NATIONAL RESEARCH UNIVERSITY
HIGHER SCHOOL OF ECONOMICS

Vera Rusinova, Alexandra Pereverzeva

PRIVACY AND THE LEGALIZATION OF MASS SURVEILLANCE: IN SEARCH OF A SECOND WIND FOR INTERNATIONAL HUMAN RIGHTS LAW

BASIC RESEARCH PROGRAM

WORKING PAPERS

SERIES: LAW
WP BRP 97/LAW/2020

Vera Rusinova,[1] *Alexandra Pereverzeva*[2]

PRIVACY AND THE LEGALIZATION OF MASS SURVEILLANCE: IN SEARCH OF A SECOND WIND FOR INTERNATIONAL HUMAN RIGHTS LAW[3]

This paper revisits the traditional trade-off between privacy and security, which underpins the compatibility of general and indiscriminate mass surveillance with international human rights instruments, and extends the orthodox patterns of legal argumentation using interdisciplinary knowledge, which is able to nurture, and to be translated into, the language of International Human Rights Law. In search of new resources and a second wind for the overburdened legal concept of privacy, this research combines a positivistic legal perspective with knowledge from sociologically framed surveillance studies, political theory, behavioral economics, and computer science, and deals with the threats and responses thereto from this epistemological standpoint.

The first of three threats singled out in the paper—the 'securitization' of the danger of terrorism—is treated through embedding the effectiveness of predictive algorithms to the proportionality test. A consensus of 'Big Brothers' to use mass surveillance tools as the second threat is considered using constitutional theory and the bridge of the 'democratic society' component included in some international human rights instruments to transpose issues of fair representation to the standard of review. The third threat is the shift of social norms towards the permissibility of being watched. Resources to cope with this challenge can be found in the complementation of an individual reading of privacy as a right and a value by a collective one, which follows a primarily socio-economic trend to consider privacy as a public good.

JEL Classification: Z

Keywords: privacy, mass surveillance, human rights, principle of proportionality, International law.

[1] Vera Rusinova is Doctor of legal sciences, LL.M (Goettingen), Professor, Head of the School of International Law of the Law Faculty, the National Research University Higher School of Economics; leader of the Research and Study Group 'International Law in the Age of Cyber'. (E-mail: vrusinova@hse.ru).

[2] Alexandra Pereverzeva is a Master's student, 'Civil and Criminal Defense Lawyer', the National Research University Higher School of Economics; member of the Research and Study Group 'International Law in the Age of Cyber' (E-mail: sasha-pereverzeva@yandex.ru).

[3] The article was prepared within the framework of the Academic Fund Program at the National Research University Higher School of Economics (HSE University) in 2020 (grant № 20-04-020) and within the framework of the Russian Academic Excellence Project '5-100'.

Introduction

We are witnessing a wave of legalization of the bulk interception of communications and metadata. Many states the world over have introduced legislation in order to regulate, and thereby from the one side to limit and from the other to legalize, the bulk interception of data at the national level. Immediately after the 2015 terrorist acts in Paris, a new law on the surveillance of international electronic communications was introduced in France, which allows the interception of all communications sent or received abroad, and the storage of their content for one year and their metadata for six years.[4] In Germany on December 23, 2016, a law on the interception of foreign communications by the Federal Intelligence Service was adopted,[5] which also governed surveillance over foreign citizens.[6] In 2016, a referendum on amendments significantly broadening the bulk interception of data took place in Switzerland and obtained approval from 65.5% of its voters.[7] In the same year, a Polish law on police and legal acts governing the use of secret surveillance came into force.[8] The UK and Swedish legislation, allowing for the bulk interception communications, forms the core of the *Big Brother Watch*[9] and *Centrum för Rättvisa*[10] cases, pending before the Grand Chamber of the European Court of Human Rights (ECtHR).

One of the most far-reaching laws was adopted in Russia. In 2016, the existing possibilities of bulk interception were amended by the so-called 'Yarovaya law', which entered into force on July 1, 2018[11]. This law requires telecom providers to store the content of voice calls, data, images and text messages for six months, and the metadata on them for three

[4] Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, Art. 1, available at: https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte (accessed on 1 November 2020).

[5] Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016, (2016) Bundesgesetzblatt Teil I. № 67 at 3346.

[6] See also Wetzling, Simon, 'Eine kritische Würdigung der BND-Reform', https://verfassungsblog.de/eine-kritische-wuerdigung-der-bnd-reform/ (accessed on 1 November 2020).

[7] https://www.theguardian.com/world/2016/sep/25/switzerland-votes-in-favour-of-greater-surveillance (accessed on 1 November 2020). See Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (stand am 1. März 2018), available at: https://www.admin.ch/opc/de/classified-compilation/20122728/index.html (accessed on 1 November 2020).

[8] See European Commission for Democracy through Law (Venice Commission), Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts of 10-11 June 2016, available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e (accessed on 1 November 2020).

[9] ECtHR, *Big Brother Watch and Others v. The United Kingdom,* Applications Nos 58170/13, 62322/14 and 24960/15, Merits and Just Satisfaction, 13 September 2018 (hereinafter: *Big Brother Watch case (2018)*).

[10] European Court of Human Rights (ECtHR), *Centrum för Rättvisa v. Sweden,* Application No 35252/08, Merits and Just Satisfaction, June 19, 2018 (hereinafter: *Centrum för Rättvisa case (2018)*).

