

The Right to Privacy and Personal Data Protection in Russia, Lithuania and Germany: From History to Current Discourses¹

Monika Rogers

Institute of Lithuanian History

✉ monika.rogers@istorija.lt

Summary. This article discusses public and legal discourses related to ideas and perceptions of privacy and personal data security in Germany, Lithuania and Russia. It investigates whether – and if so, how – the historical ideas and beliefs about privacy and personal data protection are still shaping attitudes and policies related to personal data protection and privacy of these three countries. Russia, Lithuania and Germany had similar historical experiences of living in non-democratic societies. However, today Russia is drifting towards a completely opposite normative and geopolitical trajectory than Lithuania and Germany. The article reveals how differences in political systems affect legal agendas related to personal data protection. It also takes into consideration both similarities and differences between Germany and Lithuania.

Keywords: Personal Data Protection, Respect to Privacy, Human Rights, Law, History, Lithuania, Germany, Russia.

Teisė į privatumą ir asmens duomenų apsaugą Rusijoje, Lietuvoje ir Vokietijoje: nuo istorijos iki šiandienos diskursų

Santrauka. Straipsnyje aptariami viešieji ir teisiniai diskursai, susiję su privatumo ir asmens duomenų apsaugos idėjomis ir jų suvokimu Vokietijoje, Lietuvoje ir Rusijoje. Taip pat tiriama, ar (ir jei taip, tai kaip) istorinės idėjos ir įsitikinimai apie privatumą ir asmens duomenų apsaugą vis dar formuoja požiūrį ir politiką, susijusią su asmens duomenų apsauga ir privatumu šiose trijose šalyse. Rusija, Lietuva ir Vokietija turėjo panašią istorinę gyvenimo nedemokratinėse visuomenėse patirtį. Tačiau šiandien Rusija dreifuoja į visiškai priešingą normatyvinę ir geopolitinę trajektoriją nei Lietuva ir Vokietija. Straipsnyje atskleidžiama, kaip politinių sistemų skirtumai veikia su asmens duomenų apsauga susijusias teises darbotvarkes. Taip pat atsižvelgiama į Vokietijos ir Lietuvos panašumus ir skirtumus.

Reikšminiai žodžiai: asmens duomenų apsauga, pagarba privatumui, žmogaus teisės, teisė, istorija, Lietuva, Vokietija, Rusija.

¹ The research idea was developed and the primary research on this topic was evaluated under the program “re-constitution – Exchange and Analysis on Democracy and the Rule of Law in Europe”. Dr. Monika Rogers was a program fellow in 2020–2021. More information about the program: <<https://www.reconstitution.eu/en/home>>.

Introduction

The European Convention on Human Rights, formally called Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) defines respect to privacy as one of the fundamental human rights. Article 8, titled "Right to respect for private and family life", claims: "Everyone has the right to respect for his private and family life, his home and his correspondence".²

Also, the article establishes that "there shall be no interference by a public authority with the exercise of this right", unless such an interference is executed "in accordance with the law and is necessary in a democratic society 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".³

The attempts to define the concept and the right to privacy can be traced in the ideas and cognitive frameworks of the most influential philosophers, whose thoughts have shaped Western Civilization – from Aristotle to Hannah Arendt.⁴

However, in 20th century Europe and globally, this fundamental right was harshly violated by various dictatorships and non-democratic regimes. As the Albanian scholar Fatos Lubonja experienced while living and being a political prisoner in an Albanian communist dictatorship gave him a sense that privacy, "as a dimension of freedom, has not existed as a concept in our culture, which was deeply marked by totalitarianism".⁵

Today, European countries and societies, many of whom have a non-democratic past, are facing new threats to this fundamental right, defined by multiple factors – from technological progress to growing political extremism and a frightening geopolitical situation. In 2022, the United Nations warned in their report, that "People's right to privacy is coming under ever greater pressure from the use of modern networked digital technologies whose features make them formidable tools for surveillance, control and oppression".⁶

The UN recognized the threats of these developments and claimed that, in such conditions, it is "essential that these technologies are reined in by effective regulation based

² European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15; supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Strasbourg, p. 11, <https://www.echr.coe.int/documents/d/echr/convention_ENG>.

³ *Ibid.*

⁴ H. Arendt (2013), *The Human Condition: Second Edition*, University of Chicago Press, pp. 58–72.

⁵ F. Lubonja (2001), Privacy in a Totalitarian Regime, *Social Research*, 68, 1, Privacy (Spring), p. 237.

⁶ UN Press Release, Office of the High Commissioner for Human Rights, "Spyware and surveillance: Threats to privacy and human rights growing, UN report warns", 16 September 2022, <<https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>>.

on international human rights law and standards”.⁷ According to the report, current technological developments directly pose threats to human rights and democracy, by shifting the power balance between the citizens and the authority in a negative way:

Modern data-driven technologies are dramatically shifting the balance of power between the entity carrying out the surveillance and those being monitored. Before the advent of large-scale automated surveillance and data analytics tools, there were practical limitations to surveillance that provided a certain level of protection for individuals, even when in public. (...) Today, a single officer can monitor the social media accounts of dozens of people and, with the assistance of advanced software and big data analytics, small teams can observe and profile thousands of accounts.⁸

Keeping these trends in mind, the driving idea behind this paper is to study the legal and public discourses on digital-space related to privacy and personal data security in Germany, Lithuania and Russia from the Soviet and state socialist era until this day. These three countries are chosen due to several factors:

- a) The fact that Russia, Lithuania and Germany all share the legacy a non-democratic past, defined, first, by the long-lasting state-socialist legal systems and, in the case of Germany – National Socialist totalitarianism.⁹ Having experienced harsh violations of the right to privacy in the past, they are interesting cases for comparisons with current developments related to the right to privacy.
- b) The pioneering role which Germany played in the establishment of the Right to Privacy framework within EU.¹⁰
- c) The importance of the current Russian regime in building the legal and political discourse, justifying the violation of this fundamental human right.¹¹
- d) Lithuania is an interesting and suitable case for analysis due to several factors, but, most importantly, its rapid post-Soviet transition (including dealing with the former Soviet state surveillance legacy), successful creation of the rule of law and integration in the EU – and at the same time, the geographical proximity to Russia as a NATO border region, that causes a constant threat and worries of hybrid warfare, surveillance

⁷ *Ibid.*

⁸ The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights, 4 August 2022, <<https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf>>.

⁹ It is important to mention, that Lithuania has also experienced Nazi Germany's period as well (1941–1944). However Soviet and State Socialism systems' impact was longer lasting – due to the much shorter period of Nazi occupation (4 years versus 5 decades). See more: A. Anušauskas [et al.], *Lietuva 1940–1990: Okupuotos Lietuvos istorija*, 2007.

¹⁰ F. Molnár Gábor (2018), Germany: a fair balance between scientific freedom and data subjects' rights? *Human Genetics*, 137, p. 622.

¹¹ T. Lokot (2020), Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia, *Media and Communication*, 8(2), pp. 314–322.

and propaganda. Lithuania is also an interesting case for our research because it demonstrates the success and failures of EU legislation and policies, related to the protection of personal privacy.¹²

This article investigates whether historical ideas and experiences related to privacy protection in these countries have shaped – and continue to shape – the rules, regulations and policies governing communication in the digital sphere. I also take into consideration current developments related to the right of personal data privacy in these three countries – that include, but is not limited to such topics as legal and technological developments, security risks and the current geopolitical reality, paying particular attention to Russia's full-scale aggression against Ukraine.

The research aim is to describe legal and political discourses and definitions related to personal data protection in Germany, Lithuania and Russia, their evolution and relation to the past. The research objectives include: a) attempts to indicate if (and if yes, how) the non-democratic past still influences legal and normative reality of personal data protection in these countries; b) to analyse and compare the most important laws and legal practices, including court cases, related to the protection of privacy.

Researching the historical definitions of the concept of “privacy” and “personal data protection” is only a part of my research. I question, as well, if the Soviet and state-socialist perspectives still impact today's national law, legal practices and general understanding about privacy rights and personal data protection issues in Russia, Germany and Lithuania. It is also important to investigate the vulnerabilities and difficulties that these societies might encounter or are already experiencing due to their non-democratic past and because of their long experience of living under legal systems that rather imitated than implemented the basic democratic principles (in the case of Russia, such system is still present).

The biggest challenge of the research was to find the appropriate methodological choices. The research design is based on qualitative research methods, including comparative law, and critical analysis of digital archives, public sources and academic literature.

Combining different research methods proved to be a fruitful research strategy in order to achieve the macro-perspective research aims and objectives outlined in this paper. First of all, the analysis of the legal and historical sources was performed. It was also the study of the academic literature conducted. This strategy enabled the analysis of the changes of legal, political and popular (as reflected in the mass media) approaches towards privacy and personal data security in Russia, Germany and Lithuania from the state-socialist and Cold War periods to this day.

¹² N. Bitiukova (2021), Lithuania Reports: GDPR Implementation Series, *European Data Protection Law Review (EDPL)*, Vol. 7, No. 1, pp. 108–114.

Originally this article was not supposed to cover Ukraine. However, as we will see later in this article, Russia's full-scale invasion in 2022 plays a significant role in changing attitudes, tactics and behaviour strategies, related to personal data protection and digital security in Europe and beyond, influencing Lithuania, Germany and Russia directly. Therefore, the developments in Ukraine regarding this issue will be briefly discussed in the paper.

Case studies, focusing on privacy and personal data protection, when Lithuania, Germany, or Russia are analysed separately, as individual cases, are quite common. Various aspects of this topic are investigated: from balancing new technologies, such as Large Language Models and Data Protection in today's Germany¹³ to successes and failures of the practical GDPR implementations in Lithuania (for instance, by D. Beinoravičius, V. Keršulienė and I. Mačernytė-Panomariovienė).¹⁴

Some comparative studies also exist. For example, they are comparing privacy protection in Lithuania and Poland,¹⁵ Lithuania and Latvia.¹⁶

The Russian regime's policy towards personal data is also well researched by such authors as T. Lokot.¹⁷ The same can be said about research on privacy violations from a historical perspective.¹⁸

However, this paper suggests two aspects, defining my research novelty: investigating current issues of privacy in the context of historical past; analysing Russia, Germany and Lithuania together, in one study and one paper.

