re:constitution
Working Paper

Monika Kareniauskaitė

Privacy and Personal Data Protection in Russia, Lithuania and Germany: Law, Legacy and Cyber Shift

working papers, Forum Transregionale Studien 8/2022

re:constitution - Exchange and Analysis on Democracy and the Rule of Law in Europe
c/o Forum Transregionale Studien e. V., Wallotstr. 14, 14193 Berlin

Monika Kareniauskaitė
Privacy and Personal Data Protection in Russia, Lithuania and Germany: Law, Legacy and Cyber Shift
Working Papers, Forum Transregionale Studien 8/2022
DOI: https://doi.org/10.25360/01-2022-00057

Design: Plural | Severin Wucher

The Forum Transregionale Studien is an institutional platform for the international cooperation between scholars of different expertise and perspectives on global issues. It is funded by the Berlin Senate Department for Higher Education and Research, Health, Long-term Care and Gender Equality.

Working Papers are available in open access via *perspectivia.net*, the publication platform of the Max Weber Stiftung.

re:constitution - Exchange and Analysis on Democracy and the Rule of Law in Europe is a joint programme of the Forum Transregionale Studien and Democracy Reporting International, funded by Stiftung Mercator.

Abstract

The aim of research presented in this paper is to study the ideas and perceptions on digital-sphere related privacy, control and security in three different societies: Germany, Lithuania and Russia. The paper is investigating if –and if yes, how– the historical ideas and beliefs about privacy and personal data protection are still shaping the experiences, law, perceptions and behaviour in the digital word of these three different populations, united by similar historical experiences of living in non-democratic societies. As a mean of investigating the views and opinions on privacy and data protection in Germany, Lithuania and Russia, a pilot survey was designed and tested. It was combined with the analysis of legal sources. Combining the analysis of laws and legal documents with quantitative data, historical approaches with contemporary statistical analysis turned out to be a fruitful strategy to measure different approaches towards the privacy and data security in Russia, Germany and Lithuania. As the collected data demonstrate, we can raise the hypothesis that the legal regimes and privacy definitions of the past still impact today's societies.

Keywords: Personal Data Protection, Privacy, Digitalization, Law, History, Germany, Russia, Lithuania

Suggested Citation:

Kareniauskaite, Monika, "Privacy and Personal Data Protection in Russia, Lithuania and Germany: Law, Legacy and Cyber Shift", re:constitution Working Paper, Forum Transregionale Studien 8/2022, available at https://reconstitution.eu/working-papers.html

Privacy and Personal Data Protection in Russia, Lithuania and Germany: Law, Legacy and Cyber Shift

Monika Kareniauskaitė[1]

Introduction

The driving idea behind this paper was to study the perceptions on digital-space related privacy, control and security in three different countries / legal systems: Germany, Lithuania and Russia. The paper investigates whether the historical ideas and beliefs behind privacy laws and personal data protection are still shaping the experiences, perceptions and behaviour in the digital word in these countries having been, united by similar historical experiences. All three countries – Russia, Lithuania and Germany– do have a legacy of their non-democratic past, defined, first of all, by the state-socialist legal systems.

When one takes the historical perspective into consideration, it is obvious that Lithuania, as a part of the USSR, was put under a unified Soviet system of criminal prosecution, and the Lithuanian KGB[2] officers reported directly to Moscow. Therefore, looking from the historical perspective, the way how Soviet Lithuania and Soviet Russia treated their residents in matters related to their privacy (and violation of that privacy) was more or less similar. Having said that, the unified Germany is a different case: being divided into Eastern and Western states meant also a division between a dictatorship and a democracy. It is well researched by historians today[3]

[1] Dr Monika Kareniauskaitė, a re:constitution programme Fellow in 2020-2021, specializes in Soviet and post-Soviet history, law, gender and criminality. Her research and interests cover criminal prosecution systems in Soviet and post-Soviet Lithuania and the USSR, anti-Soviet resistance, Soviet political trials and deportations, the dissident movement and the culture of remembrance in the former Eastern Bloc, and techniques of digital humanities. In 2017 she received a PhD in History (Vilnius University). She has been a Research Fellow at the University of St. Gallen (Switzerland, 2013-2014), a project coordinator and research assistant at the Berlin-Hohenschönhausen Memorial (2015), a leader of a research project on gender-based violence in twentieth-century Lithuania, a Postdoctoral Associate at Yale University (2019). She is currently a visiting fellow at the Davis Center for Russian and Eurasian Studies at Harvard University.

[2] The KGB, the Committee for State Security (Russian: Комитет государственной безопасности, КГБ) 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. The central KGB of the USSR had branches in the other Soviet republics. KGB was successor of preceding agencies such as the Cheka, GPU, OGPU, NKGB, NKVD and MGB. See more in: Aaron Bateman, "The KGB and Its Enduring Legacy", *The Journal of Slavic Military Studies*, 29/1, 2016, 23-47.