[11] Federal Law of 6 July 2016 № 374-FZ 'On amendments to the Federal Law 'On Countering Terrorism' and Other Legislative Acts of the Russian Federation in Part of the Introduction of Additional Measures to Counter Terrorism and Maintain Public Security', Rossiyskaya Gaseta, 8 July 2016, № 149; Federal Law of 6 July 2016 № 375-FZ "On Amendments to the Criminal Code of the Russian Federation and the Criminal Procedural Code of the Russian Federation in Part of the Introduction of Additional Measures to Counter terrorism and Maintain Public Security', Rossiyskaya Gaseta, 11 July 2016, № 150.

years. Online services such as messaging services, email and social networks that use encrypted data are required to permit the Federal Security Service to access and read their encrypted communications. Internet and telecom companies are required to disclose these communications and metadata, as well as 'all other information necessary' to authorities on request and without a court order.

Mass surveillance is rapidly becoming the 'new normal'.[12] It might therefore, be of no surprise, that sociologically framed surveillance studies tend to declare the human rights concept of privacy[13] as an improper and useless organizing concept.[14] Against this background, the legal literature on surveillance circumvents the question of the legality of mass surveillance *per se* and concentrates on issues of jurisdiction.[15] Without question, the development of technology and the triggered shifts and changes in social relationships have had a significant impact on the legal concepts of surveillance. But is it really justified to bemoan the death of the legal concept of privacy?

There are only two international courts that have dealt with the issue of mass surveillance so far. The ECtHR and the Court of the European Union (CJEU). Since its decision on *Weber and Saravia v. Germany* of 2006, the ECtHR,[16] and later the CJEU,[17] have started to steadily require a thorough compliance with the right to respect for private life and the protection of personal data from states. However, in 2018 the ECtHR Chambers in *Centrum för Rättvisa* and *Big Brother Watch* have significantly reversed their progressive approach, which had already started to crystallize. In these judgements, the ECtHR explicitly stated that mass surveillance *per*

[12] Lubin A., Legitimizing Foreign Mass Surveillance in the European Court of Human Rights, *JustSecurity*, 2 August 2018, available at: https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/ (accessed on 1 November 2020).

[13] About the human rights concept of privacy *see*: Oliver Diggelmann, Maria Nicole Cleis, How the Right to Privacy Became a Human Right, *Human Rights Law Review*, 2014, vol.14, issue 3, pp. 441–458.

[14] Lyon D., *Surveillance Society: Monitoring Everyday Life*, Open University Press, 2001; Cohen J., Studying Law Studying Surveillance, *Surveillance & Society*, 2015, vol. 13, issue 1, p. 96.

[15] Milanovic M., Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, *Harvard International Law Journal*, 2015, vol. 56, p. 81; Lubin A., 'We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance, 2018, *Chicago Journal of International Law*, vol. 18, issue 2, p. 502.

[16] ECtHR, *Liberty and Others v. the United Kingdom* Application No 58243/00, Merits and Just Satisfaction, July 1, 2008, para 63; ECtHR [Grand Chamber], *Roman Zakharov v. Russia* Application No 47143/06, Merits and Just Satisfaction, December 4, 2015, paras. 260-262, 265; ECtHR, *Szabó and Vissy v. Hungary* Application No 37138/14, Merits and Just Satisfaction, January 12, 2016, paras. 67, 71, 73.

[17] Court of Justice [Grand Chamber], *Requests for a Preliminary Ruling from the High Court of Ireland and the Verfassungsgerichtshof — Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, Joined cases C-293/12 and C-594/12, 8 April 2014; Court of Justice [Grand Chamber], *Requests for a Preliminary Ruling under Article 267 TFEU, made by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) (United Kingdom) - Tele2 Sverige AB v. Post- och telestyrelsen, and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, Joined Cases C-203/15 and C-698/15, December 21, 2016.

se does not violate the Convention on the Protection of Human Rights and Fundamental Freedoms (EConvHR).[18] The court refused to require that surveillance should be a suspicion-based, and emphasized the procedural requirements and safeguards at the stage of the processing of the collected data.[19] The judgments in both cases have been transferred to the Grand Chamber, thus, leaving a chance that this approach still may be revisited.[20] However, while the ECtHR had rendered its final conclusions, on October 6, 2020, the Grand Chamber of the CJEU delivered judgments on the requests for preliminary rulings in two cases—the *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* and *the La Quadrature du Net and Others v. Premier Ministre and Others*—where it found that the general and indiscriminate retention and transmission of traffic data by providers of electronic communications services to a state authority violated EU law.[21] Therefore, it is intriguing whether the Grand Chamber of the ECtHR will correct the previous deviation and thereby confirm the illegality of general mass surveillance for the members of the Council of Europe or whether the 'red light' will apply only within the EU.

Focusing on the issue of the compatibility of mass surveillance *per se* with International Human Rights Law, this paper critically assesses the strength of the 'orthodox' arguments surrounding the trade-off between security and privacy, and seeks to compliment them. For this purpose the research exceeds the realm of the pure legal analysis and searches for further resources, both internal or external to International Human Rights Law, on which the human rights concept of privacy still can rely on encountering the problem of the entrenchment of mass surveillance programs, and which can be 'translated' to the language of human rights law. For this purpose, the paper is shaped by the 'threats and responses thereto' approach. The paper identifies three major threats and discusses the resources that still may be employed by international and national judicial, administrative or quasi-judicial bodies, empowered to apply international human rights instruments. The study of these threats and resources is based on a multidisciplinary approach, combining a positivistic legal perspective with knowledge from

[18] *Big Brother Watch case (2018)*, para. 314.

[19] *Ibid*, paras. 315, 317, 329.

[20] https://hudoc.ECHR.coe.int/eng-press#{"itemid":["003-6321717-8260093"]} (accessed on 1 November 2020).

