NATIONAL RESEARCH UNIVERSITY
HIGHER SCHOOL OF ECONOMICS

Vera Rusinova

A EUROPEAN PERSPECTIVE ON PRIVACY AND MASS SURVEILLANCE AT THE CROSSROADS

BASIC RESEARCH PROGRAM

WORKING PAPERS

SERIES: LAW
WP BRP 87/LAW/2019

Vera Rusinova[1]

A EUROPEAN PERSPECTIVE ON PRIVACY AND MASS SURVEILLANCE AT THE CROSSROADS*

This article concentrates on two recent judgments issued by the European Court of Human Rights (ECHR) Chambers, on *Centrum för Rättvisa v. Sweden* and *Big Brother Watch and Others v. United Kingdom,* which expressly acknowledged that mass surveillance *per se* does not violate the Convention on the Protection of Human Rights and Fundamental Freedoms. These judgments have been recently referred to the Grand Chamber, thus giving hope that the approach taken in respect of the launch of mass interception of communications and metadata has a chance to be revisited.

The author reveals whether this approach follows from the jurisprudence of the ECHR, how plausible the argumentation of this court is and how legalization for the bulk interception of data relates to the stance taken by the ECJ, which until that time was dealing with questions of the protection of the right to respect for private life and personal data using the general paths initially paved by the ECHR. The article discloses what precise content in terms of the protection of right to respect for private life lies behind the main findings on the compatibility of bulk interception *per se* with the Convention on the Protection of Human Rights and Fundamental Freedoms, namely, in which part this court has refused to examine the measures undertaken by states in compliance with Article 8 and in which parts it has strengthened (or relaxed) already inferred criteria. Finally, taking into account the current position of the ECHR at this crossroads, the article dwells on causes that influenced the decisions of its Chambers.

JEL Classification: Z

Key words: right to respect for private life, privacy, mass surveillance, metadata, European Court of Human Rights, Court of Justice of the European Union

[1] Vera Rusinova is professor of Public International Law at the Department of general and inter-branch legal disciplines of the Law Faculty, the National Research University Higher School of Economics. (E-mail: vrusinova@hse.ru).

* The article was prepared within the framework of the Academic Fund Program at the National Research University Higher School of Economics (HSE) in 2017- 2018 (grant No.17-01-0042) and by the Russian Academic Excellence Project '5-100'.

1. Introduction

During the last decade two European judicial institutions – the European Court for Human Rights (ECHR) and the Court of Justice of the European Union (ECJ) – have steadily formed a progressive approach to the protection of privacy which promised to strictly limit the ever-growing desire of states to collect as much information about individuals as technically possible. This emerging approach was 'progressive' for two main reasons: it was based on binding judgments in comparison to the far-going and numerous, but non-binding decisions of UN quasi-judicial bodies and the opinions of the UN Special rapporteurs, and as it did not seem to lower the threshold of protection depending on the means of communications, in contrast to the concept of 'reasonable expectations of privacy' applied in US law[2].

Against this background, the judgments rendered by the ECHR Chambers, in 2018 in two cases – *Centrum för Rättvisa v. Sweden*[3] and *Big Brother Watch and Others v. United Kingdom*[4] – had a chilling effect, because they acknowledged that mass surveillance *per se* does not violate the Convention on the Protection of Human Rights and Fundamental Freedoms (EConvHR). As the ECHR put it, 'the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security', falls within the wide margin of appreciation which states enjoy in choosing 'how best to achieve the legitimate aim of protecting national security' and this stance looks like an abstract from the decision of the ECHR on *Weber and Saravia v. Germany*[5], adopted in 2006 at the dawn of the development of technical capacities for the interception, storage and processing of data and before the revelations of Edward Snowden, which demonstrated how intensively states are making use of the mass interception of communications, personal data and metadata[6] tools and how vulnerable the system is. First, because of this conclusion on the permissibility of mass interception of data *per se*, (although this court took the side of applicants by acknowledging that the legislation of the UK on a number of aspects violates the right to respect for private life and the freedom of expression (Articles 8 and 10 of the EConvHR)), this judgment was evaluated by its first commentators as a 'partial'[7] or even 'Pyrrhic victory'[8] of human rights over the 'mass surveillance'.

A question on the legality of mass surveillance under International Law is rather uncomfortable, as it examines the normativity of international legal instruments and jurisprudence of human rights bodies. It can also provide an explanation why the extensive

---

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

[3] European Court of Human Rights (ECHR), *Centrum för Rättvisa v. Sweden*, Application no. 35252/08, Judgment of 19 June 2018, at para 112. See also: Lubin, 'Legitimizing Foreign Mass Surveillance in the European Court of Human Rights', *Just Security* (2 August 2018), https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.

[4] ECHR, *Big Brother Watch and Others v. The United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, Judgment of 13 September 2018, at para 314 (*Big Brother Watch v. UK*).

[5] ECHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Decision on Admissibility of 29 June 2006.

[6] A term «*metadata*» is used in this article as 'all data not part of the content of the communication'. See: European Commission for Democracy through Law (Venice Commission), Report on the Democratic Oversight of Signals Intelligence Agencies (20-21 March 2015), at para 2, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e (Venice Commission, Report of 2015).

[7] Milanovic, 'ECHR Judgment in Big Brother Watch v. UK', *EJIL: Talk!* (17 September 2018), https://www.ejiltalk.org/ECHR-judgment-in-big-brother-watch-v-uk/; Tzanou, 'Big Brother Watch and Others v. the United Kingdom: A Victory of Human Rights over Modern Digital Surveillance?', *Verfassungsblog* (18 September 2018), https://verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/

[8] Christakis, 'A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment', *European Law Blog* (20 September 2018), http://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-ECHR-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/

legal literature on surveillance either bemoans the death of privacy in an irrevocably digitalized world[9], or concentrates on issues of jurisdiction to the detriment of its material scope[10]. This happens against a background of sociologically framed surveillance studies which if not turning a blind eye to the law in general, tend to declare the concept of privacy and, thus, human rights (understood as an international and national legal concept) as an improper and useless organizing concept in the struggle for privacy in our digitalized society[11].

The ECHR judgments in both cases, although examples of regional human rights jurisprudence, because of their binding character and epistemic force, serve an important brick in the universal legal framework of human rights protection as a stance of one of the most progressive international human rights bodies and as a pattern for 47 state parties to the EConvHR. Despite being a minimum standard of human rights protection, the approach taken by this court can be predicted to be used by states as 'permission' for mass surveillance, granted at the international level and will be even accompanied with a critique that a determined threshold is too high and time consuming, to be easily reached.