[3] See, for instance: John Christian Schmeidel, *Stasi. Shield and Sword of the Party*, Routledge: London and New York, 2008, 5.

that the activities of the Stasi[4], connected to personal privacy violations, intruded the Federal Republic of Germany and as such, after the reunification the state-socialist heritage became a shared burden of the whole German population[5].

However, investigating the historical definitions of the concepts of 'privacy' and 'control' is only a part of the research ideas discussed by this paper. The paper also asks the question if the Soviet and state-socialist perspectives on privacy rights still impact today's national law, legal practices and the general understanding about the privacy rights issues in Russia, Germany and Lithuania. It is also important to investigate the vulnerabilities / difficulties that Eastern European societies might encounter or are already experiencing due to their communist past and because of their long experience of living under legal systems that rather imitated than implemented the basic democratic principles concerning the rule of law, legality and justice. Current concerns on privacy and personal data protection also provide the background for the relevance of the research, presented in this paper.

It is important to stress, that the author of this paper completely acknowledges the research design's risks and limitations. It must also be stressed that researching the impact of historical ideas and beliefs in current societies is a problematic task on its own. The research presented here should be understood as a pilot study, proposing some initial insights on how this task could be approached. Thus, the findings of this paper should not be treated as final statements and conclusions but rather as general landmarks that may defy the directions of similar research projects of future. It is also important to emphasize that research is ongoing and some new data are to be collected and the final results will be published as a peer-reviewed academic paper in the near future.

In this working paper, the different steps of the research process and the initial observations are presented. The following steps of analysis were taken during the mentioned academic year:

a) Analysis of the law in force and the law of the state-socialist past.
b) The analysis of the press, focusing on how the concepts of 'crime', 'privacy', 'control' and 'the rule of law' were defined in the past in the public sphere – and what their content is today.

[4] The Ministry for State Security (German: 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 KGB was the Soviet counterpart and close partner of the Stasi. The Stasi had headquarteres in East Berlin. One of the Stasi's main tasks was spying on the population through a vast network of citizens-turned-informants. It arrested 250,000 people as political prisoners. 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.

[5] See, for instance: Konrad Jarausch, "Between Myth and Reality: The Stasi Legacy in German History", in: *The Stasi at Home and Abroad: Domestic Order and Foreign Intelligence*, Bulletin of the German Historical Institute, 52 Supplement 9, Washington DC, USA, 2014, 73-83.

c) The preliminary evaluation of the statistical data, collected in order to measure the perceptions of privacy and data protection related issues among individuals.

The research objectives of the whole research project are:

- To define and compare different laws on personal data protection in the mentioned countries;
- To define the perceptions of the peoples on data protection and privacy issues;
- To measure the general trust towards the different actors when it comes to their role in data protection and abuse: governments, private companies and the criminal world;
- To investigate the topic of personal data protection, control and privacy in the digital era in Russia, Lithuania and Germany from a comparative perspective.

Methods and Methodology:
The biggest challenge of the research was to find the appropriate methodological choices. The initial research design planned to use qualitative research methods, comparative law, analysis of mass media and academic literature. Having said that, the original ideas were needed to be changed during the author's visit at Bremen University, at the Research Centre for East European Studies[6] (the 'stage' time). A decision was taken to collect quantitative empirical data also. Only a part of collected surveys data is presented in this paper. Combining the empirical data analysis, together with other research methods that were applied during the research period as a re:constitution programme Fellow, seems to be a promising research strategy in order to tackle macro-perspective research goals that this paper indicates.

1. Concept of Privacy in History and in the Law

As it has been indicated above, Lithuania and Russia share the same historical legacy, when it comes to the law and ideology in general. These include definitions on and approaches towards the right to privacy and data security protection. First occupied and annexed by the Soviet Union in 1940, reoccupied in 1944, Lithuania lost is sovereignty and as such the autonomy of its legal system. The whole field of criminal prosecution, constitutional and civil law was also transformed in line with the Soviet standards and eventually, they were integrated into the unified legal system of the Soviet Union.[7] As such, when talking about the Soviet period, the Soviet definition and perception on privacy are applicable for both: to Lithuania and to Russia as well.

It is important to stress, that the Soviet legal system and society were more diverse and reflexive than Western interpretations of them, developed during the Cold war era were attempting to

[6] Forschungsstelle Osteuropa.
[7] See more in: Monika Kareniauskaitė, "The Criminal Justice System in Soviet Russia and the USSR (1917–1953): Emergence, Development and Transfer to the Lithuanian SSR", *Lithuanian Historical Studies*, 20/1, 2016, 151-182.

depict it.[8] However, the strong mechanisms of empire-building, of centralization and of lifestyle standardization[9] are also difficult to ignore. Therefore, both Soviet Russia and Soviet Lithuania followed (or, were forced to follow) the same definition and perception of the 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.[10]

As Lokot claims, according to the views of the early Soviet Bolsheviks', "anything private was deprived of social meaning and thus politically dangerous", and social duty –as a social principle, value and ideal– overruled privacy in the Soviet political and legal culture.[11] The German Democratic Republic (East Germany) transferred this ideological understanding into practical implementation on another level. The extreme efficiency of the Stasi surveillance system was infamous for its technological progressiveness of equipment, for the notorious effectiveness of its secret informants (agents) and for its network of the involved individuals.[12] However, after the 1990s, the political trajectories of these countries 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 short window of democracy under president Boris Yeltsin, came back to authoritarianism.