[21] Court of the European Union (the Grand Chamber), Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, Request for a preliminary ruling from the Investigatory Powers Tribunal – London, Judgment, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14724754(accessed on 1 November 2020) (hereinafter: *Privacy International case*); Court of the European Union (the Grand Chamber), La Quadrature du Net and Others v. Premier ministre and Others, Requests for a preliminary ruling from the Conseil d'État (Council of State, France) and from the Cour constitutionnelle (Constitutional Court, Belgium), Judgment, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf?docid=232084&doclang=en (accessed on 1 November 2020) (hereinafter: *La Quadrature du Net case*).

sociological surveillance studies, political theory, behavioral economics, and computer science, for the application of legal norms is never sterile and is not possible to apply them in a vacuum, regardless of whether 'interpretive communities'[22] are aware of it.

1. The Securitization of the Threats and Effectiveness of Predictive Algorithms

The main aim of mass surveillance programs or legislation is intrinsically connected to security and in particular to the fight against terrorism. As the ECtHR Chamber put it in the *Big Brother Watch* case, 'in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted […] the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation'.[23] By saying this, the court also stressed the lack of alternatives or even combination of alternatives able to substitute for mass surveillance.[24]

Security is one of the commonly recognized 'legitimate aims' that allow the restriction of human rights under international and national law. However, the threat to the application of the human rights concept of privacy lies not only in the broad and undetermined scope of the legal notion of 'security', but in the 'securitization' of some threats related to national security. According to Barry Buzan, Ole Wæver and Jaap de Wilde, representing the Copenhagen School,[25] which pioneered the research of 'securitization', a matter is 'securitized' in the exploitation of the 'security is about survival' approach when it is presented as 'posing an existential threat to a designated referent object', i.e. the entity that is threatened.[26] This approach, by making use of the method of social constructions, allows for the identification, behind the threats and referent objects,[27] of the act of securitization that, in addition to politicization, defines 'securitized' matters as those which 'ask for extraordinary means beyond

[22] Koh H. H., The 1998 Frankel Lecture: Bringing International Law Home, 1998, *Houston Law Rev*iew, vol. 35, p. 649-651.

[23] *Big Brother Watch* case (2018), para 314.

[24] Ibid. para 384.

[25] McSweeney B., Identity and Security: Buzan and the Copenhagen School, *Review of International Studies*, 1996, vol. 22 , issue 1, pp. 81–93.

[26] Waever O., Securitization and Desecuritization, in: *On Security* (ed. by R. Lipschutz), New York: Columbia University Press, 1998, p. 6; Buzan B., Wæver O., and de Wilde J., *Security: A New Framework of Analysis*, 1998, p. 21.

[27] Ibid, p. 207.

normal political procedures of the state'.[28] As a result of securitization, different issues—not only terror threats—but migration, asylum, drug trafficking 'have been handled through the exclusive lens of security, at the expense of other possibilities, such as social inequality or global injustice'.[29] The securitization of terrorism at the macro-level largely started after the September 11 attacks,[30] but this process is ongoing.[31]

Securitization as a political framework is allowing rules to be broken. On the one hand, International Human Rights Law has safeguards against possible abuses (the application of the right to respect for private life is shaped by the use of proportionality) in Article 17 of the ICCPR, which envisages the concept of an 'arbitrary or unlawful' interference with a person's privacy and Article 8 of the EConvHR, which explicitly relies on a trade-off, listing national security as one of the legitimate aims for a restriction of this right. On the other hand, the threat of terrorism is perceived by the 'audience' not as just falling under the notion of 'security', but in a 'securitized' form, as posing an existential threat and, thus, reasonably requiring extraordinary measures.

The use of mass surveillance raises serious concerns in respect of the general suitability of this measure for protecting security, especially when it is related to the threat of terrorism. The existence of a direct relationship between the volume of the information collected in respect of individuals and the level of protection seems to be presumed and beyond legal scrutiny[32]. The typical logical syllogism behind the assessment of proportionality is underpinned by assumptions that the prediction of crimes enhances the level of national security, the growth of information gathered by the security, intelligence and law enforcement bodies enables and strengthens the abilities of competent agencies to make predictions, and concludes that the more data collected, the stronger the protection. The question is, however, whether this logic is valid? Strictly speaking, one can either prove or challenge this conclusion only with an epistemological approach. This requires piercing 'securitization' and separating the 'discursive' part from the scientifically informed juxtaposition of the use of big-data, collected as a result of mass

[28] Does A., Securitization theory, in: *The Construction of the Maras: Between Politicization and Securitization*. Genève: Graduate Institute Publications, 2013, available at: http://books.openedition.org/iheid/719> (accessed on 1 November 2020).

[29] Balzacq T., Léonard S., Ruzicka J., 'Securitization' Revisited: Theory and Cases, *International Relations*, 2016, vol. 30, no. 4, p. 505.

[30] Buzan B., Wæver O., Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory, *Review of International Studies*, vol. 35, pp. 254, 266; Buzan B., Will the 'Global War on Terrorism' Be the New Cold War?, *International Affairs*, 2006, vol. 82, no. 6, pp. 1103-1107.

[31] Bright J., Securitisation, Terror, and Control: Towards a Theory of the Breaking Point, *Review of International Studies*, 2012, vol. 38, p. 870–875.

[32] See, for instance: *Big Brother Watch case (2018)*, paras. 325-327.

surveillance, from the effectiveness of the 'fight on terror', by reference to data science and computer programming.

There are two types of data analysis used in order to track the possibility of committing a crime—'subject-based' and 'pattern-based'. The former is based on building links from known individuals to others and is, thereby, suspicion-rooted; the latter applies statistical probabilities and is, thereby, prediction-rooted.[33] A subject-based analysis 'starts with information about specific suspects, combined with general knowledge'; a pattern-based analysis 'seeks to find new knowledge, not from the investigative and deductive process of following specific leads, but from statistical, inductive process'.[34] Data mining in course of the bulk interception programs, which are not based on suspicion and are not linked to a particular crime, uses a pattern-based analysis.