In this research, the term *discourse* means "everything that has been said and written" on the specific topic, by the members of the certain "discourse community". The discourse allows individuals to make sense of the objects and phenomena, existing in the world and in the society.¹⁹

¹³ F. Leboukh, E. Baba Aduku, O. Ali (2023), Balancing ChatGPT and Data Protection in Germany: Challenges and Opportunities for Policy Makers, *Journal of Politics and Ethics in New Technologies and AI*, 2(1), e35166.

¹⁴ D. Beinoravičius, V. Keršulienė, *Privacy Protection in the Transmission of Personal Data in Business – Insights from Lithuania*. 12th International Scientific Conference "Business and Management 2022", May 12–13, 2022, Vilnius, Lithuania; I. Mačernytė-Panomariovienė (2023), Discrimination on the Basis of Personal Data in Employment: The Case Study of Lithuania, *Baltic Journal of Law & Politics* 16:1, pp. 24–41, <<https://content.sciendo.com/view/journals/bjlp/bjlp-overview.xml>>.

¹⁵ D. Lisiak-Felicka, M. Szmit, J. Vaičiūnienė (2022), The General Data Protection Regulation 3 Years After. Implementation: A Comparison between Local Government Administration in Poland and the Republic of Lithuania, *European Research Studies Journal*, XXV, 1, pp. 382–394.

¹⁶ A. Pūraitė, N. Šilinskė (2021), State Regulation of Privacy and Its Protection in the use of VIRDs By Police: Comparative Perspective from Latvia and Lithuania, *Public Security and Public Order*, 27.

¹⁷ T. Lokot (2020), Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia, *Media and Communication*, 8(2), pp. 314–322.

¹⁸ A. Bateman (2016), The KGB and Its Enduring Legacy, *The Journal of Slavic Military Studies*, 29/1, pp. 23–47.

¹⁹ W. Teubert (2010), *Meaning, discourse and society*, Cambridge University Press, pp. 1–2.

“State socialism” is understood as the political and economic ideology within the socialist movement that advocates state ownership of the means of production – and the political regime that turns such ideology into practice.²⁰ The regimes of the Soviet Union and Soviet Lithuania were examples of state socialism – just as the GDR.

One more term – “transition” – is used while talking about the post-Soviet period. It, at least to some extent, would fit into the time frame between Perestroika (late 1980s – early 1990s) and, for Lithuania and former Eastern Germany, the integration into the Western sphere (for instance, joining the European Union and NATO, which occurred in 2004 in the case of Lithuania). For Russia, it means the attempts to build democracy in the 1990s – that failed after Putin’s first election in 2000. This period in the whole Soviet and post-Soviet sphere and beyond can be analysed using such metaphors as “transformation”, “fraction”, “turning point” and described as the active attempts to build democracy, capitalism and rule of law. For instance, the Lithuanian scholar Zenonas Norkus focused on Lithuania’s radical 1990s shift from Soviet state socialism to the market economy in relation to democratic reform, where he mostly used the term “transformation” (2008).²¹

This research paper attempts to connect history with the present and demonstrate how one affects the other, examining whether – and how – the chosen geopolitical trajectories of Russia, Lithuania and Germany affect their attitudes toward personal data privacy.

1. Concept of privacy under state surveillance: the USSR, Russia, Lithuania, the GDR

As it has been already indicated, Lithuania, Russia and Eastern Germany, despite different pre-state socialist and post-state socialist trajectories, share a similar legacy, when it comes to law and ideology – that is related to the Soviet and state socialist past. Of course, their pre- and post-socialist paths in conceptualising the right to privacy and personal data protection diverged significantly. But shared period of history under communist dictatorship is a reason why some definitions of and approaches toward the right to privacy and data security protection historically were similar.

In Russia, building the new Soviet system started right after the Bolshevik coup of 1917, in Lithuania – more than two decades later. First occupied and annexed by the Soviet Union in 1940, reoccupied in 1944, Lithuania lost its sovereignty and the autonomy of its legal system. The whole field of criminal prosecution, constitutional and civil law was also transformed in line with Soviet standards and eventually, they were integrated into

²⁰ B. Tucker (1985), *State Socialism and Anarchism and Other Essays: Including the Attitude of Anarchism Toward Industrial Combinations and Why I Am an Anarchist* (1st ed.), Colorado Springs: Ralph Myles Publisher.

²¹ Z. Norkus (2008), *Kokia demokratija, koks kapitalizmas?: pokomunistinė transformacija Lietuvoje lyginamosios istorinės sociologijos požiūriu*, Vilnius: Vilniaus universiteto leidykla.

the unified legal system of the Soviet Union.²² The repressive state apparatus, designed to maintain population control, also became a reality – including such institutions as the NKVD, which changed its names and eventually became the KGB.²³

Officers of Soviet Lithuanian law enforcement / state intelligence and surveillance institutions reported directly to Moscow – allowing the “centre” of the Soviet state to maintain the control. Therefore, looking from the historical perspective, the way Soviet Lithuania and Soviet Russia treated their residents in matters related to their privacy (and violation of that privacy) had similarities.²⁴ Therefore, in the Soviet period, a very similar definition and perception of privacy applies to both Lithuania and Russia.

It is important to stress, that the Soviet legal system and society were more diverse and reflexive than the West portrayed and depicted them during the Cold war era.²⁵ However, the strong mechanisms of centralization of lifestyle standardization²⁶ are also difficult to ignore.

Therefore, both Soviet Russia and Soviet Lithuania followed (or were forced to follow) the same definition and perception of privacy in Soviet law. According to Tetyana Lokot, “the notion of individual privacy has always been a political one throughout Russia’s Soviet and post-Soviet periods, connected as it was to the culture of pervasive state surveillance”, as the Soviet state was constantly attempting to gain control of both public and private lives of citizens.²⁷

The described approach was not only practical – but also ideological. As Lokot claims, according to the views of the early Soviet Bolsheviks, “anything private was deprived of social meaning and thus politically dangerous”, and the so-called “social duty” – as a moral principle, value and ideal – was more important than the commitment to privacy in the Soviet political and legal culture.²⁸ So, in the hierarchy of ethical principles, in Soviet Lithuania and Russia, the commitment to building and strengthening the Soviet regime was higher than the human right to privacy.

²² M. Kareniauskaitė (2017), *Crime and punishment in Lithuanian SSR*, [Doctoral Thesis], Vilnius University.

²³ The KGB, the Committee for State Security was the main security and state surveillance agency in the Soviet Union. KGB was attached to the Council of Ministers of the USSR. It existed from 1954 to 1991. See more in: Aaron Bateman, “The KGB and Its Enduring Legacy”, *The Journal of Slavic Military Studies*, 29/1, 2016, pp. 23–47.

²⁴ K. Burinskaitė (2011), *LSSR KGB veiklos ideologiniai ir politiniai aspektai 1954–1990 m.*, [Doctoral Thesis], Vilnius University.

²⁵ S. Fitzpatrick (2007), *Revisionism in Soviet History*, *History and Theory*, 46/4, pp. 77–91.

²⁶ M. R. Beissinger (2006), *Soviet Empire as ‘Family Resemblance’*, *Slavic Review*, 65/2, pp. 294–303.

²⁷ T. Lokot (2020), *Data Subjects vs. People’s Data: Competing Discourses of Privacy and Power in Modern Russia*, *Media and Communication*, 8(2), p. 315; T. Lokot (2018), *Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices*, *Surveillance & Society*, 16/3, 2018, pp. 332–346.

²⁸ T. Lokot (2020), *Data Subjects vs. People’s Data: Competing Discourses of Privacy and Power in Modern Russia*, *Media and Communication*, 8(2), p. 315.

One more illustrative example – checking private letters by the Soviets, which was witnessed by many dissidents.²⁹

Germany is a different case: being divided into Eastern and Western states meant also a division between a dictatorship and a democracy. However, it is well researched by historians³⁰ that the activities of the Stasi,³¹ connected to personal privacy violations, also intruded into the Federal Republic of Germany. After the reunification of the country, the state-socialist heritage became a shared burden of the whole German population.³²

The initial design of the German Democratic Republic (East Germany) state surveillance system was copied from the Soviet Union. The GDR transferred the Soviet ideological understanding of personal privacy – and developed a practical implementation of policy that restricted and violated this privacy that had a higher level of efficiency than in many other state-socialist countries. The Stasi surveillance system was infamous for its technological progressiveness of equipment, for the notorious effectiveness of its secret informants (agents) and for its vast network of involved individuals.³³

So, for at least several decades of the 20th century in Russia, Germany and Lithuania were marked by the limitations or even denial of the very concept and idea of the privacy, as one of the most important citizens' rights. Therefore, the full protection of individual citizens' right to privacy was not implemented.

2. Privacy and law during “transition” period: lustration as an issue

After the 1990s, the political trajectories of the former Eastern Germany (now reunited Federal Republic of Germany), Lithuanian Republic and Russian Federation slowly shifted from the previous Soviet/state-socialist model. While Germany started the process of unification, and Lithuania decided to apply for membership of the European Union, the Russian Federation, after a brief period of democracy under president Boris Yeltsin, came back to authoritarianism.

²⁹ Laiškai iš gulago (1979), *Lietuvos Katalikų Bažnyčios kronika*, Nr. 39, <<https://lkbkronika.lt/index.php/39-kronika-1979-m>>.

³⁰ J. C. Schmeidel, *Stasi. Shield and Sword of the Party*, London: Routledge, 2007.

³¹ The Ministry for State Security (Geran: Ministerium für Staatssicherheit, MfS), commonly known as the Stasi, was the state security service of the German Democratic Republic. The Stasi motto was Schild und Schwert der Partei (eng. Shield and Sword of the Party), referring to the ruling Socialist Unity Party of Germany (Sozialistische Einheitspartei Deutschlands, SED). The Stasi had headquarters in East Berlin. One of the Stasi's main tasks was spying on the population through a vast network of citizens-turned-informants. See more in: *The Stasi at Home and Abroad: Domestic Order and Foreign Intelligence*, *Bulletin of the German Historical Institute*, No. 52 Supplement 9, Washington DC, USA, 2014.