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. Several cases can be mentioned here. But for example, all these three countries had to decide the destiny of inherited huge data archives of the former secret surveillance and state repressions-related authorities, some cases were extremely sensitive in terms of personal data protection. Among the extremely numerous Stasi documentation legacy and personal data records, there was a huge archive of information, connected to personal health information. 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. Researchers would dearly love to mine this lode to extract information on possible links between cancer and exposure to carcinogens, but they

[8] See, for instance: Sheila Fitzpatrick, "Revisionism in Soviet History", *History and Theory*, 46/4, 2007, 77–91.
[9] Mark R. Beissinger, "Soviet Empire as 'Family Resemblance'", *Slavic Review*, 65/2, 2006, 294–303.
[10] Tetyana Lokot, "Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia", *Media and Communication*, 2020, 8/2, 315; Lokot, "Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices", *Surveillance & Society*, 16/3, 2018, 332–346.
[11] Lokot, "Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia", 315.
[12] Helmut Müller-Enbergs, *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 3: Statistiken*, Berlin: Christoph Links Verlag, 2008.

have hit a serious road-block. Under the Federal Data Security Act –now valid throughout Germany– the cancer register is illegal."[13]

The mentioned case very well illustrates, how the integration of the two systems, with the opposite approaches on personal data protection, created new tensions in privacy laws. Again, according to Sietmann, "the law, which reflects public fear of a return to the totalitarian past, allows medical records bearing individual names to be kept only for very specific purposes, narrowly defined in advance".[14] Another situation that can be mentioned here –that all 3 countries faced in the 1990's– whether the personal data of the former KGB or Stasi agents should be made publicly accessible.

While Germany chose a different path, the so-called law of lustration was adopted in Lithuania and 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. The decision created a controversy and resulted in a big polarization of the Lithuanian society that is still present. On the one hand, the newly-democratic now independent state 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. Former Lithuanian political prisoners or forcedly deported persons were claiming –and they are still claiming– for the right to access to certain information on who were responsible, who committed crimes against them. The Soviet systems' victims in Lithuania were comparing their situation with the situation of DDR victims. They were claiming for the similar right to get the information on their perpetrators, which in Lithuanian case was not granted.[15]

Despite these issues, Lithuania and the former DDR transformed their legal systems successfully on, privacy laws and on data protection. Today, both countries are following the European Union's legal approach in this regard. It is important to note here as Gerald Spindler has expressed, 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". According to Spindler, the Federal Republic of Germany prior to the reunification "had been the 'origin' of European data protection, leading

[13] Richard Sietmann, "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, 1991, 915, accessible online: https://www.jstor.org/stable/2875334 [last visited 30-07-2021].
[14] Ibid.
[15] Jarausch, *Between Myth and Reality: The Stasi Legacy in German History*, 76–81; Dėl sąmoningo liustracijos vilkinimo, *XXI amžius*, 84/1581, 14 November 2007, accessible online: http://www.xxiamzius.lt/numeriai/2007/11/14/nuom_02.html [last visited 30-07-2021] ; Julija Ravaitytė, "Evaluation of The Lustration Policy in Lithuania", *Politologija*, 77/1, 2015, 49–100.

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."[16]

It's hard to disagree with such perspective and it is enough to remember to the Judgment of German Federal Constitutional Court (Bundesverfassungsgericht) of 15 December 1983.[17] According to Spindler, "the legal landscape even today is marked by its rulings, which have enlarged the whole (constitutional) base for data protection, for instance, by installing a new fundamental right of the individual to trust the integrity and solidity of IT systems."[18]

Later, by decision of 27th 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.[19] 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.[20]

In case of Germany, (and, later, Lithuanian legal evolution on 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.[21] As the EU directives have binding legal force throughout every member state, after Lithuania joined the EU in 2004, it also meant joining the EU's legal system on personal data protection. The directive protected only the personal data of individuals; corporate entities were excluded from it.[22]

---

[16] Gerald Spindler, "Consumer Data Protection in Germany", in: Rainer Metz, Jörg Binding, Pan Haifeng, Florian Huber (eds.), *Consumer Data Protection in Brazil, China and Germany. A Comparative Study,* Göttingen: Göttingen University Press, 2016, 72.

[17] 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 [last visited 30-07-2021].

[18] Spindler, "Consumer Data Protection in Germany", 72.

[19] German Federal Constitutional Court (Bundesverfassungsgericht), decision of 27/02/2008 – 1 BvR 370/07, 1 BvR 595/07 – BVerfGE 120, 274, accessible online: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html [last visited 30-08-2021].