The judgments on the *Centrum för Rättvisa* and *Big Brother Watch* cases upon request of the applicants have been recently referred to the Grand Chamber, thus giving hope that the stance taken by the Chambers may be revisited[12]. This fact urges the reevaluation of the legitimacy of the approach to one of the principle issues of mass surveillance against its determinacy, coherence and adherence[13]. Such an analysis, presupposing a search for a change of paradigm, seeks to reveal whether this approach follows from the jurisprudence of the ECHR, how plausible its argumentation is and how this approach relates to the stance taken by the ECJ, which until that time was dealing with questions of the protection of the right to respect for private life and personal data using the general paths initially paved by the ECHR. An evaluation of the impact of the acknowledgment by the ECHR of mass surveillance *per se* to be compatible with the Convention can occur only on the basis of an inquiry disclosing what precise content, in terms of the protection of the right to respect for private life, lies behind this finding, namely, in which part this court has refused to examine measures undertaken by the states on compliance with Article 8 and in which part it has strengthened (or relaxed) already inferred criteria. Finally, the current position of the ECHR at this crossroads requires investigating the causes that made two Chambers acknowledge the permissibility of bulk interception of data *per se*. This article, being one of the first commentaries on the recent ECHR jurisprudence on mass surveillance cases, constitutes an attempt to meet all these aims.

2. The emergence of a progressive European approach to the protection of privacy in the age of mass surveillance

A few years ago, thanks to the activity the ECHR and the ECJ, which started to steadily require from states party to the Council of Europe or the European Union, a thorough compliance with the right to respect for private life and the protection of personal data, a sufficiently progressive approach to the maintenance of such values as human rights, the rule

[9] Cohen, 'Studying Law Studying Surveillance', 2015 13 (1) *Surveillance & Society* 91 at 96.

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

[11] Lyon, *Surveillance Society: Monitoring Everyday Life* (2001).

[12] https://hudoc.ECHR.coe.int/eng-press#{"itemid":["003-6321717-8260093"]}

[13] Franck, *Fairness in International Law and Institutions* (1998).

of law and democracy against a backdrop of the growing desire of states to apply technology under the guise of national security, became visible. An overview of this practice shows how much the stance taken by the ECHR Chambers in *Centrum för Rättvisa* and *Big Brother Watch* not only deviates, but reverses the progressive approach which had already started to emerge.

2.1. The steady development of the ECHR case-law before the Centrum för Rättvisa *judgment*

Judgments on *Centrum för Rättvisa* and *Big Brother Watch* were not the first decisions delivered after the *Weber and Saravia v. Germany* case, where the ECHR was seized with the issue of mass surveillance as a measure adopted in the fight against terrorism and state security. In order to track this practice and analyze the extent to which the facts of the two cases considered in 2018 differ from previous decisions, it is necessary to shed light on what is understood by 'mass surveillance'. This is not a legal term, but is used to characterize the scope of data collection. Thus, 'mass surveillance' can be used in criminal law – e.g. while investigating crimes or searching for missing persons – and in intelligence gathering – protecting state security. However, the borderline between these paradigms is conjectural for the fight against terrorism. 'Mass surveillance' is not exhausted by general or bulk measures, when all communications are subject to interception, and can be represented even by targeted measures, provided that the scope of persons, whose data are collected is not sufficiently determined or limited[14].'Mass surveillance' can be targeted at foreigners only, or catch communications with the participation of foreigners, or be indiscriminate. Finally, 'mass surveillance' can be either governmental or corporate.

The decision on admissibility in *Weber and Saravia v. Germany* of 2006 can be taken as a reference point for the formation of the ECHR's approach to mass surveillance. In this case the court examined the domestic legislation on 'strategic monitoring', allowing the intercept of communications in order to 'identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences', and thereby assessed the use of surveillance as a general measure[15]. Although the ECHR did not find any grounds why this 'strategic surveillance' could be regarded as violating Article 8 of the EConvHR and rejected the application as ill-founded, it has accumulated criteria, which should be applied to examine the predictability of the legal basis governing these secret measures[16].

Conclusions made in *Weber and Saravia v. Germany* were confirmed in 2008 in *Liberty and Others v. the United Kingdom*, where the ECHR was confronted with a situation connected with the mass interception of telephone, facsimile and email communications, carried on microwave radio between the two British Telecom's radio stations by the Ministry of Defense in the 1990s[17]. In this judgment, the court expressly stressed, that it 'does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programs of surveillance, on the other'[18].

In *Weber and Saravia* and in *Liberty and Others*, the ECHR did not require the existence of suspicion as a criterion, allowing the widest possible interception of data. This

[14] Venice Commission, Report of 2015 at para 64.
[15] *Weber and Saravia v. Germany* at para 4.
[16] Ibid. at para 95.
[17] ECHR, *Liberty and Others v. the United Kingdom*, Application no. 58243/00, Judgment of 1 July 2008, at para 5.
[18] Ibid. at para 63.

criterion had been used by the court only in respect of secret surveillance in criminal law[19]. The situation changed on the December 4, 2015 when the ECHR rendered its judgment on the *Roman Zakharov v. Russia* case, where it analyzed Russian legislation empowering law-enforcement bodies and intelligence agencies to wiretap phone communications. Being the chair of a regional branch of the Glasnost Defense Foundation, a watchdog NGO monitoring the state of media freedom, the applicant in this case supposed his calls to be intercepted, as the providers of the mobile services had installed equipment allowing different governmental agencies to wiretap all telephone communications[20]. Insofar as Russian law on operational-search activities includes 'obtaining information about events or activities endangering the national, military, economic or ecological security of the Russian Federation'[21] as grounds for the application of wiretapping, the court did not limit the examination to a criminal law paradigm connected with the investigation of specific crimes. Albeit acknowledging that for the protection of national security, 'predictability' does not reach far enough to require the existence of legal norms enlisting in details of which behavior can provoke secret surveillance, the ECHR stressed, that such a formulation – and it should be noted that its content had not been disclosed in any legal acts – gives the government 'an almost unlimited degree of discretion', that opens wide possibilities for abuse[22].