Subject-based analysis starts from a concrete suspicion, it does not require the bulk interception of data, and it can be implemented using individual surveillance, subject to numerous legal safeguards. It is pattern-based predictive analysis that is behind the need for collecting data about everybody and everything. But has it been proven that predictive analysis is able to produce utility and effectiveness in combatting terror crimes?

The answer to this question is manifold and includes the epistemological characteristics (and mainly, shortcomings) of the process and results gained by the application of predictive analytics. These characteristics give rise to legal concerns related to the use of such results by states. The general shortcomings of predictive analytics are already well reported, not only in data science, but also in recent legal scholarship. They include, *inter alia*: the inaccuracy of the raw data and human error[35] and other problems of 'playing with the data';[36] the reflection of the biases and values of programmers and low-level bureaucrats in the 'running models';[37] the opacity of the results (the 'black-box' phenomenon, connected with the 'explainability' problem)[38]; and the number and costs of errors ('done on populations, applied to individuals'). Translated into the legal language they may be qualified as incompatible with due process, the

[33] Jonas J., Harper J., Effective Counterterrorism and the Limited Role of Predictive Data Mining, *Policy Analysis*, 11 December 2006, no. 584, p. 6 // https://object.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf (accessed on 1 November 2020).

[34] Ibid.

[35] Rich M.L., Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, *University of Pennsylvania Law Review*, 2016, vol. 164, p. 924-925.

[36] Lehr D., Ohm P. Playing with the Data: What Legal Scholars Should Learn About Machine Learning, U.C. Davis Law Review, 2017, vol. 51, p. 655-717.

[37] Citron D. K., Technological Due Process, *Washington University Law Review*, 2008, vol. 85, p. 1260-1263.

[38] Zednik C., Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence, Philosophy and Technology, 2019, pp. 1-5.

prohibition of discrimination, the presumption of innocence, the reasonability of a suspicion, and, the right to respect for privacy.

Nonetheless, terror acts possess some features that differentiate them from other violent crimes[39] and that are crucial for the composition of algorithms and running models, exposing some drawbacks of predictive analytics. First, terror acts are rare; programming and AI needs 'cases' to compose, sustain, adjust and update models. Secondly, they are not routine crimes characterized by more-or-less common patterns of preparation, compared to the credit card fraud, for instance; and they are not 'situational crimes'.[40] Predictive analysis is based on a pattern or patterns that are specific for terrorism planning, patterns that, as some researchers claim, are 'exceedingly unlikely ever to exist'.[41] Thirdly, terrorism shows a high level of 'adaptation' and 'pattern-dependence',[42] demonstrating the learning abilities, prompt reactions to signals, and constant changes of behavior of suspects, who are 'wily' and try to avoid detection.[43]

These drawbacks affect the validity of predictions. The impact of this problem is multiplied by the extremely high costs of errors with respect to the prediction of terror acts. The complexity of processing results consists of the operational capacity to deal with a large number of false positives and negatives.[44] 'False positives' are when the program marks innocent people as suspects and 'false negatives' are when the algorithm misses suspects not marking them as suspicious. An avalanche of false positives overwhelms the system:[45] true results are then 'lost' in the false positives. For instance, a reported case of a known, but not prioritized threat, is when the NSA identified the Tsarnaev brothers as posing a threat before the bombing of the Boston marathon, but failed to act on this result.[46] Drawbacks of the predictive analytics with respect to terror acts can be also demonstrated with example of Hank Asher (the owner of Seisint, an information service), who produced a list of 1,200 people associated with the preparation of the September 11 attack. The false positive rate of this list was about 99%, and the crucial issue about this algorithm was that it had been applied after the attack, its perpetrators and their *modus*

[39] Cohen K., Johansson F., Kaati L., Mork J.C., Detecting Linguistic Markers for Radical Violence in Social Media, Terrorism and Political Violence, 2014, vol. 26, p. 248-250.

[40] Munk T.B., 100.000 False Positives for Every Real Terrorist: Why Anti-Terror Algorithms Don't Work, First Monday, 2017, vol. 22, no. 9, available at: https://firstmonday.org/ojs/index.php/fm/article/view/7126/6522 (accessed on 1 November 2020).

[41] Jonas J., Harper J., Effective Counter-Terrorism and the Limited Role of Predictive Data Mining, *Policy Analysis*, 11 December 2006, p. 9.

[42] Munk, op.cit.

[43] Schneier B., *Data and Goliath.* The Hidden Battles to Collect Your Data and Control Your World, W. W. Norton & Company, 2016, p. 138.

[44] Ibid, p. 137.

[45] Ibid, p. 138.

[46] Ibid, p. 139.

operandi were already known.[47] As Timme Munk empirically proved, the current state of computer science does not allow algorithms to be written which are able to deal with a problem of thousands of false 'positives' and 'negatives'.[48]

The approach of 'rather than look[ing] for a single needle in the haystack', to 'collect[ing] the whole haystack'[49] is not supported by the results envisaged by data science researchers. This metaphor should be treated with the full realization of now many millions of haystacks a search for one needle would require, now many false needles would be found, how long it would take to examine whether they are really false, and that a true needle might be either not found or not prioritized. Results in the realm of the prevention of terror acts come from a targeted, or a suspicion based surveillance, in other words—ordinary methods of operative work.