[20] Corinna Preuß, Jörg-Alexander Paul, "German Constitutional Court creates a new fundamental 'IT Privacy' Right", September 2008, *Bird & Bird*, Accessible online: https://www.twobirds.com/en/news/articles/2008/german-constitutional-court-creates-a-new-fundamental-it-privacy-right [last visited 30-08-2021].

[21] Accessible online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 [last visited 28-08-2021].

[22] Spindler, "Consumer Data Protection in Germany", 75.

As for Germany, the Federal Data Protection Act of 30 June 2017 should be mentioned.[23] According to Spindler: "Both the European 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."[24] It is no surprise that in Germany, concerned with the personal data protection and privacy, this topic is common in the media and ranges within a broad array of topics: for instance, the role of tech companies in potential data protection risks[25], the offers of how to solve this problem, proposing new safer software ideas.[26]

In Lithuania, Law on Legal Protection of Personal Data was adopted on 11th of June, 1996. As the first article of the law claims that the purpose of the Law is to "safeguard of the inviolability of an individual's private life in the course of processing personal data". 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."[27] 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"[28]. 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"[29]. 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

[23] 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), accessible online: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0012 [last visited 30-08-2021].
[24] Spindler, "Consumer Data Protection in Germany", 91.
[25] See, for instance: "Vertrauen und Misstrauen: 20 Jahre Google Deutschland", *Donaukurier*, 4 October 2021, accessible online: https://www.donaukurier.de/nachrichten/digital/netzundtechnik/Internet-Datenschutz-Geschichte-Unternehmen-Deutschland-USA-Vertrauen-und-Misstrauen-20-Jahre-Google-Deutschland;art251974,4817277 [last visited 30-08-2021].
[26] See, for instance: „TeamViewer will ‚erste datenschutzkonforme' Unterrichtssoftware anbieten", 28 September 2021, *Spiegel Netzwelt*, accessible online: https://www.spiegel.de/netzwelt/web/teamviewer-will-erste-datenschutzkonforme-unterrichts-software-anbieten-a-87a2ed5d-c4d0-41f9-8335-02a72be19890 [last visited 03-08-2021].
[27] 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), accessible online: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ef70b5d2f14811e78f3dc265493430ae [last visited 30-08-2021].
[28] "Online Data at Risk to Hackers", *The Baltic Times*, 842, January, 2014, 5.
[29] Ibid.

communications technologies raises new issues which are not addressed by today's legal acts."[30]

However, today both –in Lithuania and Germany, as being members of the EU, a new legal regime –the General Data Protection Regulation, or GDPR– has been implemented, entered into force on May 25, 2018. On its official website, the GDPR is characterized as "the toughest privacy and security law in the world"[31], 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"[32]. 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."[33]

According to the GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[34].

In Russia, the situation is different. First of all, one may look at the law in force. The Russian 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.[35] However, the practical implementation of this law seems to be limited or even problematic. As 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."[36]

Lotok agrees with the other scholars, for example, Greene and MacKinnon, calling today's Russia's political system "networked authoritarianism."[37] The concept is understood as "a regime in which the state prioritises developing networked infrastructure and digital connectivity, while seeking to control all spheres of the datafied social life."[38]

---

[30] Ibid.

[31] "What is GDPR, the EU's new data protection law?", *GDPR.eu*, Accessible online: https://gdpr.eu/what-is-gdpr/ [last visited 30-08-2021].

[32] Ibid.

[33] Ibid.

[34] The General Data Protection Regulation, Article 4-1, accessible online: https://gdpr.eu/article-4-definitions/.

[35] Federal Law of 27 July 2006 N 152-FZ on personal data, accessible online: https://pd.rkn.gov.ru/authority/p146/p164/ [last visited 30-08-2021].

[36] Lokot, "Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia", 315.

[37] Ibid.

[38] Ibid, 315; S. Greene, *How much can Russia really change? The durability of networked authoritarianism*, Washington, DC: PONARS Eurasia, 2012; R. MacKinnon, "Liberation technology: China's 'networked authoritarianism'", *Journal of Democracy*, 22/2, 2011, 32–46.

The very concept of privacy in Russia is rather problematic: The term 'privacy' itself [приватность] in Russian, is according to Lotok, is a term clearly borrowed from other languages. In today's Russia, the "privacy in the modern sense, including the privacy of personally identifying information, individual communications, behaviour, and digital data traces", is, according to the her, "entering the mainstream legal, political, and social discourse"[39]. However Russian law not only defines the citizen's rights towards the personal data protection, but allows the state and law enforcement entities the access to user data and metadata in order to protect the national security.[40]

So to say, in today's Russia there are two approaches – the one of government which places security higher than the privacy, and the one of local activists who are advocating for a stricter personal data privacy protection. It is quite obvious that these conceptions are competing:

> "networked authoritarian Russian state sees its citizens 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. On the other hand, 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."[41]