³² K. Jarausch (2014), *Between Myth and Reality: The Stasi Legacy in German History*, *The Stasi at Home and Abroad: Domestic Order and Foreign Intelligence*, *Bulletin of the German Historical Institute*, 52, Supplement 9, Washington DC, USA, pp. 73–83.

³³ H. Müller-Enbergs (2008), *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 3: Statistiken*, Berlin: Christoph Links Verlag.

These transformations, with no doubts, impacted perceptions about individual privacy and its protection. At the same time, all countries faced similar dilemmas concerning privacy and personal data protection, stemming from their non-democratic past. For example, all three countries had to decide how to handle the huge data archives inherited from the former secret surveillance and state repressions-related authorities – and some cases were extremely sensitive in terms of personal data protection.

Among the extensive Stasi documentation legacy, there are extremely numerous personal data records, including a huge archive of information connected to personal health. As one of the foreign observers, Richard Sietmann, commented in the press in 1991 – “But among the old East German government’s files was one set of data that medical researchers now find themselves fighting to preserve: a huge array of epidemiological information, gathered since 1957, on more than 2 million cases of cancer – 95% of all the cases that occurred in East Germany”³⁴. According to him, “Researchers would dearly love to mine this lode to extract information on possible links between cancer and exposure to carcinogens, but they have hit a serious road-block. Under the Federal Data Security Act – now valid throughout Germany – the cancer register is illegal”.³⁵

The mentioned case very well illustrates, how the interchange between two systems, with such different approaches on personal data protection, created new tensions in privacy laws. According to Sietmann, the chosen legal path – strictly limit disclosure of information, collected violating citizens’ right to privacy, even if it could be useful for scientific research and medical innovations – reflected “public fear of a return to the totalitarian past”.³⁶ At that time, united Germany allowed “medical records bearing individual names to be kept only for very specific purposes, narrowly defined in advance”.³⁷

The above discussed German decision today is more relevant than ever – having in mind the current discussion on compromising the right to privacy when it is seen as a limit for innovation cultivation, research and technological progress.³⁸

Another situation that can be mentioned here, that all three countries faced in the 1990s, was related to the mainly political decision – whether the personal data of the former KGB or Stasi agents should be made publicly accessible.

³⁴ R. Sietmann (1991), East German Cancer Data: A Benefit of Big Brother? A detailed database put together by totalitarian East Germany may tempt the new Germany to relax privacy laws, *Science, New Series*, 252/5008, <<https://www.jstor.org/stable/2875334>>.

³⁵ *Ibid.*

³⁶ *Ibid.*

³⁷ *Ibid.*

³⁸ L. Hornuf, S. Mangold, Y. Yang (2023), Data Protection Law in Germany, the United States, and China, *Data Privacy and Crowdsourcing. Advanced Studies in Diginomics and Digitalization*, Springer, Cham.

Germany was the first country to open files of secret police to the public – a decision was taken to provide “unlimited access to the victims concerning the data on the agent as well, and to government agencies to request background checks on their employees”.³⁹

In Lithuania, the so-called law of lustration was adopted in 1998. A decision was made to create a state commission to which a former KGB informant could voluntarily confess his or her past activities – and, in exchange, the archived information about his or her involvement with the KGB would be closed for both: academic researches and general public.⁴⁰

This Lithuanian decision created a controversy and resulted in a big polarization of Lithuanian society that is still present. On the one hand, the newly-democratic now independent state of Lithuania chose to be cautious and caring about the personal data of the co-workers of the former repressive apparatus – if they confessed to the Lithuanian authorities (interpreting this confession as the act of loyalty). On the other hand, the victims of the crimes against humanity, state violence, repressions and abuses, committed by the former Soviet authorities including the KGB, interpreted the so-called ‘lustration law’ as an act of injustice.⁴¹

Former Lithuanian political prisoners or forcedly deported persons were claiming – and they are still claiming – for the right to access certain information on who was responsible, who committed crimes against them. The Soviet systems’ victims in Lithuania were comparing their situation with the situation of GDR victims. They demanded a similar right to get the information about their perpetrators, which in the Lithuanian case was not granted.⁴²

In Russia this path was different. During Perestroika and the 1990s there were high hopes that the former KGB archives will be opened, lustration will happen and justice for the victims of state socialism will finally be achieved.⁴³

However, lustration in Russia did not happen. According to J. Michael Waller, even though, in the beginning of the first decade of the 21st century, “the state security system

³⁹ G. Halmai (2007), Lustration and Access to the Files in Central Europe, *Lustration and Consolidation of Democracy and the Rule of Law in Central and Eastern Europe*, 5, Zagreb, p. 37.

⁴⁰ Įstatymas „Dėl SSRS valstybės saugumo komiteto (NKVD, NKGB, MGB, KGB) vertinimo ir šios organizacijos kadrinių darbuotojų dabartinės veiklos“, 1998 m. birželio 30 d., Nr. VIII-823, Vilnius, <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/TAIS.59758?jfwid=-n2mqd3363>>.

⁴¹ K. Jarausch (2014), Between Myth and Reality: The Stasi Legacy in German History, The Stasi at Home and Abroad: Domestic Order and Foreign Intelligence, *Bulletin of the German Historical Institute*, 52, Supplement 9, Washington DC, USA, pp. 76–81; J. Ravaitytė (2015), Liustracijos politikos Lietuvoje vertinimas, *Politologija*, 77/1, 2015, p. 49–100.

⁴² Dėl sąmoningo liustracijos vilkinimo (14 November 2007), *XXI amžius*, 84/1581, p. 14, <http://www.xxiamzius.lt/numeriai/2007/11/14/nuom_02.html>; J. Ravaitytė (2015), Liustracijos politikos Lietuvoje vertinimas, *Politologija*, 77/1, p. 49–100.

⁴³ D. N. Khubova (1994), Imprisoned History: the KGB archives, *The Journal of the International Institute*, Vol. 1, Issue 1, Winter, <<https://quod.lib.umich.edu/j/jii/4750978.0001.103?view=text;rgn=main>>.

in Russia” was “no longer the centralized, monolithic force of the USSR KGB, but it has preserved a bureaucratic ideology that reveres the Bolshevik Cheka secret police as its lineal ancestor and maintains a cult-like devotion to Cheka founder Feliks Dzerzhinsky” (2004). So, FSB continued the KGB traditions – violating citizens’ rights in order to “defend” Russia’s political regime, including the right to privacy.⁴⁴

3. Shared approach towards personal data protection in the digital era in Lithuania and Germany: from the Federal Republic of Germany experience to the European GDPR

Despite the issues with transitional justice and lustration, Lithuania – as well as the former GDR – eventually transformed their legal systems successfully when it comes to privacy laws and data protection. Today, both countries are following the European Union’s legal approach in this regard.

German experience is very important here. As Gerald Spindler noted, it is important to recognize that “German data protection law has largely influenced EU data protection directives and implements them; therefore, any overview of the German legal framework would be incomplete without reference to European law”.⁴⁵ According to Spindler, the Federal Republic of Germany prior to the reunification “had been the ‘origin’ of European data protection, leading the way in the early-1970s with one of the first acts on data protection”, while “the German Constitutional Court influenced the international debate heavily by deriving the fundamental right of ‘personal data self-determination’ from the Constitution as part of the fundamental rights of mankind”.⁴⁶

It’s hard to disagree with such view – as it is important to remember the Judgment of the German Federal Constitutional Court (Bundesverfassungsgericht) of 15 December 1983, which has established the fundamental right to informational self-determination. The ruling declared that, in an era of automated data processing, individuals must have the authority to decide if and to what extent their personal data can be used and made public.⁴⁷ In academic literature, this decision is seen as a key turning point not only in German constitutional law, but also in wider European legal perspective.⁴⁸

⁴⁴ A. Bateman (2016), The KGB and Its Enduring Legacy, *The Journal of Slavic Military Studies*, 29/1, pp. 23–47.

⁴⁵ G. Spindler (2016), Consumer Data Protection in Germany, Metz, R., Binding, J. Haifeng, P., Huber, P. (eds.), *Consumer Data Protection in Brazil, China and Germany. A Comparative Study*, Göttingen: Göttingen University Press, p. 72.

⁴⁶ *Ibid.*

⁴⁷ Abstract of the Federal Constitutional Court’s Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83. Accessible online: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html>.

⁴⁸ G. Spindler (2016), Consumer Data Protection in Germany, Metz, R., Binding, J. Haifeng, P., Huber, P. (eds.), *Consumer Data Protection in Brazil, China and Germany. A Comparative Study*, Göttingen: Göttingen University Press, pp. 71–76.

Later, by decision of 27 of February 2008, the German Federal Constitutional Court annulled the previously adopted provisions of the North-Rhine Westphalian state that allowed the government to conduct online surveillance of personal computers. The decision declared unconstitutional the lack of respect of individual's right to confidentiality of stored data of technology systems, as well as the integrity of information technology systems themselves. It was referred to as the 'IT Privacy' right by the mass media. Basically, it meant that unjustified online surveillance violated the fundamental right to privacy.⁴⁹

In the case of Germany (and later in the Lithuanian legal evolution of personal data protection), one cannot ignore European Law such as the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.⁵⁰ As EU directives have binding legal force throughout all member states, Lithuania's accession to the EU in 2004 also meant its integration into the EU legal system for personal data protection.

It is very important to stress that the directive protected only the personal data of individuals; corporate entities were excluded from it.⁵¹

As for Germany, the Federal Data Protection Act (BDSG) of 30 June 2017 should be mentioned. According to Spindler: "Both the European Union Data Protection Directive (DPD) and the proposed GDPR, as well as the BDSG, are characterized by certain fundamental principles of data protection", as "the objective of the directive is to protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data, and to guarantee the free flow of personal data between member states".⁵² It is no surprise that in Germany, concerned with the personal data protection and privacy, the topic of protection of these values is common in the media. This topic covers a wide range of issues: for instance, the role of tech companies in addressing potential data protection risks,⁵³ possible solutions to this problem and proposals for new, more secure software solutions.⁵⁴

⁴⁹ C. Preuß, J.-A. Paul (2008), *German Constitutional Court creates a new fundamental 'IT Privacy' Right*, September, Bird & Bird, Accessible online: <<https://www.twobirds.com/en/news/articles/2008/germanconstitutional-court-creates-a-new-fundamental-it-privacy-right>>.