The threat of securitization and the capacities of predictive analysis were ignored by the ECtHR Chambers in the *Big Brother Watch* and *Centrum för Rättvisa* cases. The CJEU Grand Chamber, on the contrary, adopts a line of argumentation, which aims to fight possible abuses of the national security trump. In the *La Quadrature du Net* case this court, acknowledging that 'the objective of safeguarding national security is […] capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives',[50] required states by the imposition of the retention of data to concretize this threat and demonstrate that it is genuine, present and foreseeable, and to limit the application of these measures by time and to limit their scope to categories of persons or geographical criterion.[51] This judgment should be read in conjunction with second one adopted by the Grand Chamber on the same date—*Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, where the court found that the EU law precludes national legislation to enable 'a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security'.[52] However, despite taking measures to pierce the real and potential securitization of the threats to national security, neither this, not any other international court went as far as to question whether predictive analysis was an adequate tool for the prevention of such non-pattern based threats as terrorism.

---

[47] Jonas, Harper, p. 10.

[48] Munk, op.cit.

[49] Nakashima E., Warrick J., For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All', *The Washington Post*, 14 July 2013, available at: https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html (accessed on 1 November 2020).

[50] *La Quadrature du Net case*, para. 75.

[51] Ibid, para. 1 (operative part).

[52] *Privacy International case*, para. 2 (Operative Part).

2. A Consensus of 'Big Brothers' and Procedural Democracy

The *Centrum för Rättvisa* and *Big Brother Watch* judgments of the ECtHR Chambers are based on giving state-parties to the EConvHR the freedom to decide whether to launch bulk interception programs, and the redirection of the court's scrutiny from the legal regulation of the interception to the processing stages of mass surveillance technology: the filtering, the selection by search criteria, and the examination by analysts.[53] In the *Big Brother Watch* case the Chamber directly linked its reasoning to the doctrine of the 'margin of appreciation'.[54] However, the strikingly general character of the arguments and an appeal to only one mode of state behavior, reveal that the ECtHR was neither emphasizing why national authorities are better placed to decide upon the question of mass surveillance, nor addressing the existence of different national approaches. Thereby, the use of the margin of appreciation doctrine as a 'substantive' concept[55] cannot camouflage the application of the proportionality principle and the trade-off between individual rights and collective goals. Taking into account that, in this form, the doctrine provides no normative added value, its use in this judgment is superficial and misleading.[56]

Besides an explicit reference of the ECtHR to the use of the margin of appreciation doctrine,[57] what stood behind this judgment was not a lack of consensus between parties to the EConvHR, but the wide unanimity in respect of the principled question of the legality of the bulk interception of communications and their metadata. Therefore, deviating in the *Centrum för Rättvisa* and *Big Brother Watch* cases from its own approach, the ECtHR went down the path of the national approaches of European states.

In deciding on the *Big Brother Watch* case, the ECtHR might have not been released from its implied institutional bias, encompassing, *inter alia*, the reverse impact of the skepticism of European states to implement the judgments of international judicial bodies related to the restriction of governmental powers in the use of the bulk interception of data. For instance, a majority of EU member states did not execute or did not fully execute the judgment of the CJEU on the *Digital Rights Ireland* case.[58] There is also a general tendency in European states whose legislation has changed in the aftermath of this judgment, that such legislation was not launched

[53] *Centrum för Rättvisa case (2018)*, paras. 112-114; *Big Brother Watch case*, paras. 315, 329.

[54] Ibid, para. 314.

[55] See Letsas, *A Theory of Interpretation of the European Convention on Human Rights*, 2007, pp. 80-81, 84-90.

[56] Gerards J., Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights, *Human Rights Law Review*, 2018, vol. 18, p. 500-502.

[57] *Big Brother Watch case (2018)*, para. 314.

[58] Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017, p. 12, available at: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf (accessed on 1 November 2020).

by state bodies, but resulted from lawsuits initiated by non-governmental entities.[59] Russia and Hungary still have not adopted general measures to implement the judgment on *Roman Zakharov* and *Zabo and Vissy*.[60] It can be supposed that for the ECtHR, whose albeit not 'authority', but 'power' has been challenged by the 'strategic non-execution' of its judgments by several member states,[61] the ability and readiness to go against an approach that has emerged at the national level might be limited, at least due to the institutional survival instinct.

A way to deal with this threat, although not appealing for universality, can be found in the resort to democracy. The EConvHR has a 'democratic society' component in the test provided for by the text of the Article 8 § 2, envisaging the right to respect for private and family life, and set forth in the preamble, that stresses 'effective political democracy' as a basis for human rights protection;[62] and the Charter of Fundamental Rights of the European Union in its preamble also mentions 'the principles of democracy' as the basis of the union.[63] The ECtHR in its 2018 judgments on mass surveillance revealed the 'necessity in democratic society' as a duty to check whether 'a system of secret surveillance set up to protect national security' does not 'undermine or even destroy democracy under the cloak of defending it', which was then confined to a number of safeguards and guarantees applicable at the processing stage.[64] The CJEU in the *Privacy International case* made an appeal to the 'democratic society' argument by connecting the importance of the rights to privacy and the right to protection of personal data with the importance of the freedom of expression.[65]

However, these ways do not exhaust the possibilities of using the 'democratic society' component contained in some international human rights instruments. One such possibility is the implication of the reference to democracy with the standard of review. This intellectual operation is possible through the mediation of the concept of representation, and, as an outcome, it allows

---

[59] Ibid, p. 13.

[60] UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Hungary of 29 March 2018, CCPR/C/HUN/CO/6, para. 43, available at: https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/HUN/CO/6&Lang=En (accessed on 1 November 2020); Council of Europe, Committee of Ministers, 1302nd meeting, 5-7 December 2017 (DH), H46-26, Roman Zakharov v. Russian Federation (Application No. 47143/06), Supervision of the Execution of the European Court's judgments, available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168076d500 (accessed on 1 November 2020).