Dealing with the question of the authorization of wiretapping, the ECHR came out for the applicability of 'reasonable suspicion' against a person concerned not only in respect of planning, committing or having committed criminal acts, but also in respect of other acts, which may give rise to surveillance, directly pointing out at 'acts endangering national security'[23]. In the *Roman Zakharov v. Russia* case it was revealed that the sphere of court's scrutiny was restricted: without having access to the evidence, Russian courts were not able to check, whether there was a 'sufficient factual basis' for reasonable suspicion of the individual[24]. As a result, the ECHR criticized the practice where courts granted interception authorizations without mentioning a specific person or telephone number, extending these measures to all telephone communications in the area where a criminal offense has been committed[25].

A slightly different but comparable approach to the legitimacy of the restriction of the right to respect for private life permeates the subsequent judgment on *Szabó and Vissy v. Hungary*[26]. In this case the ECHR, acting on the application of staff members of an opposition NGO, who suspected they were being subjected to surveillance, examined the Hungarian legislation in part, in which it allowed the use of this measure to collect the information for the purposes of the 'prevention of terrorist acts or in the interests of Hungary's national security'[27]. Although domestic legislation scrutinized by the court did not explicitly provide for the applicability of mass surveillance, ECHR in this decision dwelt upon this situation, finding that individuals against whom an interception can be applied were allowed to be defined in terms of a 'range of persons', which can be interpreted as meaning anybody,

[19] See ECHR: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment of 28 June 2007, at paras 79, 80; *Iordachi and Others v. Moldova*, Application no. 25198/02, Judgment of 10 February 2009, at para 51.

[20] ECHR, *Roman Zakharov v. Russia*, Application no. 47143/06, Judgment [GC] of 4 December 2015, at para 10.

[21] Article 7 (2) of the Operational-Search Activities Act of 12 August 1995 № 144-FZ, (1995) 33 Sobranie zakonodatelstva 3349.

[22] *Roman Zakharov v. Russia* at para 246-248.

[23] Ibid. at para 260.

[24] Ibid. at paras 261-262.

[25] Ibid. at para 265.

[26] See Pásztor 'Secret Intelligence Gathering — a Low Threshold Still Too High to Reach' (2017) 1 *ELTE Law Journal* 99 at 104-112.

[27] ECHR, *Szabó and Vissy v. Hungary*, Application no. 37138/14, Judgment of 12 January 2016, at paras 7, 10-11.

subsequently extending surveillance measures to a large number of citizens[28]. The use of this legal technique made it sufficient for the national authorities to appeal to the reasons, justifying the necessity of this measure without the individualization of its targets. This aspect of Hungarian law has been heavily criticized by the ECHR as not corresponding to the principle of 'strict necessity', which requires that the identification of a range of persons subjected to surveillance should be based on an 'individual suspicion', provided that there are sufficient supporting materials[29].

'Secret surveillance can be found as being in compliance with the Convention, […] only if it is strictly necessary […] for the safeguarding of democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation', and required from the domestic authorities to verify whether sufficient reasons for intercepting a specific individual's communications existed in each case[30]. Among the guarantees, which should be respected during interception operations, the ECHR included judicial authorization, adding that only in exceptional circumstances it can be permissible on the authority of executive bodies, subject to a subsequent court review[31]. The subsequent notification of persons targeted by an interception was highlighted by the ECHR as another safeguard against the abuse of power[32]. Such strict ramifications of secret surveillance for the purposes of obtaining the information necessary for the protection of national security brought the possibility of using the bulk interception of data almost to zero.

The emergence of the strict attitude of the ECHR to interference into the private life in mass surveillance can be traced to the critique expressed by Judge de Albuquerque in his Concurring Opinion where he contested the argumentation used in the *Szabó and Vissy* judgment as being not tough enough due to the lowering of the threshold for the applicable standard to the level of an 'individual', instead of a 'reasonable suspicion', as it was done by the Grand Chamber in the *Roman Zakharov* case[33].

Thus, notwithstanding the slight decrease of the requirements of suspicion, at the beginning of 2016 the ECHR remained a proponent of the permissibility of surveillance, which is targeted and subject to a number of safeguards against possible state abuses. A steady development of the jurisprudence of this court inspired confidence that the direction of dealing with cases connected with a bulk interception of data was generally determined for the Council of Europe members[34]. This confidence, as the Chamber judgments on *Centrum for Rattvisa* and *Big Brother Watch* cases have shown, was just an illusion.

2.2. The promise of ECJ jurisprudence

The crystallization of the ECJ position in respect of the bulk interception of data began in 2014, when it heard the *Digital Rights Ireland* case[35]. In this dispute, the court was seized with the issue of the validity of Directive 2006/24 in light of the Charter of Fundamental Rights of the European Union, which required telephone communications service providers to

[28] Ibid. at para 67.
[29] Ibid. at para 71.
[30] Ibid. at para 73.
[31] Ibid. at paras 77, 80, 81.
[32] Ibid. at para 86-87.
[33] *Szabó and Vissy v. Hungary*: Concurring Opinion of Judge Pinto de Albuquerque at para 18-20.
[34] See: Golubok 'Roman Zakharov v. Russia: Big Brother Under Control?' 2015 3-4 (8) *Journal for Constitutionalism and Human Rights* 20 at 25.
[35] 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, Judgment of 8 April 2014. (Digital Rights Ireland).

retain traffic and location data relating to those providers. The court ruled this Directive invalid by having qualified measures imposed thereby to be a disproportional interference into the rights of respect for private life and of the protection of personal data (Art. 7, 8 and 52 (1) of the Charter)[36]. The key premises at the heart of this decision were that, however fundamental the aim of combatting crime may be, it does not by itself justify general measures on the interception of data, and that derogations and limitations in relation to the protection of personal data should be 'strictly necessary'[37]. Moreover, citing the case-law of the ECHR, the ECJ built on the necessity for clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards making it possible for the targeted persons to effectively protect their rights[38].

Based on these principles, the ECJ, first of all, criticized the general scope of the interception of data: the Directive extended it over 'all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime',[39] or preventing threats to public security[40]. As pointed by the court, this legal act neither offered an objective criterion, or substantive or procedural conditions, limiting the access of national authorities to the retained information and subjecting this access to judicial or independent administrative review, nor required to set such limits from the Member States[41]. Finally, the data retention period, being set between 6 and 24 months was not made dependent upon the categories of data and any objective criteria ensuring that they are limited to what is strictly necessary[42].