⁵⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>>.

⁵¹ G. Spindler (2016), *Consumer Data Protection in Germany*, Metz, R. Binding, J. Haifeng, P., Huber, P. (eds.), *Consumer Data Protection in Brazil, China and Germany, A Comparative Study*, Göttingen: Göttingen University Press, p. 75.

⁵² *Ibid.*, p. 91.

⁵³ See, for instance: "Vertrauen und Misstrauen: 20 Jahre Google Deutschland", Donaukurier, 4 October 2021, <<https://www.donaukurier.de/nachrichten/digital/netzundtechnik/Internet-Datenschutz-Geschichte-Unternehmen-Deutschland-USA-Vertrauen-und-Misstrauen-20-Jahre-Google-Deutschland;art251974,4817277>>.

⁵⁴ See, for instance: "TeamViewer will, erste datenschutzkonforme' Unterrichtssoftware anbieten", 28 September 2021, *Spiegel Netzwerk*, <<https://www.spiegel.de/netzwelt/web/teamviewer-will-erste-datenschutzkonforme-unterrichts-software-anbieten-a-87a2ed5d-c4d0-41f9-8335-02a72be19890>>.

In Lithuania, the Law on Legal Protection of Personal Data was adopted on 11 June 1996. As the first article of the law claims that the purpose of the Law is to “safeguard the inviolability of an individual’s private life in the course of processing personal data”⁵⁵. The law regulates “relations arising in the course of the processing of personal data by automatic means, and during the processing of personal data by other than automatic means in filing systems: lists, card indexes, files, codes, etc”⁵⁶.

It seems that the implementation of the law in Lithuania was not always a smooth process and practical challenges have arisen even having sufficient legislation. For instance, in 2014, it was discussed in the media that “the National Audit Office conducted an audit in state institutions and has determined that there are flaws in the protection of personal data”.⁵⁷

According to the media, the aim of this process was to check whether personal data that had been processed by algorithms were well protected. The follow-up report concluded, that “individual rights to personal privacy are insufficiently ensured in Lithuania” and that “not all legislation or personal data protection requirements are implemented in the public sector”. Also, it was stressed that “the regulation in this area is falling behind progress in information and communications technologies”.⁵⁸ Moreover, the report underlined:

“Even though the Law on Legal Protection of Personal Data and its implementing legislation was amended several times from 2008–2012, rapid progress in information and communications technologies raises new issues which are not addressed by today’s legal acts”.⁵⁹

Talking about the Lithuanian public discourse on personal data privacy, the situation has changed significantly in the last two decades. In the early 2000s there was more concern about the state’s illegal action in collecting citizens’ personal data. For instance, during the impeachment⁶⁰ of Lithuanian president Rolandas Paksas, concerns were

⁵⁵ Republic of Lithuania Law on Legal Protection of Personal Data, 11 June 1996 No I-1374 (As last amended on 3 November 2016 – No. XII-2709), <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae>>.

⁵⁶ *Ibid.*

⁵⁷ Online Data at Risk to Hackers (2014), *The Baltic Times*, 842, January, p. 5.

⁵⁸ *Ibid.*

⁵⁹ *Ibid.*

⁶⁰ On 26 February 2003 a term by Rolandas Paksas, as elected President of Lithuania, began. Soon concerns arose that he had ties to the Russian mafia. Yuri Borisov, who was a president of the aviation company Avia Baltika, had donated \$400,000 to his campaign, and was given Lithuanian citizenship by Paksas’ decree. This decree was later ruled to be unconstitutional by Constitutional Court of Lithuania and Paksas’ connections were investigated by the State Security Department of Lithuania. In early 2004, the Seimas started impeachment proceedings against him. On 31 March 2004 the Constitutional Court of Lithuania found him guilty of violating the constitution and his oath of office, on 6 April 2004, the Parliament voted positively on removing Paksas from the presidency. See more in: “Lithuanian Parliament Removes Country’s President after Casting Votes on Three Charges”, *New York Times*, 7 April 2004, accessible online: <<https://www.nytimes.com/2004/04/07/world/lithuanian-parliament-removes-country-s-president-after-casting-votes-three.html?pagewanted=1>>.

raised whether Lithuanian security services had violated the law, for instance, by “tapping telephone conversations of suspected public officials, including Paksas himself”.⁶¹

Having said that, the last decade witnessed a shift in Lithuanian public discourse: the concerns about the potential violations by the state regarding personal data seem to be overshadowed by the concerns of other digital threats posed by other actors. For instance, in 2012, as officially reported by Google and covered in the press, “Lithuanian officials were initially reluctant to proceed” with the Street View application initiative “due to privacy and security concerns, a complaint which Google had to previously contend with in other countries”.⁶²

However, the state has been blamed more often for not providing enough security than for deliberately violating the citizens’ personal data. As the *Baltic times* wrote in 2015:

“Cyber security used to be a rather a narrow topic, interesting only to specialists; yet after terror attacks in France, and the events in Ukraine it has been attracting public attention in Lithuania. Some 81 percent of Lithuanian residents feel a growing risk of being targeted by electronic crimes, according to a recent Eurobarometer survey, and worries have not subsided since the government’s launching of a new Cyber Security Center at the start of the year”.⁶³

In an effort to better ensure data security and citizens’ privacy, financial challenges arose: the state had to offer competitive salaries to IT specialists. But, as the press underlined, Lithuanian minister of the Interior of that time, Saulius Skvernelis stated that the government “certainly sees the importance of Lithuania upping the ante with its cyber security” and “the right to privacy and personal data protection as becoming as crucial as saving people’s lives”.⁶⁴

In recent years public discourse in Lithuania was expressing more and more interest in data privacy and personal data security issues by discussing cases related to concerns about ensuring privacy: from cases of customers’ data leak by local enterprises⁶⁵ to the recommendation of Lithuania’s Ministry of National Defence for consumers to avoid buying Chinese mobile phones.⁶⁶

Despite the mentioned doubts and risks still existing in law implementation, today both Lithuania and Germany, as EU members, share a very similar legal reality, defined by

⁶¹ A. Racas (4 December 2003), Doubts on privacy rights raised in scandal, *The Baltic Times*, 386.

⁶² Lietuva in Brief (14 June 2012), *The Baltic Times*, 805.

⁶³ Lithuania short of cyber sleuths (15 March 2015), *The Baltic Times*, 856, p. 4.

⁶⁴ *Ibid.*

⁶⁵ Hacker who leaked CityBee user data tells media cyber security was poor (February 17, 2021, *BNS, LRT*, <<https://www.lrt.lt/en/news-in-english/19/1346403/hacker-who-leaked-citybee-user-data-tells-media-cyber-security-was-poor>>.

⁶⁶ A. Sytas (22 September 2021), Lithuania says throw away Chinese phones due to censorship concerns, *Reuters*, <<https://www.reuters.com/business/media-telecom/lithuania-says-throw-away-chinese-phones-due-censorship-concerns-2021-09-21/>>.

the General Data Protection Regulation (GDPR).⁶⁷ It entered into force on 25 May 2018. On its official website, the GDPR is characterized as “the toughest privacy and security law in the world”, and according to its official explanation, “imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU”.⁶⁸ Finally, it is also underlined that it “will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of Euros”.⁶⁹ Thus, with the EU bringing two countries closer together, a shared legal reality has emerged.

4. Personal data protection in Putin’s Russian Federation: towards the networked authoritarianism

While in Russia, the Federal Law on Personal Data (No. 152-FZ) was adopted by the State Duma on 8 July 2006 and, approved by the Federation Council on 14 July 2006. This law constitutes the core of Russian privacy laws. It requires protecting personal data against any unlawful or accidental access.⁷⁰

However, the practical implementation of the mentioned law seems to be limited and problematic. As Tetyana Lokot claims, in the digital era “privacy has become an even more contested concept in Russia, given the citizens’ embrace of digital technologies and the state’s preoccupation with control over data and information flows as part of the national security and sovereignty project”.⁷¹ Lokot agrees with the other scholars, for example, Greene and MacKinnon, calling today’s Russian political system “networked authoritarianism”.⁷²

The concept is understood as “a regime in which the state prioritizes developing networked infrastructure and digital connectivity, while seeking to control all spheres of the datafied social life”.⁷³

According to Lokot, the very concept of privacy in Russia is rather problematic. The term ‘privacy’ [приватность] in Russian language seems to be borrowed from other languages. So, historically, Russia seems to lack the deep relation to “privacy” as a value, ideal and crucial human right. It happened only in Putin’s Russia, that the concept of “privacy in the modern sense”, entered “the mainstream legal, political, and social discourse”. The

⁶⁷ General Data Protection Regulation, Article 4-1, <<https://gdpr.eu/article-4-definitions/>>.

⁶⁸ “What is GDPR, the EU’s new data protection law?”, <<https://gdpr.eu/what-is-gdpr/>>.

⁶⁹ *Ibid.*

⁷⁰ Federal Law of 27 July 2006 N 152-FZ on personal data, <<https://pd.rkn.gov.ru/authority/p146/p164/>>.

⁷¹ T. Lokot (2020), Data Subjects vs. People’s Data: Competing Discourses of Privacy and Power in Modern Russia, *Media and Communication*, 8(2), p. 315.

⁷² *Ibid.*

⁷³ *Ibid.*; S. Greene (2012), *How much can Russia really change? The durability of networked authoritarianism*. Washington, DC: PONARS Eurasia; MacKinnon, R. (2011), Liberation technology: China’s ‘networked authoritarianism’, *Journal of Democracy*, 22/2, 2011, pp. 32–46.

mentioned Russian law not only defines the citizens' rights towards personal data protection, but also allows the state and law enforcement authorities to access user data and metadata in order to protect the national security.⁷⁴

Before the full-scale invasion of Ukraine, in Putin's Russia there were two dominating approaches towards the right to privacy: a) that of the government which prioritized national (or, more precisely, the current regime's) security over privacy – it chose to play a paternalistic and protective role towards the citizens, presenting itself as guardian from “evil tech companies”; b) that of local activists who were advocating for stricter protection of personal data privacy.