It has been seen similarly in the Russia media. For instance, a speech of Vladimir Putin from Davos in 2021, reported excessively by the Russian press, radio and television, included the section on tech giants and social media networks. Putin expressed the 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, it "tries 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 was characterised by a paternalistic view, namely, that only the state shall collect and control the citizens' data for good, already noticed and described by Lokot.[42] The news that Russian Government targeted Twitter followed shortly afterwards.[43] The speed of Twitter was slowed down, after it failed to remove what the Russia's media censors described as the inappropriate content.[44]

---

[39] Lokot, "Data Subjects vs. People's Data: Competing Discourses of Privacy and Power in Modern Russia", 316.
[40] Ibid, 315-316.
[41] Ibid, 316.
[42] "Geopolitics, Sanctions And Social Media Giants: Putin's Davos Speech, in Quotes", *The Current Digest of the Russian Press*, 5/73, 2021, accessible online: https://dlib-eastview-com.ezp-prod1.hul.harvard.edu/browse/doc/65934951 [last visited 10-09-2021].
[43] "Russia Cracks Down on Twitter", *The Current Digest of the Russian Press*, 11/73, 3-6, 2021, accessible online: https://dlib-eastview-com.ezp-prod1.hul.harvard.edu/browse/doc/67052305 [last visited 10-09-2021].
[44] 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

Talking about the Lithuanian public discourse on personal data privacy, the situation has changed greatly in the last two decades. In the early 2000's there was more concern on state's illegal action on collecting the citizen's personal data. For instance, during the impeachment[45] of Lithuanian president Rolandas Paksas, the concerns were raised whether Lithuanian security services breached legality by, for instance, "tapping telephone conversations of suspected public officials, including Paksas himself"[46].

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 the Google officially reported and the press wrote, "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."[47] While rather the state has been blamed more for not providing enough security than for being the entity one, violating the citizen's personal data on purpose. 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."[48]

To put more efforts in ensuring the data security and citizen's privacy, financial problems arose: offering competitive salaries to IT specialists by the state. However, as the press underlined, Lithuanian minister of the Interior of that time, Saulius Skvernelis stated that "certainly sees the

in: Anna Chernova, Zahra Ullah, "Russia's Twitter crackdown ends up taking out government websites", *CNN Business*, 2021, accessible online: https://edition.cnn.com/2021/03/10/tech/russia-twitter-crackdown-website-outages/index.html, [last visited 10-12-2021].

[45] 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 [last visited 10-09-2021].

[46] Arturas Racas, "Doubts on privacy rights raised in scandal", *The Baltic Times*, 386, 4 December 2003, 5; Steven Paulikas, "Report: Paksas scandal raises privacy concerns", *The Baltic Times*, 414, 8 July 2004, 5.

[47] "Lietuva in Brief", *The Baltic Times*, 805, 14 June 2012.

[48] Lithuania short of cyber sleuths, *The Baltic Times*, 856, March 2015, 4.

importance of Lithuania upping the ante with its cyber security: he sees the right to privacy and personal data protection as becoming as crucial as saving people's lives".[49]

Today's public discourse in Lithuania is expressing more and more interest in the data privacy and personal data security issues by discussing cases, related to the data protection and privacy ensuring concerns: from the customer's data leak cases by local enterprises[50] to the recommendation of Lithuania's Defense Ministry on avoiding consumers to buy Chinese mobile phones[51].

2. Plot survey data

To investigate the relative conceptions on privacy and data protection in German, Lithuania and Russia, a pilot survey was designed and tested. The survey consisted of 19 questions. A total of 156 surveys were collected from the three countries (DE, Germany n=50; LT, Lithuania n=56; RU, Russia n=50). Two different online services were used to collect the responses from Russia and Germany and the processors were monetarily compensated. Due to the smaller population of Lithuania and the scale of this pilot study, the Lithuanian version of the survey was administered with a convenience sample from social media outreach. The collected results have been used to guide the revisions of the survey for subsequent studies but not to put under a rigorous analysis. Therefore, no specific conclusions can be drawn from this pilot survey. However, an insight has been gained from the process which will be used for follow up survey designs. Subsequent versions of this survey can be conducted in a way to allow to process a larger amount of responses. That is to say, statistically relevant analysis can be conducted to better represent the views of the general populations.

The survey questions were translated into the German, Lithuanian and Russian. Some expressions were difficult to identically translate in the tree languages. Therefore, the next iteration of this survey design will include careful rewording of some of the questions to minimize such differences. Also, some questions will be altered to allow a better statistical analysis. Data processing and analysis was conducted using the programming language Python (version 3.9).

The survey results have been presented in this manuscript serve to illustrate and test the general methods that will be refined for the next iteration of this study. Due to variations in the data

[49] Ibid.
[50] "Hacker who leaked CityBee user data tells media cyber security was poor", *BNS*, *LRT*, 17 February 2021, accessible online: https://www.lrt.lt/en/news-in-english/19/1346403/hacker-who-leaked-citybee-user-data-tells-media-cyber-security-was-poor [last visited 10-09-2021].
[51] Andrius Sytas, "Lithuania says throw away Chinese phones due to censorship concerns", *Reuters*, 22 September 2021, accessible online: https://www.reuters.com/business/media-telecom/lithuania-says-throw-away-chinese-phones-due-censorship-concerns-2021-09-21/ [last visited 10-09-2021].

collection methods (survey sources), the results may not be used for general consideration or interpretations.