Hereafter, these conclusions were repeated and developed in the *Tele2 Sverige AB and Watson case (Tele2) case,* the judgment on which was issued by the ECJ on December 21, 2016. The subject of consideration in this case were prejudicial requests of two courts on the interpretation of Art. 15 (1) of Directive 2002/58, and, in particular, on the extent to which findings made in *Digital Rights Ireland* are applicable to the national legislation implementing Directive 2006/24, which was declared void in the latter judgment. The Swedish Administrative Court of Appeal addressed the ECJ in the framework of the proceedings in which 'Tele2 Sverige AB', a communications service provider, contested an order on the bulk interception of traffic and location data of its subscribers and users[43]. The second request was brought by the Court of Appeal of England and Wales, seized with the issue of conformity with EU law of Section 1 of the British legislation concerning data retention.[44] After having repeated all the tenets formulated in the *Digital Rights Ireland* case, the ECJ concretized that they did not ban use of the interception of metadata as a preventive measure, provided that this retention is of a targeted, not mass, character, and subject to a number of safeguards[45]. The interception should, moreover, correspond to the purpose of fighting serious crimes and be subordinated to the principle of strict necessity[46]. In particular, national legislation should be based on 'objective evidence, which makes it possible to identify a public whose data are

[36] Ibid. at paras 69, 71.
[37] Ibid. at paras 51,52.
[38] Ibid. at para 54.
[39] Ibid. at para 57.
[40] Ibid. at para 59.
[41] Ibid. at paras 60-62.
[42] Ibid. at paras 63-64.
[43] 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, Judgment of 21 December 2016 at para 2 (*Tele2*).
[44] Ibid.
[45] Ibid. at para 108.
[46] Ibid.

likely to reveal a link, at least an indirect one, with serious criminal offenses, and to contribute in one way or another to fighting serious crime or preventing a serious risk to public security'[47]. The principle of 'strict necessity', according to the ECJ, ought to be respected at the stage of the regulation of the substantial and procedural conditions under which national authorities can get access to the intercepted data[48]. Among these requirements were highlighted a prior review from the courts or independent administrative bodies; the retention of the intercepted data within the EU; the irreversible destruction of the data at the end of the data retention period and the notification of affected persons as soon as that notification is no longer liable to jeopardize the investigations[49]. Finally, the ECJ proscribed member-states to set up a review of the compliance of the national legal regime to the level of protection guaranteed by EU law[50].

Without doubt, this judgment is a piece of unprecedentedly firm resistance to any attempt to lower the threshold of the protection of right for respect of private life and personal data in the face of new technological opportunities. It is conspicuous, how close it echoes the ECHR judgment on *Roman Zakharov v. Russia*. Alongside this, an answer to the question of whether the judgment on *Tele2* sent the national legislation legitimizing bulk interception on a 'knock-out'[51], remains unclear.

The point is that both prejudicial requests subject to consideration in *Tele2* related to data interception in the framework of 'fighting crime'[52] and did not touch upon such aims as the maintenance of defense or the protection of state security. However, mass surveillance is applied, as a rule, not in a criminal law model. In the text of Directive 2002/58 'activities concerning public security, defense, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law' are expressly excluded from its scope of application[53]. Conversely, Article 15 (1) of this Directive permits member states to adopt legislative measures limiting the scope of both the rights and obligations for the protection of 'national security (i.e. state security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offenses or of the unauthorized use of the electronic communication system'[54]. Not only parties to the proceedings, but also states disagreed between themselves in respect of the applicability of this Directive even in the case of the introduction of measures to fight crime[55].

Addressing this issue, the ECJ found that, should these types of activity fall outside the scope of the application of Directive 2002/58, the provision envisaged in Article 15 (1) would be 'deprived of any purpose'[56]. What must be highlighted is that the court did not confine this conclusion to the measures aimed at fighting crime by pointing out that the Directive authorizes states to introduce limitations, only provided that all requirements set up in this legal act are met[57]. Hence, the ECJ confirmed the applicability of Directive 2002/58 to measures undertaken for the protection of public security, defense and state security.

---

[47] Ibid. at para 111.

[48] Ibid. at paras 114, 116-119.

[49] Ibid. at paras 120-123.

[50] Ibid. at para 123.

[51] Verbruggen, Royer, Severijns, 'Reconsidering the Blanket-Data-Retention-Taboo, for Human Rights' Sake?' *European Law Blog* (1 October 2018), http://europeanlawblog.eu/author/frankverbruggen/.

[52] *Tele2.* at para 62 et seq.

[53] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, Article 1 (3), OJ L 201, 31.7.2002 at 37–47, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058

[54] Ibid.

[55] *Tele2.* at paras 63, 65.

[56] Ibid. at para 73.

[57] Ibid.

Despite the fact that the *Tele2* judgment is dedicated only to those measures that are taken in the course of fighting crime, the text implies the general stance of the ECJ in respect of mass surveillance undertaken for the other purposes. By stressing that data interception should be limited to persons suspected of having planned or committed or otherwise been involved in a serious crime,, the court formulated – as a matter of exception – that 'in particular situations, where for example vital national security, defense or public security interests are threatened by terrorist activities, access to the data of *other persons* might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities'[58]. Of course, it should be borne in mind that this conclusion is *obiter dictum*, but, taking into account, that the judgment on *Tele2* case was issued by the Grand Chamber and remains until now, the first and only statement of the ECJ on bulk interception for the purposes of national and state security and public safety, one cannot exclude that it draws a vector for the consideration of the cases belonging to this field in future. Among the key elements of this position are the extraordinary character of such measures, the necessity of objective evidence and a link to a specific case.

Nonetheless, this judgment left a number of principled questions unanswered. Firstly, it is not clear, how far the notion of 'other persons' used by the ECJ in the above quotation can be stretched: can it mean 'all' or does the linkage to objective evidence the mention of a specific case and the highlighting of the 'effectiveness' of the contribution that surveillance might have in fighting of terror, exclude this scenario? Secondly, the statement of the ECJ relates to access to data, not to interception *per se*, and the part of the judgment dedicated to interception deals exclusively with a criminal law model. Expressing its opinion on the parameters of access to data and allowing an extension of the circle of persons to 'others', the court could not have overlooked that these data are somehow intercepted, but which requirements should guide this interception remains outside the *Tele2* judgment. The ECJ only acknowledged that Directive 2002/58 be applicable to both the interception and access to the data and construed its provisions in light of the *Digital Rights Ireland* judgment. However, the latter decision was also limited to the consideration of measures to fight crime. Therefore, it remains a matter of conjecture, how strict the ECJ will treat the issue of the interception of data for the purposes of the protection of state security and public safety. As there are three prejudicial requests which deal with interpretation of the *Tele2* Judgment and touch upon articulated questions before the ECJ, it will soon become known, in which direction the position of this court is moving.