The first targets were foreign companies, but soon it became clear that the local social networks also have the capacity to mobilize the opposition within Russia: “the 2011 to 2012 anti-government protests have sensitized the ruling regime to new media's mobilization capacities”, “strategic measures have been taken to bring such possibilities under control”.⁷⁵

It is not a surprise that already before the Russian full-scale invasion of Ukraine, the Russian government chose violating privacy of its citizens, while seeing them “as vulnerable data subjects with little agency, whose private identities and communications should be protected from ‘foreign interference,’ but must always remain visible and accessible to the state”⁷⁶

However, before the invasion there was at least some opposition to this approach, as “Russian digital rights activists advocate for privacy as a human right and argue that technologies such as encryption and VPNs should be widely adopted by citizens to preserve their agency and protect their data and identities from the state”.⁷⁷

The controlled Russian mass media, as expected, chose the first approach. The Russian press, radio and television, for instance, extensively reported about the speech of Putin from Davos in 2021, that included the section on tech giants and social media networks. In that speech Putin expressed concern about the growing impact of the large tech companies, naming their surveillance and tech powers as a threat to the state apparatus: “these are no longer just economic giants – in some areas they are already de-facto competing with states. Where's the line between [a state and] a successful global business with popular services”. Moreover, according to Putin, commercial corporate tech powers attempt

⁷⁴ T. Lokot (2020), *Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia*, *Media and Communication*, 8(2), pp. 315–316.

⁷⁵ A. Akbari, R. Gabdulhakov (2019), *Platform surveillance and resistance in Iran and Russia: The case of Telegram*, *Surveillance & Society*, 17 (1/2), p. 226.

⁷⁶ T. Lokot (2020), *Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia*, *Media and Communication*, 8(2), p. 316.

⁷⁷ *Ibid.*

“to rudely and arbitrarily control society, replace legitimate democratic institutions [and] restrict an individual’s natural right to decide how to live, what to choose and what viewpoints to freely express”. The speech emphasized that only the state should collect and control citizens’ data.⁷⁸

So, we can notice that the Russian authoritarian regime interpreted the activity of tech companies as a danger to its own power and saw the Russian state as competing with them for a valuable asset – personal data. The news that the Russian Government targeted Twitter followed shortly after Putin’s Davos speech.⁷⁹ The speed of Twitter was slowed down, after it failed to remove what the Russia’s media censors described as inappropriate content.⁸⁰

The Russian pre-invasion measures and methods to control the mass media and social content had wide spectrum – “from basic internet filtering to strategic ownership of domestic platforms”. The regime’s policy was based on securing access to data by “forcing foreign platforms to comply with demands for privacy invasion imposed by means of strategic legislation”. Social media networks were forced to share data with the state, if they wanted to exist and operate in Russia – companies such as Facebook complied. Also, in 2014, the State Duma passed the so-called “blogger law”. It required bloggers with a daily audience of 3,000 or more to register as mass media, consequently increasing bloggers’ “vulnerability to criminal prosecution”.⁸¹

Some social media channels attempted to challenge such an approach. Telegram is particularly worth mentioning here. It was founded in 2013 by the brothers Nikolai and Pavel Durov, in response to Russia’s action against the other popular Russian social media network VK. N. and P. Durov left VK (that they also founded and owned) in 2014, under claims that it had been taken over by the government.⁸²

P. Durov marketed Telegram as safe, privacy respecting messaging app and multiple times refused to hand the users encrypted data over to the Russian authoritarian regime – which is why he is regarded in Russia as both a dissident and a hero. Not only Russia, but

⁷⁸ Geopolitics, Sanctions And Social Media Giants: Putin’s Davos Speech, in Quotes (2021), *The Current Digest of the Russian Press*, 5/73, <<https://dlib-eastview-com.ezp-prod1.hul.harvard.edu/browse/doc/65934951>>.

⁷⁹ Russia Cracks Down on Twitter (2021), *The Current Digest of the Russian Press*, 11/73, pp. 3–6, 2021, <<https://dlib-eastview-com.ezp-prod1.hul.harvard.edu/browse/doc/67052305>>.

⁸⁰ According to the CNN, Russian “officials warned they would take action against social media companies that didn’t filter posts about protests that the Kremlin deemed as illegal or inciting people to demonstrate”. See more in: Anna Chernova, Zahra Ullah, “Russia’s Twitter crackdown ends up taking out government websites”, *CNN Business*, 2021, <<https://edition.cnn.com/2021/03/10/tech/russia-twitter-crackdown-website-outages/index.html>>.

⁸¹ A. Akbari, R. Gabbulhakov (2019), Platform surveillance and resistance in Iran and Russia: The case of Telegram, *Surveillance & Society*, 17 (1/2), p. 226.

⁸² Pavel Durov left Russia after being pushed out (22 April 2014), Agence France-Presse; Hakim, D. (2 December 2014), Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile, *The New York Times*.

also Iran demanded Telegram to localize its servers and grant them access to user data, but both failed as, “conflicting with totalitarian and strategic surveillance systems, Telegram entered the scene with a promise of freedom, privacy, and resistance”.⁸³

However, on 24 August 2024, Durov was arrested himself – on criminal charges relating to an alleged lack of content moderation on Telegram and refusal to work with police, which allowed the spread of criminal activity. We will discuss his situation in the next chapter.

Last but not the least, we should discuss the recent case law development, related to Russia – ECHR verdict in the case *PODCHASOV v. RUSSIA* (13 February 2024). The court questioned Russia’s “Statutory requirement” for “Internet communication organizers” to store and retain Internet communications and related communications data”, and to “provide law-enforcement authorities or security services access to those data and to decrypt encrypted communications”.⁸⁴

The Court concluded that Russia’s legislation, requiring to grant security services “direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications” violates the Convention: *“In so far as this legislation permits the public authorities to have access, on a generalized basis and without sufficient safeguards, to the content of electronic communications, it impairs the very essence of the right to respect for private life under Article 8 of the Convention. The respondent State has therefore overstepped any acceptable margin of appreciation in this regard”*.⁸⁵

The verdict was noticed in international arena of digital sphere activists. The Electronic Frontier Foundation called the verdict “a milestone judgment” in the fight to protect the “human right to privacy”.⁸⁶

5. Current developments: from the war in Ukraine to new EU regulations

The current development of legal and public discourse towards the protection of privacy and personal data in Lithuanian, Germany and Russia are marked by several significant events and processes: implementations of GDPR at the country levels (that in some cases, as we will see, bring even new court decisions and legal regulations to the EU level); rapid technological progress in the digital sphere that brings both threats and opportunities; deteriorating overall regional and global security environment – including Russia’s full

⁸³ A. Akbari, R. Gabdulhakov (2019), Platform surveillance and resistance in Iran and Russia: The case of Telegram, *Surveillance & Society*, 17 (1/2), p. 227.

⁸⁴ ECHR Case of Podchasov v. Russia, Application no. 33696/19, JUDGMENT, <[⁸⁵ *Ibid.*](https://hudoc.echr.coe.int/en-g/#{“itemid”:“001-230854”}”>https://hudoc.echr.coe.int/en-g/#{“itemid”:“001-230854”}”>>.</p></div><div data-bbox=)

⁸⁶ C. Schmon (5 March 2024), European Court of Human Rights Confirms: Weakening Encryption Violates Fundamental Rights, <<https://www EFF.org/deeplinks/2024/03/european-court-human-rights-confirms-undermining-encryption-violates-fundamental>>.

scale invasion of Ukraine, wars in the Middle East and Africa, tensions with China, more active espionage, terrorism, cybercrime, political extremism and growing other threats. Many of these threats are well reflected and addressed within the EU, using the umbrella term “hybrid threats”.⁸⁷

Such a global and regional environment poses threats to democracies and human rights globally – and the right to privacy and personal data protection is no exception. Tension and contradiction grow between the states’ authorities and control institutions, seeking easier access to personal data as the way to ensure public safety and security – and the institutional and legal environment, aimed at protecting personal privacy.⁸⁸

While large tech companies are even more eager to use data as the best resource for ensuring their business growth and perfecting marketing strategies. Today data globally is perceived as the “new oil”, “driving the business models of the digital economy” and posing “considerable privacy risks for those operating in the digital space”.⁸⁹

It is not a surprise, that this tension, gradually increasing over more than a decade, recently manifested in a famous judgment *Meta vs Bundeskartellamt*, delivered on 4 July 2023, by the European Court of Justice (Case C-252/21).⁹⁰ Having in mind the previous role of Germany in the formation of the European policies and legislation towards personal data protection, it is not a surprise that this decision also came as an outcome of conflicting attitudes towards personal data protection between German institutions and global tech corporations.

The background for the mentioned judgment was the 2019 competition decision from the federal competition authority in Germany, the Bundeskartellamt (Bka), against the activities of Meta (then known as Facebook). This agency found that “Meta’s practice of combining personal data across its many services, in addition to data collected through the integration of its services into third-party websites and apps, constitutes a violation of competition law”.⁹¹ (van de Waerd, 2023, 1077)

⁸⁷ On EU definition and actions towards the hybrid threats see more on: <https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en>.

⁸⁸ C. Coyer (28 August 2024), Personal Info in AI Models Threatens Split in US, EU Approach, *Bloomberg*, <<https://news.bloomberglaw.com/privacy-and-data-security/personal-info-in-ai-models-threatens-split-in-us-eu-approach>>.

⁸⁹ L. Hornuf, S. Mangold, Y. Yang (2023), Data Protection Law in Germany, the United States, and China, *Data Privacy and Crowdsourcing. Advanced Studies in Diginomics and Digitalization*, Springer, Cham, <https://doi.org/10.1007/978-3-031-32064-4_3>.

⁹⁰ Judgment of the Court (Grand Chamber) of 4 July 2023, *Meta Platforms Inc and Others v Bundeskartellamt*, Case C-252/21, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252>>.

⁹¹ Peter J. van de Waerd (2023), From Monocle to Spectacles: Competition for Data and ‘Data Ecosystem Building’, *European Competition Journal*, 19 (2): 191–225. doi:10.1080/17441056.2023.2169366.