Figure 1 shows the results of how many hours per day the survey takers spent online. This question was added to the survey to see how the number of hours spent online might influence the responses to the other survey questions. The preliminary results summarized in Fig. 1 indicate that several hours have been reported in all three countries. For a future survey, it may be helpful specify question into more detailed sub questions, such as on hours using a smart phone or PC to access online services.

Figure 2 presents a summary of the answers from the survey takers on the methods they usually use to protect their privacy and data. The results are in percent relative to the number of responses for the corresponding country. There seems to be similarities in the responses between all three countries. It is important to note again, that these results (and for all the pilot survey questions) only concern the collected sample sets and cannot be generalized to the entire population of the countries. Further versions of this study would require larger samples to prove this.

Figure 3 summarizes the greatest threats concern of the source of potential abuse to the individuals' personal data. Finally, Fig. 4 shows how the interviewees saw the change in data protection since 1990's.

Conclusion

Combining the desk analysis of law and legal documents with quantitative data, historical approaches with contemporary statistical analysis turned out to be a fruitful strategy aiming at to measuring different approaches towards the privacy and security in Russia, Germany and Lithuania. The final conclusions of this research, based on the broader statistical data sample and on a deeper analysis, will be published in the near future. However, as the given figures demonstrate, we can clearly raise the hypothesis that the legal regimes and privacy definitions of the past still impact today's societies.

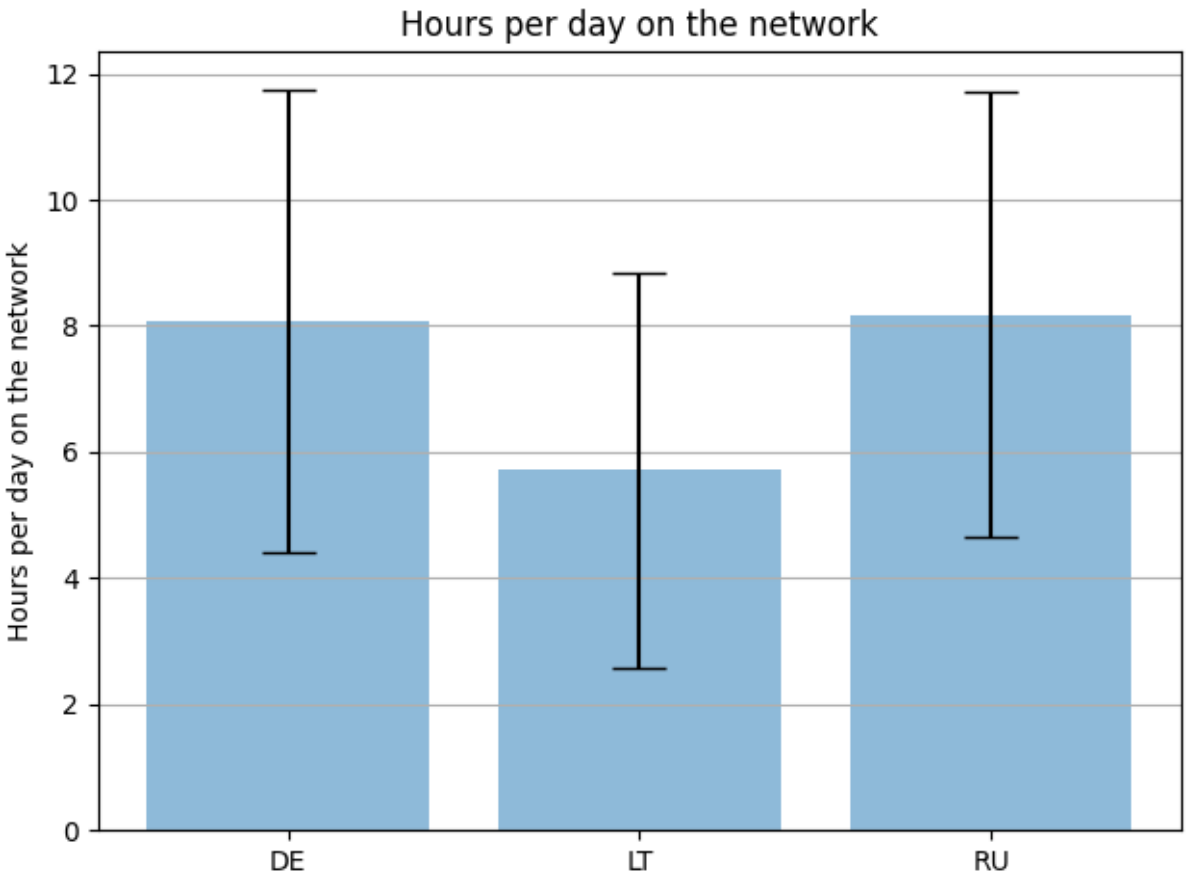

Figure 1. Survey results by country on the number of hours spent online per day. The error bars are the standard deviation of the responses.