[61] *Madsen M.R.*, The Challenging Authority of the European Court of Human Rights: from Cold War Legal Diplomacy to the Brighton Declaration and Backlash, Law And Contemporary Problems, 2016, vol. 79, p. 175. See also *de Londras F., Dzehtsiarou K.*, 'Mission Impossible? Addressing Non-Execution Through Infringement Proceedings in the European Court of Human Rights', International and Comparative Law Quarterly, 2017, vol. 66, p. 467-490.

[62] Convention on Protection of Human Rights and Fundamental Freedoms, signed 4 November 1950, ETS No. 005.

[63] Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

[64] *Centrum för Rättvisa case (2018)*, paras. 104-107; *Big Brother Watch* case, paras. 308, 314-320.

[65] *Privacy International case*, para. 62.

for taking into account the institutional biases and blind spots of national state bodies and agencies involved in the legislation process at the national level. A doctrine that enables this linkage is the procedural democracy doctrine, primarily elaborated by John Hart Ely[66]. Although it discusses the US constitutional system, it has been already tested by scholars in the sphere of international adjudication.[67] This theory is based on the idea of the courts as representation-reinforcing institutions and interrelates issues of democratic representation with the standard of review used by the adjudicators. This process requires judges to define a 'particular group, whose representation they are called on to ensure' and the 'values central to the system of democratic process in which they participate', and then 'to review more intrusively', when 'particular interests seem to be disadvantaged'.[68]

With respect to the examination of the legitimacy of mass surveillance, this theory can be used through the identification of the most vulnerable groups affected by the use of the mass surveillance programs and not represented in the legislative process. This approach can be useful for the states that primarily designed this tool as aiming at foreigners, such as France or Germany. In the seminal 'Democracy and Distrust', Ely used example of alienage (citing Justice Blackmun) as an example of a 'discrete and insular minority … for whom … heightened judicial solicitude is appropriate'.[69] Foreign citizens usually do not have voting rights and legislators 'lack the sort of firsthand expertise with aliens that would enable them to empathize with their problems and needs'.[70] Therefore, it is for the courts—national and international—to pay more attention and to be stricter in the reviewing measures infringing the human rights of these persons.

The application of this argument can be extended from such cases to those where citizens sue their own governments. Even provided that the mass surveillance programs of particular states exclude their own citizens, 'we are all foreigners',[71] because a prohibition on the surveillance of a state's own citizens can be easily circumvented by means of the international co-operation of intelligence agencies.

---

[66] Ely J.H., *Democracy and Distrust: A Theory of Judicial Review*, Cambridge, London: Harvard University Press, 11th Ed., 1995.

[67] Pirker B., Democracy and Distrust in International Law. The Procedural Democracy Doctrine and the Standard of Review Used by International Courts and Tribunals, in: *Deference in International Courts and Tribunals: Standard of Review and Margin of Appreciation* (ed. by L. Gruszczynski, W. Werner), Oxford: Oxford University Press, 2014, p. 62-72.

[68] Ibid, p. 73.

[69] Ely J.H., op. cit., p. 151.

[70] Posner R.B., Democracy and Distrust Revisited, *Virginia Law Review*, 1991, vol. 77, p. 643.

[71] Cole D., We Are All Foreigners: NSA Spying and the Rights of Others, *Just Security Blog*, 29 October 2013, available at: https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/ (accessed on 1 November 2020).

3. 'To Be Watched' Becomes a Social Norm and a Collective Dimension of Privacy

The next threat challenging the international human rights conception of privacy is that 'to be watched' is becoming a social norm.[72] This follows the 'panopticumization' of our society. The dissemination of the Internet ended up with the creation of numerous panopticums which, depending on the participating actors, can be represented as government-citizen, corporation-customer, employer-employee, or citizen-citizen. They not only co-exist and multiply, but blend and splice. Hence, a contemporary society can be characterized as a mixture of panopticums.[73]

A general legal approach to the protection of privacy on the Internet in private relations is dealing with personal data as a commodity and the application of the principle of informed consent. The 'notice and choice' model is based on the pragmatism that, in the reality of the ubiquitous dissemination of the Internet and its indispensability, choice is an illusion.[74] This mass voluntary abandonment of privacy by individuals in their roles as customers and users of Internet social networks has both direct and indirect implications for the government-individual system. As a direct implication, a splicing of governmental, business and social panopticums reveals the direct result of the unknown access of the government (or governments) to personal data and the content of communications. A less visible, but perhaps a more dangerous, impact is indirect. The abandonment of privacy in 'private', which are only 'quasi-non-governmental' relations, has been slowly but surely transferred to relations in the government-individual system, legally framed by human rights at the domestic and international level. This transfer can be traced in at least two directions. First, during a determination of what is protected: a concept of an 'estimated privacy'[75] is based on the collective subjective perception of what is 'normal' and, thus, should be protected, or the doctrine of a special 'privacy on-line'.[76] A lowering of expectations on the Internet leads to changes in the legal domain being introduced by the means of interpretation. Second, a change of social norms influences the balance during the application of the proportionality principle, as it is linked to the weight that is given to different values. Should privacy as a value demonstrate a weakening, this automatically would raise the other side of the scale.

Traditional discourse in international human rights builds up legal arguments around the trade-off between privacy as an individual right and the value of security as a collective value.

---

[72] Timan T., Galic M., Koops B-J., Surveillance theory and its implications for law, 2017, in: *The Oxford Handbook of Law, Regulation, and Technology* (ed. by Brownsword R., Scotford E., Yeung K.), Oxford: Oxford University Press, p. 738-741.

[73] Ibid.

[74] Sloan R., Warner R., Beyond Notice and Choice: Privacy, Norms, and Consent, *Journal of High Technology Law*, 2014, vol. 14, no. 2, p. 370 et seq.

[75] *Katz v. United States*, 389 U.S. 347, 361 (1967).