3. Judgment of the ECHR Chamber on the Big Brother Watch *case: time to dispel the illusions?*

The judgment of the ECHR Chamber on the *Big Brother Watch* case was intended to play a central role in the jurisprudence of the court well before its pronouncement on the September 13, 2018. This process was strategic for a number of human rights NGOs, which thought to persuade the ECHR to strengthen its approach to the evaluation of mass surveillance[59]. In this case, arising from the applications lodged by NGOs, companies and individuals, the ECHR was seized with the question of whether three aspects of the UK legislation on mass surveillance are compatible with the EConvHR: first, the bulk interception of communications under Section 8(4) of the Regulation of Investigatory Powers Act 2000; secondly, intelligence sharing; and, thirdly, the acquisition of communications data by

[58] Ibid. at para 119.
[59] See *Big Brother Watch v. UK*, Appendix at 186.

providers of telecommunication services.[60] The applicants – not without the incentive of the 'Snowden factor' – aimed to make the ECHR take into account the qualitative leap in the technical capacities of states allowing the interception, storage and processing of big data.

Expectations from *the Big Brother Watch* case were met, at least, in the sense that the ECHR Chamber rendered a very detailed judgment, which along with paving a direction for the consideration of similar cases in the future, is designed to provide the governments of the Members of the Council of Europe with a 'road map' for the legal regulation of the mass interception of data. Being incomparable in detail, this decision has overshadowed the judgment of the ECHR on the *Centrum för Rättvisa v. Sweden* case[61], which was adopted three months earlier and was the first to deviate from the emerging progressive approach to the evaluation of mass surveillance.

In the *Big Brother Watch* case, answering the question whether mass surveillance is lawful in the light of the Convention, the ECHR Chamber repeated its gambit tested in the *Centrum för Rättvisa v. Sweden* by refusing to follow the line defined in the cases on *Roman Zakharov* and *Sabo and Vissy* cases, and coming back to the approach articulated in the *Weber and Saravia* case almost a decade earlier. A key approach, used in both the *Big Brother Watch* and the *Centrum för Rättvisa* cases, is that states enjoy a wide margin of appreciation at the introduction of the interception regime for the protection of national security, but the discretion afforded to them in operating such a regime is narrower and should correspond to the criteria to minimize the risk of the misuse of power.[62] Thus, the lengthy text of the judgment presents a rigorous elaboration of the content and applicability of these criteria to different types and stages of activities on bulk interception, including co-operation with the intelligence agencies of foreign states.

Substantially, the approach of the Chamber to the compatibility of mass surveillance with the EConvHR, and, in particular, with Article 8, is based on the combination of an acknowledgement that the bulk interception regime is permissible *per se* (which is embodied in the exemption of a number of key parameters of these measures from the test of 'lawfulness', 'necessity in a democratic society' and 'proportionality') and some specificities of the applicability of this test in respect of other elements of this regime. The Court distinguishes four stages of mass surveillance technology: the interception of data, the filtering, the selection by search criteria, and the examination by the analysts, – and, at least, promises that the discretion given to states at the first stage will be accompanied by control at other stages.[63] Reading this judgment gives, however, a slightly different picture of what was exactly excluded from the examination and how complete the court's scrutiny of the remaining parameters was.

3.1. The parameters of mass surveillance exempted from an 'ordinary' Article 8 test

As a consequence of the acknowledgment of the lawfulness of mass surveillance *per se*, the ECHR has used multiple parameters of mass surveillance from the applicability of the well-established test under Article 8 of the Convention. It is noteworthy, that the Chamber has explicitly marked not all, but only two of these exceptions: it disabled the 'reasonable suspicion' criterion in respect of persons whose data are intercepted and the consequent notification of surveillance[64].

[60] *Big Brother Watch v. UK* at para 269.
[61] *Centrum för Rättvisa v. Sweden* at para 112.
[62] *Big Brother Watch v. UK* at paras 315, 329; *Centrum för Rättvisa v. Sweden* at para 113.
[63] *Big Brother Watch v. UK* at paras 315, 329.
[64] Ibid. at para 317.

A refusal of the applicability of the 'reasonable suspicion' standard should be read as a refusal of the application of any kind of suspicion and, thereby, an obvious deviation from the ECHR's own position, formulated in the cases of *Roman Zakharov* and *Szabo and Vissy*. By exempting the requirement of *ex post facto* notification, the court has even relaxed the approach taken in the first case concerning mass surveillance – *Weber and Saravia*[65]. Before 2018, the ECHR had, on numerous occasions, reiterated that the 'subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and, hence, to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively'; and that a notification should be carried out as soon as it does not jeopardize the purpose of these measures.[66] Although the court did not assume the absolute character of this requirement in *Weber and Saravia*, it was far from renouncing it.

As another exception, the Chamber ceased to consider as imperative the requirement for prior judicial authorization of bulk interception. By doing so, the court noted that this decision does not follow from the non-compatibility of this requirement with a conclusion on lawfulness of mass surveillance *per se*.[67] In respect of the bulk interception of data, the ECHR Chamber found prior judicial authorization to be no more than 'best practice'.[68] This stance is tinged with mischief. The Chamber based its conclusion on the argument that a judicial decision authorizing such an operation does not guarantee the absence of abuse. However, this line of reasoning suffers from inconsistency when the ECHR appeals to the cases where national courts gave prior authorizations, but because of the limited scope of the judicial scrutiny, they could not evaluate the proportionality and necessity of this measure. This reduced the authorization procedure to a mere formality, which was thereby not enough to prevent abuse[69]. On these grounds, the Chamber is right in its conclusion that judicial authorization by itself 'can neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention'[70]. Though this inference must be appraised against the conclusions the ECHR drew from it. Instead of interpreting the requirement for prior judicial authorization as including an examination of its "quality", the court decided to refuse from its application altogether[71]. The Chamber, following an opinion of the Venice Commission, concludes that 'independent oversight may be able to compensate for an absence of judicial authorization'[72].