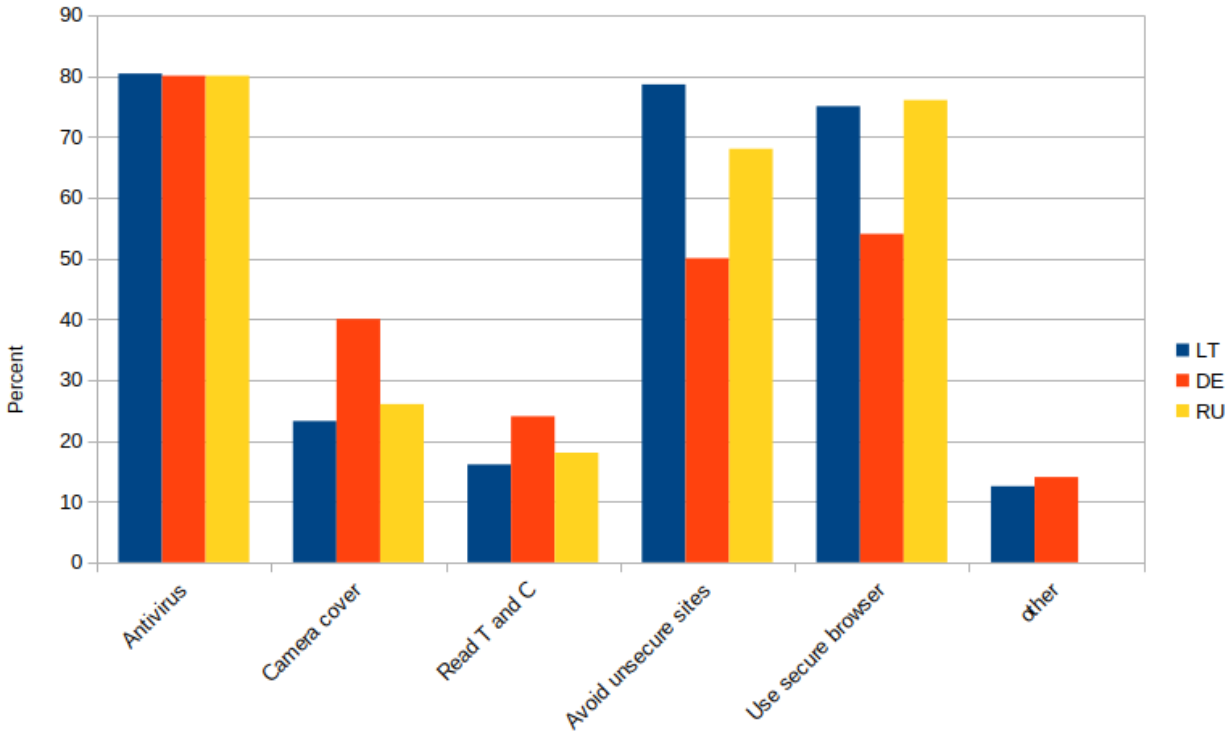

Figure 2. Question: What cyber security or data protection methods are you applying? A) antivirus, B) camera covering, C) reading terms and conditions, D) avoiding insecure websites, E) Using secure web browsers, F) other. Each respondent to this survey question could select all methods that they use.