[76] See Nissenbaum H., A Contextual Approach to Privacy Online, *Daedalus*, 2011, vol. 140, no. 4, p. 38.

One of these patterns is to stress the importance of individual privacy. Many international human rights instruments explicitly recognize the fundamental role of personal autonomy or freedom and dignity in their preambles, and privacy is widely considered a *sine qua non* condition for personal autonomy, freedom and dignity; these issues are inseparable. In contrast to utilitarian human rights theories, which are viewed as the 'biggest enemies to the rights',[77] all anti-utilitarian human rights doctrines (interest-based and reason-blocking)—although to different extents—recognize personal autonomy and dignity to be key values and principles of human rights law. As John Rawls put it in 'A Theory of Justice', 'I assume that the parties view themselves as *free persons* [emphasis added] who have fundamental aims and interests in the name of which they think it legitimate for them to make claims on one another concerning the design of the basic structure of society'.[78] In his theory, individuals are seen as free and equal agents who can rationally choose, revise, or alter their conception of a good life.[79] Hence, 'personal autonomy'[80] is a value and a precondition for the enjoyment of legally protected basic rights. But can a comprehensively profiled individual still maintain his or her personal autonomy? Although it is possible to distinguish privacy and autonomy and to argue that the latter will be undermined when the privacy-violating subject is 'in one way or another influencing the other person', taking into account that this influence can take different forms, including feeling the pressure of being observed that makes her alter behavior, or even without knowing of the observation, being manipulated; bulk interception leaves no chances but to claim the infringement of both.[81] This argument has already used in the legal realm by the Special Rapporteur on the right to privacy Martin Scheinin.[82]

However, as stated above, the approach to give more weight to privacy in the trade-off with security is underpinned by the individualistically shaped perception of privacy as a human right and value. Without any contestation of this dimension, sociological and economic studies dedicated to the contemporary erosion of privacy emphasize the group or community dimension of privacy and prove the social, and, therefore, collective nature of privacy as a value and as a good.[83] Although these researchers are mainly focused on the privacy in multifaceted, but

[77] Letsas G., *A Theory of Interpretation of the European Convention on Human Rights*, Oxford: Oxford University Press, 2007, p. 100.

[78] Rawls J., *A Theory of Justice*, Cambridge: Harvard University Press, 1999, p. 131.

[79] Letsas, p. 106.

[80] Raz J., The Morality of Freedom, Oxford: Oxford University Press, 1988, p. 190.

[81] Becker M., Privacy in the Digital Age: Comparing and Contrasting Individual Versus Social Approaches Towards Privacy, *Ethics and Information Technology*, 2019, vol. 21, p. 308.

[82] United Nations, *Report of the Special Rapporteur on the right to privacy*, 27 February 2019, A/HRC/40/63, para. 9.

[83] Fairfield J.A.T., Engel Ch., Privacy as a Public Good, *Duke Law Journal*, 2015, vol. 65, p. 433-456; *Tisne M*. The Data Delusion: Protecting Individual Data Isn't Enough When The Harm is Collective, 2020, p. 32-48, available at: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/the_data_delusion_formatted-v3.pdf (accessed

private—mainly consumer—dimensions and draw conclusions on the regulatory role of governments, their tenets may also have implications for the trade-off between privacy and security.

Sociologists first opened the doors for the perception of the value of privacy in its collective dimension. The most cited approach singling out the different social dimensions of privacy as a common, a public and a collective value was by Priscilla Regan. According to her privacy is 'a *common* value in that all individuals value some degree of privacy and have some common perceptions about privacy'; 'a *public* value in that it has value not just to the individual as an individual or to all individuals in common but also to the democratic political system', and, 'a *collective* value in that technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy' (emphasis added).[84]

Research using economic theory takes a step further by conceptualizing and empirically testing privacy in terms of it being a public good. A public good is an ideal concept defined by a pair of related characteristics: 'non-rivalrousness in consumption and non-excludability of benefits'.[85] Once such a good is provided, it is available for all, no one can be prevented from the enjoying the good, and 'one actor's use of the good does not impact other potential users' ability to enjoy the good'.[86] Henrik Saetra classifies privacy as an 'aggregate public good': 'no single actor can solve it alone, but it does not require all to take part in its provision', and 'it is provided to the degree that most, or at the very least the most influential, actors actively take part in its provision'.[87] The question of how privacy as a public good can coexist with the famous 'privacy paradox', when individuals disclose personal information, despite their expressed interests in privacy, is explained by behavioral economists through reference to the 'uncertainty of risks and rewards' connected with privacy: 'people discount or devalue the future', therefore, harm to or invasion of privacy is 'not likely to immediately result from an action or inaction, but, instead, will, or will not, occur at a later time', therefore it can 'be put off until a later date'.[88]

In mainstream economic theory, markets do not provide efficient public goods, and this

---

on 1 November 2020); Roessler B., Mokrosinska D., Introduction, in: *Social Dimensions of Privacy: Interdisciplinary Perspectives* (ed. by B. Roessler, D. Mokrosinska), Cambridge: Cambridge University Press 2015, pp. 1-8.

[84] Regan P.M., Privacy as a Common Good in the Digital World, *Information, Communication & Society, 2002*, vol. 5, no. 3, p. 399.

[85] Kaul I. Public Goods: A Positive Analysis, in: *Advancing Public Goods* (ed. by J.-Ph. Touffut), Cheltenham: Edward Elgar Publishing, 2006, p. 13; ver Eecke W., Public goods: An ideal concept, *The Journal of Socio-Economics*, 1999, vol. 28, no. 2, p. 139.

[86] Saetra H. P. Privacy as an Aggregate Public Good, *Technology in Society*, 2020, 63, p. 4.

[87] Ibid, p. 6.