It seems that this is a conclusion about the compatibility of mass surveillance *per se* with the Convention – no matter that the court was trying to disavow it – which truly backs this argumentation. The requirement for judicial authorization for interception operations, if not carried out as a formality, is conjunct with the necessity for the courts to use a standard of review that would not be possible without an examination of the evidence. The absence or lack of evidence (as it is an absolutely blanket character of suspicion – if not its complete absence – which usually forms the basis for mass surveillance), restricted judicial access to

[65] *Weber and Saravia v. Germany* at para 135.
[66] *Weber and Saravia v. Germany* at para 135; *Szabó and Vissy v. Hungary* at para 86.
[67] *Big Brother Watch v. UK* at para 317.
[68] Ibid. at paras 318-320.
[69] *Roman Zakharov v Russia* at para 319; ECHR: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment of 28 June 2007 at para 85; *Mustafa Sezgin Tanrikulu v. Turkey*, Application no. 27473/06, Judgment of 18 July 2017 at para 64.
[70] *Big Brother Watch v. UK* at para 320.
[71] See *Big Brother Watch v. UK*, Partly Concurring, Partly Dissenting Opinion of Judge Koskelo, Joined by Judge Turkovic at para 25.
[72] Ibid. at para 318.

the evidence because of its 'below the water-line' secrecy status, multiplied by the volume and number of cases are the key characteristics of bulk interception.

In the examination of the 'predictability' of national legislation, the Chamber also made other withdrawals. In relation to the nature of offenses that might serve as the basis for the initiation of bulk interception, the court pointed out that the accent of control should be shifted to the selection for the examination stage[73]. How much the ECHR weakened this requirement becomes apparent when it admits that the general reference in the applicable legal acts about threats to national security is sufficient enough. The mere fact that this term can embrace almost everything was evaluated by the court as its strength, not a weakness[74]. As a matter of argument, the Chamber appealed to the fact that the term 'national security' 'was frequently employed in both national and international legislation and constituted one of the legitimate aims to which Article 8 § 2 referred' and added that its flexibility allows states to address threats which are not predictable[75]. Neither was the court strict in respect of the determination of the scope of offences in warrants or certificates for concrete interception operations. The judgment contains examples of such formulations, including 'material providing intelligence on terrorism […] including, but not limited to, terrorist organizations, terrorists, active sympathizers, attack planning, fund-raising'[76]. The Chamber confined itself to a remark that the use of 'more specific terms' 'would be highly desirable', thus finding this level of generalization acceptable[77]. The striking readiness of the court to settle for this may be dictated by the previous decision on the widest possible discretion of states on the launch of bulk interception.

In respect of the ability to define categories of people against whom the interception measures will be applied, which is another part of the foreseeability test, the Chamber dryly noted, 'it is clear that this category is wide' [78]. A distinction between 'external communications' (where one of the parties is known to be outside the British Isles) and 'internal communications' and the exemption of the latter from bulk interception[79] were not an attempt to restrict and differentiate the scope of the applicability of these measure, and appeared in the argumentation of the ECHR only because such an approach had been used in the legislation of the UK.

The court further implied that intelligence agencies are proceeding according to the principle of self-restriction and, thus, 'while anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence services are neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish'.[80] Describing the limits of this discretion, the Chamber pointed at the proportionality of measures for bulk interception[81]. Taking into account a stance of this court in respect of formulation of the aim, it is clear that determining the categories of persons whose data is liable to be intercepted is not required at all.

The comprehensive character of mass surveillance also predetermined that the ECHR refused to use a rule previously inferred in the case of *Weber and Saravia*[82], according to which the selectors and search criteria applicable to the intercepted data should be listed in the

[73] *Big Brother Watch v. UK* at para 329.
[74] Ibid. at paras 333, 332.
[75] Ibid. at para 333.
[76] Ibid. at paras 342, 156.
[77] Ibid. at para 342.
[78] Ibid. at para 336.
[79] Ibid. at paras 336, 337.
[80] Ibid. at para 337.
[81] Ibid.
[82] *Weber and Saravia v. Germany* at para 32.

warrant ordering the operation. Recalling the *Liberty* case, the court noted that it would 'unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic'[83], and arguing that instead of such disclosure, these selectors and search criteria should be subject to independent oversight[84]. The absence of such oversight served in the *Big Brother Watch* case as grounds for the Chamber to find a violation of Article 8[85].

Hence, using the logical course of acknowledging that mass surveillance *per se* does not violate the Convention, the ECHR Chamber restricted the application of the right to respect for private life to an even larger extent than in 2006 in the *Weber and Saravia* case.

3.2. The examined parameters of mass surveillance: severity or mercy?

Turning to the parameters of mass surveillance examined by the ECHR, in the *Big Brother Watch* case the Chamber did not suggest any new criteria. Firstly, the judgment was based on six requirements, set in the *Weber and Saravia case*, except first two – the nature of offences that might give rise to an interception order and a definition of the categories of people liable to have their communications intercepted[86] – which were abandoned as a consequence of the compatibility of mass surveillance *per se* with the Convention. The remaining four requirements included: a limit on the duration of the interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed[87]. Secondly, the judgment added requirements inferred in the *Roman Zakharov v. Russia* case: the supervision of secret surveillance measures, the use of notification mechanisms and the existence of the remedies provided for by national law[88].

The first novelty of the *Big Brother Watch* judgment, which many commentators hastened to call a victory in the fight for privacy[89], consisted in the enlargement of the ambit of information, the interception of which can constitute interference in the right to respect for private life from the content of communications to their metadata[90]. The Chamber justified its position in respect to metadata arguing that 'the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, internet browser tracking, the mapping of communication patterns, and insight into who a person interacted with'[91]. Whereas protection of the EConvHR was extended to this type of data, there is, at least, one 'wrinkle', which seriously offsets this otherwise progressive step. The point is that after having repeated cherished phrases, for which the NGOs were so intensively fighting, the ECHR did not equal the examination algorithms for the content of communications and their metadata. The Court did not step forward to apply requirements from the *Weber and Saravia* case to metadata, having just pointed out that it is not justified in exempting this type of data from the guarantees provided for by national legislation[92]. Consequently, it seems too early to mark an end of the endeavors to acknowledge the collection of metadata as not less intrusive, than the interception of the content of communications.