The mentioned decision was made cooperating with German data protection institutions. It concluded that Facebook has abused its dominant market position on the basis of a violation of the General Data Protection Regulation (GDPR). According to Peter J. van de Waerdt, the relationship between EU competition law and data protection law has become even more prominent since then.⁹²

The Court of Justice of the European Union imposed strict limitations on the personalized use of consumers' personal data by social media platforms – especially in the cases when personal data are used for targeted advertising. The CJEU ruled that competition authorities of a Member State have the authority to investigate and sanction an infringement of the GDPR in the cases when companies exploit their dominant market position.⁹³

The CJEU ruled that “apart from consent, no legal bases from the GDPR justify Facebook's data processing”.⁹⁴

Recently the new document – Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Article on Lawfulness of processing) was published. Among the other issues, it also explains what is the acceptable legal order within the EU when it comes to personal data collection and disclosure in the cases of criminal and other threats. According to the Guidelines, “indicating possible criminal acts or threats to public security and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal acts or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller”.⁹⁵

But there are limitations: “the reference to “individual cases” and “same criminal acts or threats” suggests that the generalized and preventive collection of personal data by private business operators to systematically report possible criminal acts or threats to law enforcement authorities is not what is envisaged (...) as a legitimate interest pursued by the controller”.⁹⁶

According to the document, “in any event, such transmission should be prohibited if the processing is incompatible with legal, professional or other binding obligation of secrecy of the controller”, because “in *Meta v. Bundeskartellamt* the CJEU found that, in principle, collecting and sharing personal data with law enforcement authorities in order to prevent, detect and prosecute criminal offenses is not an objective that is capable of constituting a legitimate interest pursued by a private business operator whose activity

⁹² *Ibid.*, p. 1077.

⁹³ Judgment of the Court (Grand Chamber) of 4 July 2023, *Meta Platforms Inc and Others v. Bundeskartellamt*, Case C-252/21, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252>>.

⁹⁴ *Ibid.*

⁹⁵ Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, Adopted on 8 October 2024, p. 35, <https://www.edpb.europa.eu/system/files/202410/edpb_guidelines_202401_legitimateinterest_en.pdf>.

⁹⁶ *Ibid.*

is essentially economic and commercial in nature”. However, in some cases the transfer of such data to the authorities is possible, as “business operator may share information with law enforcement authorities on the basis of Article 6(1)(c) GDPR, provided that, processing is necessary to comply with a specific legal obligation to which that operator is subject”.⁹⁷

In the case if “the third country authority” requests to access data, “The controller must first analyse the context and legal framework of the request. If it results from the implementation of an international agreement, which makes such request binding and enforceable under EU or Member State law, the disclosure may be mandatory and, thus, constitute a legal obligation under Article 6(1)(c) GDPR”.⁹⁸

However, “in situations where disclosure based on an international agreement is not mandatory, but such cooperation is permitted under EU or Member State law, Article 6(1)(e) GDPR could apply. Furthermore, in specific cases, the vital interests of the data subject (or another natural person may justify the reply to a request from a third country authority, provided that the conditions set out in international law are met and, thus, Article 6(1)(d) GDPR could be applicable.”⁹⁹

The guidelines state that “A controller could nevertheless have a legitimate interest in complying with a request to disclose personal data to a third country authority, in particular if the controller is subject to third country legislation and non-compliance with such request would entail sanctions under foreign law” but “any processing based on a legitimate interest pursued by the controller must also be necessary and balanced against the interests or fundamental rights and freedoms of the data subjects”.¹⁰⁰

Thus, we can see how different the EU law (mostly designed with the leadership of Germany, but mandatory in other countries, including Lithuania) is from the Russian law of “networked authoritarianism” described in a previous chapter.

It does not mean that the public discourse does not reflect debates and concerns in both EU countries under our analysis.¹⁰¹

One of the latest controversies – related to both EU and Russia – is the arrest of (in?) famous and already mentioned Telegram founder, Pavel Durov, in Paris last August. Telegram’s long-lasting policy not to disclose the encrypted data to the authorities in such

⁹⁷ *Ibid.*, p. 35–36.

⁹⁸ *Ibid.*, pp. 36–37.

⁹⁹ *Ibid.*, p. 37.

¹⁰⁰ *Ibid.*, p. 37.

¹⁰¹ Nuo liepos – pokyčiai asmens duomenų apsaugos srityje: kas svarbiausia? (25 June, 2024), <https://www.15min.lt/verslas/naujiena/finansai/nuo-liepos-pokyciai-asmens-duomenu-apsaugos-srityje-kas-svarbiausia-662-2263640?utm_medium=copied>; Wegner will Datenschutz in Deutschland neu diskutieren (15 May, 2024), <<https://www.rbb24.de/politik/beitrag/2024/05/berlin-wegner-japan-japanreise-digitalisierung-datenschutz-big-data.html>>.

countries as Russia and Belarus meant giving room for protest action, saving freedom of speech and, possibly protesters' and opposition activists' freedom or even lives.¹⁰²

However, according to the article in *Le Monde*:

"Inside the European Union (EU), in an open media context, Telegram is of little interest to news sites, political movements or non-profits, which have other communication spaces at their disposal. By contrast, illegal content thrives there". Also, In Russia and well beyond its borders, the platform has been taken over by traffickers of all kinds. It is home to drug, arms and prostitution networks, as well as a wide variety of conspiracy sites".¹⁰³

The arrest of Durov was interpreted in the public discourse mostly in the context of the Digital Services Act (DSA) – an EU regulation adopted in 2022.¹⁰⁴

This regulation addresses illegal content, transparent advertising and disinformation and updates the Electronic Commerce Directive 2000 in EU law. The DSA applies to online platforms and intermediaries. DSA bans targeted advertising based on a person's sexual orientation, religion, ethnicity, or political beliefs and puts restrictions on targeting ads to children. Key requirements also include disclosing to regulators how their algorithms work, providing users with explanations for content moderation decisions, and implementing stricter controls on targeted advertising. It also imposes specific rules on "very large" online platforms and search engines (those with more than 45 million monthly active users in the EU).¹⁰⁵

Some observers believe that adoption of DSA was related to the Russia's full-scale invasion to Ukraine – as with Russia using social media platforms to spread misinformation about the 2022 Russian invasion of Ukraine, European policymakers felt a greater sense of urgency to move the legislation forward to ensure that major tech platforms were transparent and properly regulated.¹⁰⁶

In Durov's case, however, the EU commission denied that his arrest was related to the DSA, claiming:

¹⁰² O. Herrero, V. Goury-Laffont, E. Braun (5 September 2024) France's hunt for Telegram CEO Pavel Durov: The inside story, <<https://www.politico.eu/article/the-hunt-for-pavel-durov/>>.

¹⁰³ F. Daucé (5 September 2024), Pavel Durov's arrest marks the emergence of sovereign digital spaces, *Le Monde*, <https://www.lemonde.fr/en/opinion/article/2024/09/05/pavel-durov-s-arrest-marks-the-emergence-of-sovereign-digital-spaces_6724871_23.html#>>.

¹⁰⁴ A. Hern (27 August, 2024), What the Telegram founder's arrest means for the regulation of social media firms, *The Guardian*, <<https://www.theguardian.com/technology/article/2024/aug/27/what-does-the-telegram-founders-arrest-mean-for-the-regulation-of-social-media-companies-pavel-durov>>.

¹⁰⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), <<https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>>;

¹⁰⁶ C. Zakrzewski (22 April, 2022), Europe to slap new regulations on Big Tech, beating U.S. to the punch, *The Washington Post*, <<https://www.washingtonpost.com/technology/2022/04/22/european-lawmakers-digital-services/>>.

“Criminal prosecution is not among the potential sanctions for a breach of the DSA. The DSA does not define what is illegal nor does it establish any criminal offence and can therefore not be invoked for arrests. Only national [or international] laws that define a criminal offence can be invoked”.¹⁰⁷

According to Samuel Duraivel, “The arrest of Pavel Durov, the CEO of Telegram, represents a critical moment in the ongoing discourse surrounding free speech and content moderation. This event exemplifies the tension between upholding individual liberties and addressing the potential societal harms caused by unregulated digital communication”.¹⁰⁸

Telegram plays an important role during Russia’s war in Ukraine. According to Le Monde – as the Russian state, unable to ban it, decided to use it for its own purposes, including official channels of Kremlin.¹⁰⁹

So, the app is used by the Russian authorities for the purpose of information warfare. However, multiple Ukrainian communities, from the first months of the full-scale invasion phase of the war, also used Telegram to gain and spread knowledge on such topics as the course of military action, Russian atrocities and humanitarian aid – this can be said also about such Ukrainian mass media channels as UNIAN.¹¹⁰

The technical possibilities such as Telegram – according to scholars, a highly popular platform in Ukraine – created a new reality of war, experienced by the rise of inconspicuous war witnessing.¹¹¹

But Telegram is just one aspect here. This war, determined by Russian aggression, can be characterized by a large number of digital innovations and widely-used cyber warfare. Rising concerns of data security, including personal data, is an important component here.

First of all, Russia attempted to spread its policies towards digital data and personal privacy (non)protection to the occupied territories of Ukraine and war zones. According to Lokot, “Russia’s full-scale invasion of Ukraine in February 2022 has seen the Kremlin

¹⁰⁷ C. Kroet (26 August 2024), Arrest of Telegram CEO has nothing to do with DSA, Commission says, *Euronews*, <<https://www.euronews.com/my-europe/2024/08/26/eu-commission-distances-itself-from-french-telegram-spat>>.

¹⁰⁸ S. Duraivel (2024), The Arrest of Telegram CEO Pavel Durov: A Crossroad between Free Speech and Content Moderation through the Lens of the Harm Principle, Preprints 2024, No. 2024082053, <<https://doi.org/10.20944/preprints202408.2053.v1>>.

¹⁰⁹ F. Daucé (5 September 2024), Pavel Durov’s arrest marks the emergence of sovereign digital spaces, *Le Monde*, <https://www.lemonde.fr/en/opinion/article/2024/09/05/pavel-durov-s-arrest-marks-the-emergence-of-sovereign-digital-spaces_6724871_23.html#>>.

¹¹⁰ P. Gerard, S. Volkova, L. Penafiel, K. Lerman, T. Weninger (2024), *Modeling Information Narrative Detection and Evolution on Telegram during the Russia-Ukraine War*, <<https://arxiv.org/abs/2409.07684>>.