[88] Regan P.M., Response to Privacy as a Public Good, *Duke Law Journal Online*, 2016, vol. 65, p. 52.

failure 'is seen to justify state intervention'.[89] These implications have been reflected in the legal scholarship as proof for the need to conceptualize the 'collective harm'[90] of privacy breaches and revisit the approach to the scope of victims and their *jus standi*, for 'group privacy has little to no legal traction at present' and 'it will be hard for it to gain that traction'.[91] However these tenets were accompanied by an important caveat that 'a group level of privacy as an enhancement and safeguard for the individual right to privacy, rather than as a potential substitute for it'.[92]

Although conclusions revealing the nature of privacy as a public good are inferred from the analysis based on consumer relations, they are also relevant for governmental mass surveillance programs, on at least two grounds. First, different contemporary panopticums are more than interconnected, and the boarders between them are blurred in the 'surveillant assemblage'[93] that also includes state actors. Information collected as a result of privacy resignation in the (nominally) private relations forms the big data accumulated by governmental bulk interception programs. Secondly, objects of governmental and private data collection partly coincide, and the inseparability of privacy as a public good presupposes that it covers all private information, regardless of the type of operators, mediators or organizers of data mining. The impact of the recognition of privacy as a public good for the application of the trade-off under international human rights law lies in the perception of the necessity of governmental intervention in the role of a 'privacy warrior' that should be relevant for all types of private data collection. In addition to this mission, the public-good nature of privacy enhances its collective character, which is mainly overlooked in an individualistically framed application of privacy under different international human rights instruments, but should be of relevance for the assessment of national legislation.

4. Conclusions: Resources for a Second Wind

Although the Grand Chamber of the CJEU has recently, courageously, made its choice in favor of the illegality of general and indiscriminate mass surveillance in EU states, it is still not clear what stance will be taken by the ECtHR and, consequently, whether an enhanced level of

[89] Kaul, p. 13.

[90] van der Sloot B., How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One, *Information and Communication Technology Law*, 2015, vol. 24, no. 1, p. 95-103; see also Cohen J. E., Studying Law Studying Surveillance, *Surveillance and Society*, 2015, vol. 13, no. 1, p. 98.

[91] Taylor L., van der Sloot B., Floridi L., Conclusion: What Do We Know About Group Provacy?, in: *Group Privacy* (ed. by Taylor L., Floridi L., van der Sloot B.), Springer International Publishing, 2017, p. 233.

[92] Ibid, p. 235.

[93] Haggerty K., Ericson R., The Surveillant Assemblage, *The British Journal of Sociology*, 2000, vol. 51, no. 4, p. 608-620.

privacy protection will remain the privilege of EU citizens. Even in respect of these states, the question of the permissibility of the intelligence agencies' sharing of data collected in bulk interception has not yet been legally solved, leaving a significant hole in the protection of their citizens' privacy. It can be presumed that other judicial and quasi-judicial bodies at international and national levels will encounter the problem of the compatibility of mass surveillance and international human rights instruments. The present stage of the adjudicatory response to this, in many senses existential, dilemma shows a very cautious approach. It has made the impression that neither the national[94] nor the international human rights concept of privacy is rolling with the punches, fueled by extremely rapid technological development, and, therefore, needs to get a second wind.

Applying the logic of threats and responses, this paper has singled out three threats that influence the trade-off between privacy and security. The first of them is in the politicization of the threat of the terrorism in the form of securitization—that exploiting the survival argument justifies the transformation of the otherwise exceptional state of emergency into something commonplace. Besides the necessity of unmasking securitization, the proportionality test to examine infringements of privacy can be shifted from the purely discursive to the scientifically informed and to check the correctness of widely-used syllogisms connecting the scope of private data collected by state bodies and agencies with the level of protection against a terror threat.

The second threat, presented as a 'consensus of Big Brothers', epitomizes the unprecedented concurrence of the approaches by states with different political regimes in their use of mass surveillance. Although the example used in this paper says that this threat is complicated to cope with, due to institutional survival instincts, the same logic can be extrapolated to other national and international adjudicating bodies. A suggested solution—although without the ambition of universality—invites the courts to use the 'democratic society' component in the logic paved by constitutional theory and embedded in the examination of fair representation to the standard of review. This primarily procedural examination is inevitably substantial in respect of aliens. More than that, this line of argumentation has a potential especially in the cases of intelligence sharing, as 'we all are foreigners'.[95]

The third threat to the protection of privacy under international human rights law reflects the dilemma, when, on the one hand, to be watched becomes a social norm and individuals quite easily renounce their privacy for comfort, entertainment, communication and so forth, and, on

[94] See Bundesverfassungsgericht, Beschluss des Zweiten Senats (13. Oktober 2016), 2 BvE 2/15, available at: http://www.bverfg.de/e/es20161013_2bve000215.html (accessed on 1 November 2020).

[95] Cole, op. cit.

the other, a necessity to justify, why individual privacy should be protected even when the collection of data enables the enhanced protection of such a collective value as security. A socio-economic perspective adds an individualistic reading of privacy to the collective one by means of the application of the public good category, which can equip the 'interpretive community' with more grounds to require from governments due care and solicitude and thereby resist to the trivialization of the balancing process.

Vera Rusinova

Doctor of legal sciences, LL.M (Goettingen), Professor, Head of the School of International Law of the Law Faculty, the National Research University Higher School of Economics; leader of the Research and Study Group 'International Law in the Age of Cyber'. (E-mail: vrusinova@hse.ru).

Alexandra Pereverzeva

Master's student, 'Civil and Criminal Defense Lawyer', the National Research University Higher School of Economics; member of the Research and Study Group 'International Law in the Age of Cyber' (E-mail: sasha-pereverzeva@yandex.ru).