (1).
61. Tankard C. What the GDPR means for businesses. *Network Security*. 2016; 6.
62. Tiago M.T.P.M.B., Veríssimo J.M.C. Digital marketing and social media: Why bother? *Business Horizons*. 2014; 57 (6).
63. Tiwasing P. Social media business networks and SME performance: A rural-urban comparative analysis. *Growth and Change*. 2021; 52 (3).
64. Toh M. How Facebook managed to 'unfriend' Australia while Google came out on top. *CNN*. 2021; February 18.
65. Volk C. The problem of sovereignty in globalized times. *Law, Culture and the Humanities*. 2022; 18 (3).
66. Wallach O. The world's tech giants, compared to the size of economies. *Visual Capitalist*. 2021; July 7.
67. Walt S.M. Big tech won't remake the global order. *Foreign Policy*. 2021; November 8.

68. Watson H.J. Tutorial: Big data analytics: Concepts, technologies, and applications. *Communications of the Association for Information Systems*. 2014; 34.
69. Wong J.C. Facebook to be fined $5bn for Cambridge Analytica privacy violations — reports. Guardian. 2019; July 12.
70. Xuereb K., Grima S., Bezzina F., Farrugia A., Marano P. The impact of the general data protection regulation on the financial services' industry of small European states. *IJEBA*. 2019; 7 (4).
71. Zheltukhina M.R., Slyshkin G.G., Muzykant V.L., Ponomarenko E.B., Masalimova A.R. Fu nctional characteristics of the English and Russian media texts about the Sochi 2014 Winter Olympic Games: Political and linguistic aspects. *XLinguae Journal*. 2017; 10 (3).

DOI: 10.22363/2313-2272-2023-23-4-851-865
EDN: DLIPUS

Социологическое исследование киберугроз как составная часть общего регулирования защиты данных*

М.А. Муксит[1], В.Л. Музыкант[2], Р.Р. Пратомо[1]

[1]UPN Университет Джакарты,
ул. Р.С. Фатмавати Рая, Депок, Западная Ява, Индонезия, 12450

[2]Российский университет дружбы народов,
ул. Миклухо-Маклая, 6, Москва, 117198, Россия

(e-mail: munadhil@upnvj.ac.id; vmouzyka@mail.ru; rizkyridho0897@gmail.com)

Аннотация. Социология изучает общество и особенности его развития, социальные процессы, институты, отношения, структуры, сообщества и те культурные ценности, которые обусловливают их изменения. В то же время социология анализирует и человеческое поведение — как оно воздействует на макроструктуры и как люди ведут себя в разных социальных группах. Не игнорирует социология и вопрос суверенитета: в научной литературе этот феномен имеет множество определений, но большинство подчеркивает его абсолютный и иерархический характер. В ходе истории трактовка суверенитета как территориально обусловленного постепенно утрачивала свою релевантность под влиянием технологического прогресса. Сегодня, в контексте вопросов технологического развития и национальной безопасности, территориальные правила не работают по трем причинам: технологии затрудняют формулировку последовательных и предсказуемых территориальных определений; информация часто распространяется вопреки интересам пользователей и законодателей; технологии позволяют государственным и частным акторам нарушать территориальные правила, причем часто они делают это незаметно [12]. Другое следствие технологического развития — появление новых акторов с сильным международным влиянием благодаря глобализации, свободным рынкам и инновациям. Среди этих акторов наибольший интерес представляют мультинациональные компании, работающие на внетерриториальной основе, что создает проблемы скорее юрисдикции, чем суверенитета в его формальной трактовке [40]. Но остается ли тогда суверенитет релевантным понятием для государства? С приходом Интернета концепт национального го-

Статья поступила 28.07.2023 г. Статья принята к публикации 16.10.2023 г.

сударства подвергается критике, поскольку его акторы утрачивают прежнее доминирование. Интернет поддерживает власть многих международных акторов, но наиболее значимые среди них — технологические компании. Их доминирование порождает вызовы экономического, юридического, политического и социального характера, а потому государство пытается регулировать их деятельность. Авторы утверждают, что государственный суверенитет все еще релевантное понятие, несмотря на массу противоположных аргументов. В качестве обоснования в статье приведены два примера: Общий регламент по защите данных (ОРЗД) и Кодекс сделок для новых медиа (КСНМ). Национальное государство демонстрирует свой суверенитет, принимая законы, которые регулируют деятельность крупных компаний, т.е. ограничивая власть технологических гигантов.

Ключевые слова: кибер-угрозы; информационный суверенитет; цифровая эпоха; технологические компании; Общий регламент по защите данных (ОРЗД); Кодекс сделок для новых медиа (КСНМ)