¹¹¹ M. Bareikytė, M. Makhortykh (2024), Digitally witnessable war from pereklychka to propaganda: Unfolding Telegram communication during Russia’s war in Ukraine, *Media, War & Conflict*, 0(0).

mixing its usual external cyber warfare tactics with internet control and information manipulation approaches inspired by its internal networked authoritarian regime".¹¹²

According to Lokot, this – together with attacks on Ukrainian communication systems and critical infrastructure – had multiple consequences. It disconnected the populations of occupied Ukraine from any trustworthy sources of information, including the information about the real situation outside the occupied zones. Also, "Russia's seizure of control over telecommunications infrastructure means Ukrainian civilians in occupied regions are increasingly subject to Russian internet regulations, surveillance, and censorship characteristic of the networked authoritarian regime". Ukrainians also became targets of punishment for "violating the draconian Russian internet regime", that are "similar to those habitually faced by Russians" in Russia. Russia also targets and surveils digital communications of Ukrainians in the occupied zones, to search for proof of their loyalty to Ukraine – and this has led and can lead to severe punishments.¹¹³

In this context, Ukraine itself faced the urgent need to protect its citizens in warzones and occupied territories, who were helping Ukrainian armed forces in data collection. According to Paul Burke, who recognizes the value of such data for Ukraine defence forces, such activities also increased the risks for civilians to become targets of the Russian military: as "citizen-derived or crowdsourced Intelligence has provided an additional strand of source reporting for Ukraine during the conflict", the ethical question came into being, related to the "citizens putting themselves in ever-greater danger to collect information which they believe may be useful".¹¹⁴

On the other hand, the overall awareness about the importance of data security increased in Ukraine and beyond. As "the Russian Invasion of Ukraine in early 2022 resulted in a rapidly changing (cyber) threat environment", a new trend has emerged in Ukrainian social media: sharing advice on personal data security. The awareness of data security increased – although still much more needs to be learned and done.¹¹⁵

According to Lokot: "Ukrainian citizens, whether military or civilian, will benefit from a broadening effort to increase digital literacy, empowering them to protect their privacy and their security online and to make informed decisions about verified information sources and trustworthy digital actors".¹¹⁶ This provides an opportunity for the entire EU to learn from Ukraine's experiences – and to reduce the privacy data violations risks and the

¹¹² T. Lokot (2023), Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience, *In Ukraine*, p. 145.

¹¹³ *Ibid.*, 153.

¹¹⁴ P. Burke (2022), The Issues in the Collection, Verification and Actionability of Citizen-Derived and Crowdsourced Intelligence during the Russian Invasion of Ukraine, *Strategic Panorama*, November, 94–103, p. 94.

¹¹⁵ Schmüser [et al.], 2022.

¹¹⁶ T. Lokot (2023), Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience, *In Ukraine*, p. 158.

lack of digital literacy in the future, especially if the security situation in Europe further deteriorates.

Conclusions

As the analysis presented in this article has demonstrated, Lithuania, Eastern Germany and Russia, despite different pre-state socialist and post- state socialist trajectories, after the collapse of state socialism in the 1990s, had similar experiences and approaches, related to the communist period of history. They were at the same starting position in the beginning of attempts to build the rule of law in the 1990s.

However, their trajectories later diverged. While Lithuania and reunited Germany, guided by the heritage of the privacy law coming from 20th century Western Germany, started to develop and further strengthen the right to privacy and personal data protection, Russia, sinking into authoritarianism, developed so-called “networked authoritarianism”.

Of these three countries, Germany still seems to be the most concerned about the protection of the right to privacy. But Lithuania, as a EU member, is following this example.

Today – especially after the full-scale aggression against Ukraine – the split between EU members Germany and Lithuania and Russia is even more obvious, as rights of Russian citizens are further targeted and violated, including the rights to privacy and personal data protection. This also applies to Ukrainian citizens in Russian occupied territories. Keeping in mind the harsh reality of Russia’s war of aggression and in honour of the Russian victims in Ukraine, it is worth mentioning that Ukraine today is teaching the EU an important lesson: to be more concerned and careful about the protection of sensitive data, including privacy-related data.

However, as the case of Telegram’s CEO Pavel Durov demonstrates, protection of personal data faces new challenges even in Western democracies. Interference in encrypted data by the state agencies today can be justified by their need to ensure general safety and security – and that further challenges the right to privacy.

Sources and literature

Legal sources, regulations and explanatory statements

1. Abstract of the Federal Constitutional Court's Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html>.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>>.
3. ECHR Case of Podchasov V. Russia, Application no. 33696/19, JUDGMENT, <[https://hudoc.echr.coe.int/eng/#{"itemid":\["001-230854"\]}](https://hudoc.echr.coe.int/eng/#{)>.
4. European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15; supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Strasbourg, <https://www.echr.coe.int/documents/d/echr/convention_ENG>.
5. Federal Law of 27 July 2006 N 152-FZ on personal data, accessible online: <<https://pd.rkn.gov.ru/authority/p146/p164/> [last visited 30-08-2023]>.
6. General Data Protection Regulation, Article 4-1, <<https://gdpr.eu/article-4-definitions/>>.
7. German Federal Constitutional Court (Bundesverfassungsgericht), decision of 27/02/2008 – 1 BvR 370/07, 1 BvR 595/07 – BVerfGE 120, 274, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html>.
8. Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0 Adopted on 8 October 2024, <https://www.edpb.europa.eu/system/files/202410/edpb_guidelines_202401_legitimateinterest_en.pdf>.
9. Įstatymas „Dėl SSRS valstybės saugumo komiteto (NKVD, NKGB, MGB, KGB) vertinimo ir šios organizacijos kadrinių darbuotojų dabartinės veiklos“, 1998 m. birželio 30 d. Nr. VIII-823, <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/TAIS.59758?jfwid=-n2mqd3363>>.
10. Judgment of the Court (Grand Chamber) of 4 July 2023. Meta Platforms Inc and Others v Bundeskartellamt. Case C-252/21, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252>>.
11. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), <<https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>>.
12. Republic of Lithuania Law on Legal Protection of Personal Data, 11 June 1996 No I-1374 (As last amended on 3 November 2016 – No XII-2709), <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae>>.
13. The Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626), <https://www.gesetze-im-internet.de/englisch_bds/englisch_bds.html#p0012>.

14. The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights, 4 August 2022,
<<https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf>>.
15. UN Press Release, Office of the High Commissioner for Human Rights, "Spyware and surveillance: Threats to privacy and human rights growing, UN report warns", 16 September 2022,
<<https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>>.
16. "What is GDPR, the EU's new data protection law?",
<<https://gdpr.eu/what-is-gdpr/>>.

Mass Media Sources

1. Coyer C. (28 August 2024), Personal Info in AI Models Threatens Split in US, EU Approach, *Bloomberg*,
<<https://news.bloomberglaw.com/privacy-and-data-security/personal-info-in-ai-models-threatens-split-in-us-eu-approach>>.
2. Chernova A. (2021), Zahra U., Russia's Twitter crackdown ends up taking out government websites, *CNN Business*,
<<https://edition.cnn.com/2021/03/10/tech/russia-twitter-crackdown-website-outages/index.html>>.
3. Daucé F. (5 September 2024), Pavel Durov's arrest marks the emergence of sovereign digital spaces", *Le Monde*,
<https://www.lemonde.fr/en/opinion/article/2024/09/05/pavel-durov-s-arrest-marks-the-emergence-of-sovereign-digital-spaces_6724871_23.html#>.
4. Dėl sąmoningo liustracijų vilkinimo (14 November 2007), *XXI amžius*, 84/1581, 14,
<http://www.xxiamzius.lt/numeriai/2007/11/14/nuom_02.html>.
5. Geopolitics, Sanctions And Social Media Giants: Putin's Davos Speech, in Quotes (2021), *The Current Digest of the Russian Press*, 5/73,
<<https://dlib-eastview-com.ezp-prod1.hul.harvard.edu/browse/doc/65934951>>.
6. Hacker who leaked CityBee user data tells media cyber security was poor (February 17, 2021, *BNS, LRT*,
<<https://www.lrt.lt/en/news-in-english/19/1346403/hacker-who-leaked-citybee-user-data-tells-media-cyber-security-was-poor>>.
7. Hakim D. (2 December 2014), Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile, *The New York Times*.
8. Hern A. (27 August, 2024), What the Telegram founder's arrest means for the regulation of social media firms, *The Guardian*,
<<https://www.theguardian.com/technology/article/2024/aug/27/what-does-the-telegram-founders-arrest-mean-for-the-regulation-of-social-media-companies-pavel-durov>>.

9. Herrero O., Goury-Laffont V., Braun E. (5 September 2024) France's hunt for Telegram CEO Pavel Durov: The inside story, <<https://www.politico.eu/article/the-hunt-for-pavel-durov/>>.
10. Kroet C. (26 August 2024), Arrest of Telegram CEO has nothing to do with DSA, Commission says, *Euronews*, <<https://www.euronews.com/my-europe/2024/08/26/eu-commission-distances-itself-from-french-telegram-spat>>.
11. Laiškai iš gulago (1979), *Lietuvos Katalikų Bažnyčios kronika*, Nr. 39, <<https://lkbkronika.lt/index.php/39-kronika-1979-m>>.
12. Lietuva in Brief (14 June 2012), *The Baltic Times*, 805.
13. Lithuanian Parliament Removes Country's President after Casting Votes on Three Charges, 7 April 2004), *The New York Times*, <<https://www.nytimes.com/2004/04/07/world/lithuanian-parliament-removes-country-s-president-after-casting-votes-three.html?pagewanted=1>>.
14. Lithuania short of cyber sleuths (15 March 2015), *The Baltic Times*, 856, 4.
15. Nuo liepos – pokyčiai asmens duomenų apsaugos srityje: kas svarbiausia? (25 June, 2024), <https://www.15min.lt/verslas/naujiena/finansai/nuo-liepos-pokyčiai-asmens-duomenu-apsaugos-srityje-kas-svarbiausia-662-2263640?utm_medium=copied>.
16. Online Data at Risk to Hackers (2014), *The Baltic Times*, 842, January.
17. Pavel Durov left Russia after being pushed out (22 April 2014), *Agence France-Presse*.
18. Racas A. (4 December 2003), Doubts on privacy rights raised in scandal, *The Baltic Times*, 386.
19. Roth, E. (25 August 2023), The EU's Digital Services Act goes into effect today: here's what that means, <<https://www.theverge.com/23845672/eu-digital-services-act-explained>>.
20. Russia Cracks Down on Twitter (2021), *The Current Digest of the Russian Press*, 11/73, 3–6, 2021, <<https://dlib-eastview-com.ezp-prod1.hul.harvard.edu/browse/doc/67052305>>.
21. Schmon C. (5 March 2024), European Court of Human Rights Confirms: Weakening Encryption Violates Fundamental Rights, <<https://www.eff.org/deeplinks/2024/03/european-court-human-rights-confirms-undermining-encryption-violates-fundamental>>.
22. Sytas A. (22 September 2021), Lithuania says throw away Chinese phones due to censorship concerns, *Reuters*, <<https://www.reuters.com/business/media-telecom/lithuania-says-throw-away-chinese-phones-due-censorship-concerns-2021-09-21/>>.
23. TeamViewer will, erste datenschutzkonforme' Unterrichtssoftware anbieten (28 September 2021), *Spiegel Netzwelt*, accessible online: <<https://www.spiegel.de/netzwelt/web/teamviewer-will-erste-daten-schutzkonforme-unterrichts-software-anbieten-a-87a2ed5d-c4d0-41f9-8335-02a72be19890>>.