---

[83] *Big Brother Watch v. UK* at para 340.
[84] Ibid. at para 340.
[85] Ibid. at paras 347, 387.
[86] Ibid. at paras 424, 423.
[87] Ibid.
[88] *Roman Zakharov v. Russia* at para 238.
[89] See, for instance, Milanovic, 'ECHR Judgment in Big Brother Watch v. UK', Op. cit.
[90] Note, that the ECHR made use of a term «related communications data».
[91] *Big Brother Watch v. UK* at para 356.
[92] *Big Brother Watch v. UK* at paras 352-357.

The appearance of another novelty in the *Big Brother Watch* judgment presented not a change of an already applied approach, but arose from the fact that a question on the use of intercepted data received by intelligence exchange from foreign agencies was begged before this court for the first time[93]. Having excluded the stage of data interception from the scope of the examination because it cannot be attributed to the respondent state[94], the Chamber concentrated on the regime for obtaining such material from foreign governments, its subsequent storage, examination and usage[95]. The validity of this exception provokes doubts. The ECHR Chamber itself distinguished situations depending on how the information is obtained and, having excluded cases when material was provided to the UK intelligence services unsolicited (following the position of the respondent that it was 'implausible and rare') and when the information was gained not upon a request (because the applicants failed to elaborate what that meant), the court dealt only with the case when the information was intercepted or already intercepted information was conveyed to the authorities of the respondent state upon their request[96]. The Chamber, by making reference to the Articles on the Responsibility of States for Internationally Wrongful Acts[97], firmly claimed that this situation did not fall under any rule invoking the responsibility of the state obtaining the intercepted data. Acting under instructions, or under the direction or control of another state could have been a relevant rule, if not a very high threshold in respect of inter-state relations – an 'actual direction of an operative kind'[98]. A solution might have been found in the application of shared responsibility, but it still lacks a normative character[99]. Another problem is jurisdiction under Article 1 of the EConvHR[100]. Hence, both the current stage of the law of responsibility and the scope of application of the Convention impede moving on to the examination of the interception of data in intelligence sharing. According to the judgments of Chambers in both *Centrum för Rättvisa v. Sweden* and *Big Brother Watch v. UK*, interception is left at the wide discretion of states. According to this logic, obtaining information collected by foreign states, falls out from the analysis of the compatibility with the Convention. It leaves a significant gap in the protection of human rights, which may be well exploited or has been already exploited by parties to the Convention.

However, this exception was not the only one in the examination under Article 8 applied by the ECHR in respect of the co-operation of intelligence agencies. It might seem that the Chamber was using criteria (except first two) implied in *Weber and Saravia* and *Roman Zakharov*, but though explicitly pointing out a relaxation of the requirement to set out the circumstances in which intercept material can be requested from foreign intelligence services[101], it, nonetheless, did not apply any criterion related to the duration of the interception, which prescribes a necessity to terminate this process. Moreover, what is striking is that whilst examining the use of intercepted data acquired from abroad, the court, though evaluating the same domestic legal norms on the second turn, decided not to repeat its finding on the lack of oversight of the entire selection process and the absence of safeguards

[93] Ibid. at para 416.
[94] Ibid. at para 420.
[95] Ibid. at para 421.
[96] Ibid. at paras 418, 420.
[97] Draft articles on Responsibility of States for Internationally Wrongful Acts, Article 8, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
[98] Crawford, *The International Law Commission's Articles on State Responsibility. Introduction, Text and Commentaries* (2002) at 154; Draft articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries 2001, (2001) Yearbook of the International Law Commission Vol. II. Part Two at 68-69.
[99] See Nollkaemper, Jacobs, 'Shared Responsibility in International Law: A Conceptual Framework' (2013) 34 *Michigan Journal of International Law* at 363.
[100] Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 *Harvard International Law Journal* at 124-129.
[101] *Big Brother Watch v. UK*. at para 424, 428-430.

applicable to the selection of related communications data for examination[102]. One can only guess, how conciseness such an omission was.

Several aspects of the Chamber judgment on *Big Brother Watch* relaxed the previous position taken by the ECHR. First, it is the decision to lower the previous threshold for oversight. The judgment of the Grand Chamber on the *Roman Zakharov v. Russia* case clarified that if this competence is granted not to a judicial body, it still can be compatible with the EConvHR, 'provided that that authority is sufficiently independent from the executive'[103]. In the *Big Brother Watch* judgment the court went backwards by arguing that it had required it 'generally', and by saying so disavowed the sense of the requirement, claiming that the 'actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse […], such as the authorization of secret surveillance measures haphazardly, irregularly or without due and proper consideration'[104]. Secondly, notwithstanding the acknowledgment of the general character of permissible bulk interception, in previous cases the ECHR insisted on the applicability of a necessity test. In *Big Brother Watch*, by analyzing the UK legislation, the Chamber revealed that one of the cases when the intercepted data can be disclosed and copied was formulated as 'likely to become necessary' for an 'authorized purpose'[105]. This finding did not lead to the acknowledgment of a violation of the Convention, as the Court took into consideration that the scope of persons, authorized to obtain this information is limited to those having the appropriate level of security clearance, who has a 'need to know', and, thus, ended up with a recommendation to define the term 'likely to become necessary' more clearly[106].

4. Looking behind the ECHR Chamber judgments on mass surveillance

The ECHR Chamber was more than laconic in exploring, in the *Big Brother Watch* judgment, the grounds of its strategic choice to acknowledge the legitimacy of mass surveillance *per se*. First of all, not denying the quantum leap in information technology, the court, nevertheless, emphasized, that it had been used by 'terrorists and criminals', whom it helps 'to evade detection on the internet'[107]. The Chamber justified the use of bulk interception by pointing to the 'unpredictability of the routes via which electronic communications are transmitted'[108]. And, finally, arguing on effectiveness of this measure and praising its proactive function, the Chamber stressed the lack of alternatives or even combination of alternatives able to substitute for mass surveillance[109]. These arguments seem to be obviously one-sided: taking into account the advancement of technology, the court noticed only 'terrorists and criminals', preferring to remain silent about the appetites of states for collection and analysis of information about individuals, which are increasing at an exponential pace. Less than ten years ago these expectations were technologically restrained by a lack or the ineffectiveness of big data storage and operating systems. In its last argument the Chamber did not even mention measures of targeted surveillance, nor did it speak about any comparison with bulk interception. A glaringly too frequent use of expressions like 'it is clear that' in the reasoning of the ECHR, which might mean either common sense, or the effectiveness of the measures, technical abilities or both, in the majority of cases are just a

[102] Ibid. at para 387.
[103] *Roman Zakharov v. Russia* at para 258.
[104] *Big Brother Watch v. UK* at para 377.
[105] Ibid. at para 368.
[106] Ibid.
[107] Ibid. at para 314.
[108] Ibid.
[109] Ibid. at para 384.

thinly disguised *renvoi* to the general tenet, that the bulk interception of data *per se* does not violate the Convention.