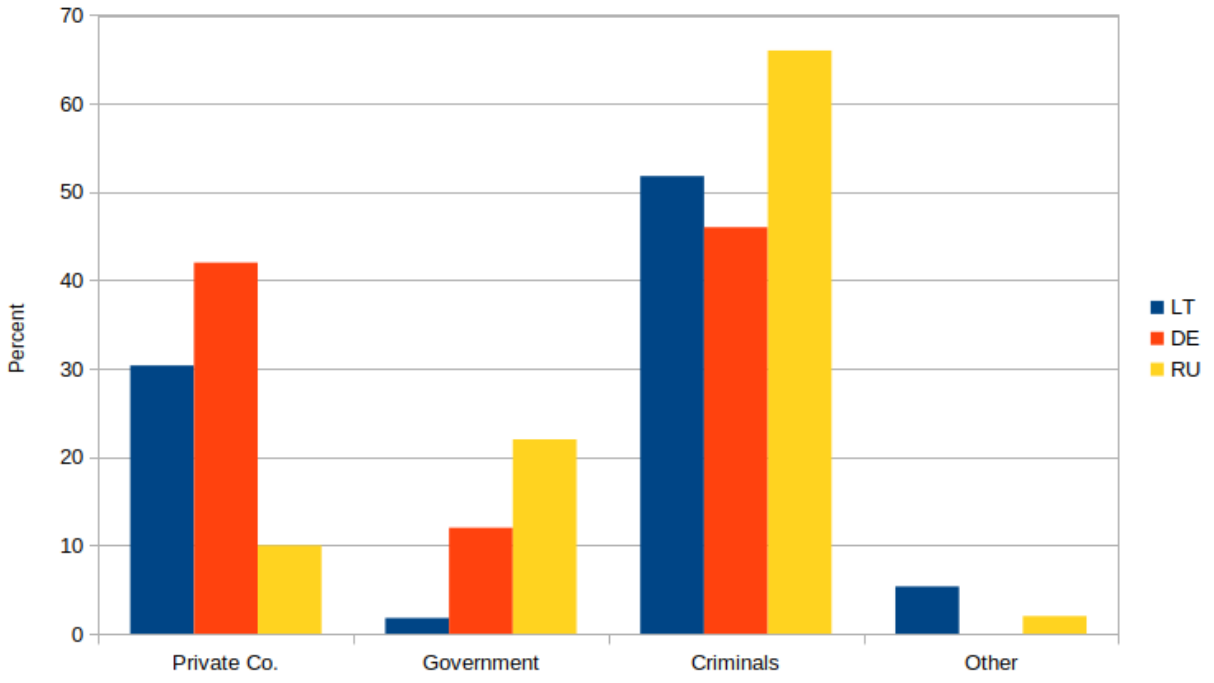

Figure 3. Question: What poses the biggest threat to your personal data? A) private companies, B) government/military/police, C) criminals, D) other. In this question, the respondents had to select only their number one concern and could not choose more than one option. A future version of this question could be expanded to include a ranking of their concerns.

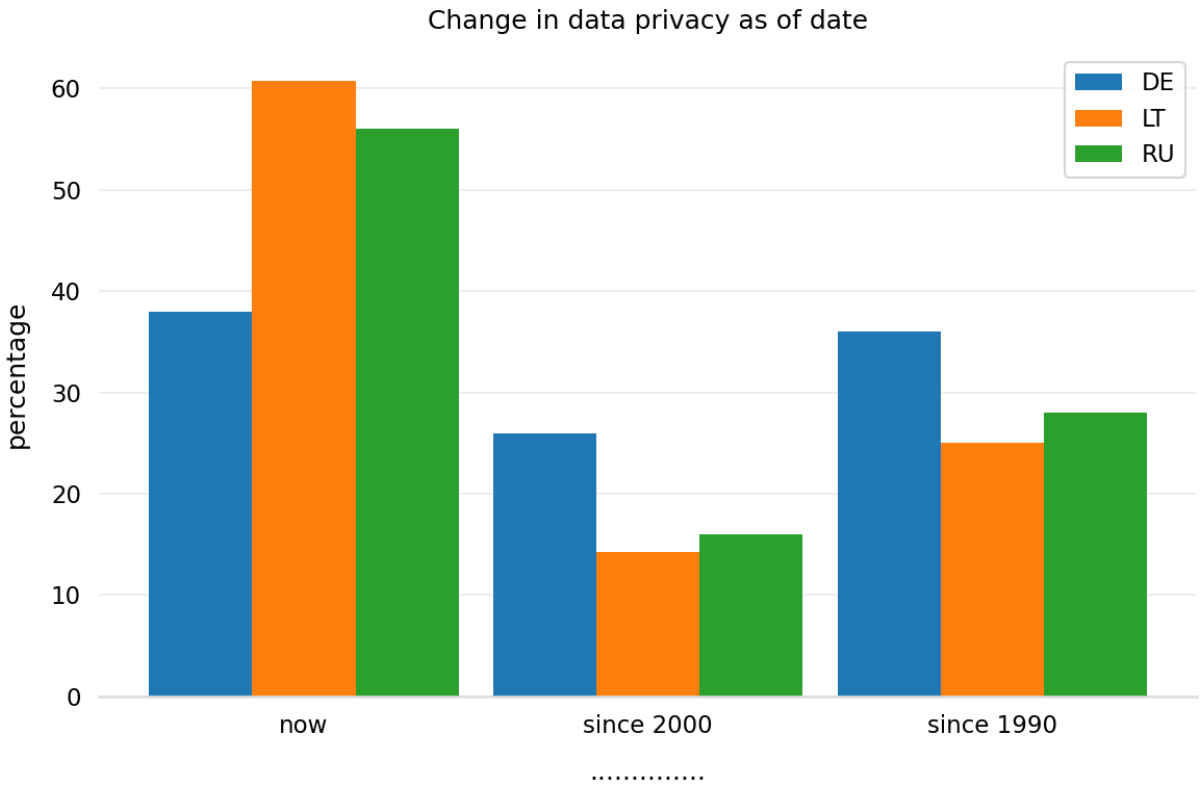

Figure 4. Question: When do you feel that your privacy and personal data were more protected: today or in the past? A) Now, B) Since 2000 C) Since 1990.

Forum Transregionale Studien e.V.
Wallotstraße 14
14193 Berlin
T: +49 (0) 30 89001-430
office@trafo-berlin.de
www.forum-transregionale-studien.de