24. Wegner will Datenschutz in Deutschland neu diskutieren (15 May, 2024), <<https://www.rbb24.de/politik/beitrag/2024/05/berlin-wegner-japan-japanreise-digitalisierung-datenschutz-big-data.htm>>.
25. Zakrzewski C. (22 April, 2022), Europe to slap new regulations on Big Tech, beating U. S. to the punch, *The Washington Post*, <<https://www.washingtonpost.com/technology/2022/04/22/european-lawmakers-digital-services/>>.

Academic literature

1. Akbari A., Gabdulhakov R. (2019), Platform surveillance and resistance in Iran and Russia: The case of Telegram, *Surveillance & Society*, 17 (1/2), pp. 223–231.
2. Arendt H. (2013), *The Human Condition: Second Edition*, University of Chicago Press.
3. Bareikytė M., Makhortykh M. (2024), Digitally witnessable war from pereklychka to propaganda: Unfolding Telegram communication during Russia's war in Ukraine, *Media, War & Conflict*, 0(0), <<https://doi.org/10.1177/17506352241255890>>.
4. Bateman A. (2016), The KGB and Its Enduring Legacy, *The Journal of Slavic Military Studies*, 29/1, pp. 23–47.
5. Beinoravičius D., Keršulienė V., *Privacy Protection in the Transmission of Personal Data in Business – Insights from Lithuania*. 12th International Scientific Conference “Business and Management 2022”, May 12–13, 2022, Vilnius, Lithuania.
6. Beissinger M. R. (2006), Soviet Empire as ‘Family Resemblance’, *Slavic Review*, 65/2, pp. 294–303.
7. Bitiukova N. (2021), Lithuania Reports: GDPR Implementation Series, *European Data Protection Law Review (EDPL)*, Vol. 7, No. 1, 2021, pp. 108–114.
8. Burinskaite K. (2011), LSSR KGB veiklos ideologiniai ir politiniai aspektai 1954–1990 m., [Doctoral Thesis], Vilnius University.
9. Burke P. (2022), The Issues in the Collection, Verification and Actionability of Citizen-Derived and Crowdsourced Intelligence during the Russian Invasion of Ukraine, *Strategic Panorama*, November, pp. 94–103, <<https://doi.org/10.53679/2616-9460.specialissue.2022.09>>.
10. Duraivel S. (2024), The Arrest of Telegram CEO Pavel Durov: A Crossroad between Free Speech and Content Moderation through the Lens of the Harm Principle, Preprints 2024, No. 2024082053, <<https://doi.org/10.20944/preprints202408.2053.v1>>.
11. Fitzpatrick S. (2007), Revisionism in Soviet History, *History and Theory*, 46/4, 2007, pp. 77–91.
12. Gerard P., Volkova S., Penafiel L., Lerman K., Weninger T. (2024), *Modeling Information Narrative Detection and Evolution on Telegram during the Russia-Ukraine War*, <<https://arxiv.org/abs/2409.07684>>.
13. Greene S. (2012), *How much can Russia really change? The durability of networked authoritarianism*, Washington, DC: PONARS Eurasia.

14. Halmai G. (2007), Lustration and Access to the Files in Central Europe, *Lustration and Consolidation of Democracy and the Rule of Law in Central and Eastern Europe*, 5, Zagreb, pp. 17–46.
15. Hornuf L., Mangold S., Yang Y. (2023), *Data Protection Law in Germany, the United States, and China. Data Privacy and Crowdsourcing. Advanced Studies in Diginomics and Digitalization*. Springer, Cham.,
<https://doi.org/10.1007/978-3-031-32064-4_3>.
16. Jarausch, K. (2014), Between Myth and Reality: The Stasi Legacy in German History. *The Stasi at Home and Abroad: Domestic Order and Foreign Intelligence*, *Bulletin of the German Historical Institute*, 52, Supplement 9, Washington DC, USA, pp. 73–83.
17. Kareniauskaitė M. (2017), Crime and punishment in Lithuanian SSR, [Doctoral Thesis], Vilnius University.
18. Khubova D. N. (1994), Imprisoned History: the KGB archives, *The Journal of the International Institute*, Vol. 1, Issue 1, Winter,
<<https://quod.lib.umich.edu/j/jii/4750978.0001.103?view=text;rgn=main>>.
19. Leboukh F., Baba Aduku E., Ali O. (2023), Balancing ChatGPT and Data Protection in Germany: Challenges and Opportunities for Policy Makers, *Journal of Politics and Ethics in New Technologies and AI*, 2(1), e35166,
<<https://doi.org/10.12681/jpentai.35166>>.
20. *Lietuva 1940–1990: Okupuotos Lietuvos istorija* (2007), Anušauskas A. [et al.], Vilnius: Lietuvos gyventojų genocido ir rezistencijos tyrimo centras.
21. Lisiak-Felicka D., Szmit M., Vaičiūnienė J. (2022), The General Data Protection Regulation 3 Years After. Implementation: A Comparison between Local Government Administration in Poland and the Republic of Lithuania, *European Research Studies Journal*, XXV, 1, pp. 382–394.
22. Lokot T. (2018), Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices, *Surveillance & Society*, 16/3, pp. 332–346.
23. Lokot T. (2020), Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia, *Media and Communication*, 8(2), pp. 314–322.
<https://doi.org/10.17645/mac.v8i2.2883>
24. Lokot T. (2023), Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience, *In Ukraine*.
25. Lubonja F. (2001), Privacy in a Totalitarian Regime, *Social Research*, 68, 1, Privacy (Spring), pp. 237–254.
26. MacKinnon R. (2011), Liberation technology: China's 'networked authoritarianism', *Journal of Democracy*, 22/2, 2011, pp. 32–46.
27. Mačernytė-Panomariovienė I. (2023), Discrimination on the Basis Of Personal Data in Employment: The Case Study of Lithuania, *Baltic Journal of Law & Politics* 16:1, pp. 24–41,
<<https://content.sciendo.com/view/journals/bjlp/bjlp-overview.xml>, DOI: 10.2478/bjlp-2023-0002>.

28. Molnár-Gábor F. (2018), Germany: a fair balance between scientific freedom and data subjects' rights?, *Human Genetics*, 137, pp. 619–626, <<https://doi.org/10.1007/s00439-018-1912-1>>.
29. Müller-Enbergs H. (2008), *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 3: Statistiken*, Berlin: Christoph Links Verlag.
30. Norkus Z. (2008), *Kokia demokratija, koks kapitalizmas?: pokomunistinė transformacija Lietuvoje lyginamosios istorinės sociologijos požiūriu*, Vilnius: Vilniaus universiteto leidykla.
31. Preuß C., Paul J. A. (2008), *German Constitutional Court creates a new fundamental 'IT Privacy' Right*, September, Bird & Bird, Accessible online: <<https://www.twobirds.com/en/news/articles/2008/germanconstitutional-court-creates-a-new-fundamental-it-privacy-right>>.
32. Ptaszek G., Yuskiv B., & Khomych S. (2024), War on frames: Text mining of conflict in Russian and Ukrainian news agency coverage on Telegram during the Russian invasion of Ukraine in 2022, *Media, War & Conflict*, 17(1), pp. 41–61, <<https://doi.org/10.1177/17506352231166327>>.
33. Pūraitė A., Šilinskė N. (2021), State Regulation of Privacy and Its Protection in the use of VIRDs By Police: Comparative Perspective From Latvia and Lithuania, *Public Security and Public Order*, 27.
34. Ravaitytė J. (2015), Evaluation of The Lustration Policy in Lithuania, *Politologija*, 77/1, pp. 49–100.
35. Schmeidel J. C., *Stasi. Shield and Sword of the Party*, London: Routledge, 2007.
36. Sietmann R. (1991), East German Cancer Data: A Benefit of Big Brother? A detailed database put together by totalitarian East Germany may tempt the new Germany to relax privacy laws, *Science, New Series*, 252/5008, <<https://www.jstor.org/stable/2875334>>.
37. Spindler G. (2016), Consumer Data Protection in Germany, Metz R., Binding J., Haifeng P., Huber P. (eds.), *Consumer Data Protection in Brazil, China and Germany. A Comparative Study*, Göttingen: Göttingen University Press.
38. Teubert W. (2010), *Meaning, discourse and society*, Cambridge University Press.
39. The Stasi at Home and Abroad: Domestic Order and Foreign Intelligence, *Bulletin of the German Historical Institute*, (2014), 52, 9, Washington DC, USA.
40. Tucker B. (1985), *State Socialism and Anarchism and Other Essays: Including the Attitude of Anarchism Toward Industrial Combinations and Why I Am an Anarchist* (1st ed.), Colorado Springs: Ralph Myles Publisher.
41. Waerd Peter J. van de (2023), From Monocle to Spectacles: Competition for Data and 'Data Ecosystem Building', *European Competition Journal*, 19 (2): 191–225, doi:10.1080/17441056.2023.2169366.
42. Waller Michael J. (2004), Russia: Death and Resurrection of the KGB, *Demokratizatsiya: The Journal of Post-Soviet Democratization*.