In its reliance on these grounds the Chamber directly linked its reasoning to the doctrine of the 'margin of appreciation'[110]. However, the strikingly general character of the arguments and an appeal to only one mode of state behavior, reveal that the ECHR 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[111] can hardly camouflage the application of the proportionality principle and 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[112].

What stood behind this judgment was not a lack of consensus between parties to the EConvHR, but the opposite – a wide unanimity in respect of the principled question of the legality of the bulk interception of communications and their metadata. Both public opinion and the attitude of the Council of Europe (and the European Union) to the permissibility of 'mass surveillance' has repeatedly changed[113]. The pendulum swung once again following the revelations Edward Snowden made in 2013, which having opened eyes to the magnitude of mass surveillance programs, catalyzed political and legal attempts to call state authorities on their responsibility and formalized an appeal, to significantly shorten and restrict, if not to prohibit, governmental abilities on bulk interception. However, following the wave of terrorist acts which swept through Europe (Paris, Brussels, Nice, Berlin, Manchester, London, Barcelona), public opinion swung back, and many states have not failed to make use of this by introducing appropriate legislation 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 terrorist acts in Paris, a new Law on the surveillance of international electronic communications[114] was introduced in France which allows the interception of all communications sent or received abroad[115], and to store their content for one year and their metadata for six years[116]. In the Federal Republic of Germany on December 23, 2016 a law on the interception of foreign communications by the Federal Intelligence Service was adopted[117], governing surveillance over foreign citizens[118]. In 2016, a referendum on amendments significantly broadening powers to introduce the bulk interception of data took place in Switzerland and obtained approval from 65.5% of its

[110] Ibid. at para. 314.

[111] See Letsas**,** *A Theory of Interpretation of the European Convention on Human Rights* (2007) at 80-81, 84-90.

[112] Janneke, 'Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights', (2018) 18 *Human Rights Law Review* 495 at 500-502.

[113] European Parliament, Resolution on the First Report on the Implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2004-0104+0+DOC+XML+V0//EN&language=en; European Council, Declaration on Combating Terrorism of 25 March 2004 at para 11, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf; *Maras*, 'The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'?, (2012) 40 International Journal of Law, Crime and Justice at 65-66.

[114] Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte

[115] Ibid. Article 1.

[116] Ibid.

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

[118] See also Wetzling, Simon, 'Eine kritische Würdigung der BND-Reform', https://verfassungsblog.de/eine-kritische-wuerdigung-der-bnd-reform/

participants[119]. The same year a Polish law on police and legal acts governing the use of secret surveillance came into force[120].

Therefore, taking the judgments on the cases of *Centrum för Rättvisa v. Sweden* and *Big Brother Watch and Others v. United Kingdom*, the ECHR deviated from its own approach and moved in the direction of the development of national legislation and the approaches of European states. As a confirmation, the judgment on the *Big Brother Watch* case is abundant in references to the Report of the European Commission for Democracy through Law (Venice Commission) on the Democratic Oversight of Signals Intelligence Agencies adopted in 2015[121]. In particular, the conclusion of the ECHR Chambers on the permissibility of mass surveillance *per se* was based on the stance of this Commission, which acknowledged that the 'main interference' into the right to respect for private life occurs not at the stage of collection, but at the stages of access and the subsequent processing of the intercepted data[122]. It ought to be highlighted that the Commission preceded this conclusion by a reference to a 'European perspective'[123]. Albeit this notion is not disclosed in the report, the Venice Commission appears to have meant a somewhat common approach evolved from the national level, and not the practice of the ECHR or the ECJ. This follows from the fact that in the report there is a tacit shift of the emphasis to the access and processing of the collected data, which was not squared with the differentiation between the purposes of surveillance, whereas at the time of the adoption of this report both European courts demanded states to carry out secret surveillance in the framework of fighting crime, including data collection only on the basis of a reasonable suspicion[124].

Moreover, deciding on the *Big Brother Watch* case, the ECHR might have not been released from its implied institutional bias, encompassing, *inter alia*, the reverse impact of the skepticism of the 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 ECJ on the *Digital Rights Ireland* case[125]. There is also a general tendency in the European states whose legislation has changed in the aftermath of this judgment, that such legislation was not launched by state bodies, but resulted from the lawsuits initiated by non-governmental entities[126]. The Russian Federation and Hungary still have not adopted general measures to implement the judgment on *Roman Zakharov* and *Zabo and Vissy*[127]. It can be supposed that for the ECHR, whose albeit not 'authority', but 'power' has been challenged by

---

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

[120] 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, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e

[121] Venice Commission, Report of 2015.

[122] Ibid. at para 60.

[123] Ibid.

[124] See ECHR: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment of 28 June 2007 at paras 79, 80; *Iordachi and Others v. Moldova*, Application no. 25198/02, Judgment of 10 February 2009 at para 51; *Digital Rights Ireland* at para 57.

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

[126] Ibid. at 13.

[127] UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Hungary of 29 March 2018, CCPR/C/HUN/CO/6 at para 43. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/HUN/CO/6&Lang=En; 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, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168076d500

the so called 'strategic non-execution' of its judgments by several member states[128], 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.

5. Concluding remarks

Many scholars who have analyzed the application of International Human Rights Law in the digital age both before and after the ECHR Chambers issued judgments on *Centrum för Rättvisa v. Sweden* and *Big Brother Watch and Others v. United Kingdom* proceeded from the premise that electronic mass surveillance does not *per se* constitute a violation of the international legal obligations of states related to the sphere of privacy[129]. However, by marginalizing the possibility to declare the use of bulk interception illegal in light of international law, and considering it as utopian (according the well-known dichotomy used by Martti Koskenniemi), we cannot notice a gradual transformation of our states to dystopia.

The ECHR is not the sole international body competent to examine the compliance of states with human rights, but it cannot be excluded that its judgments on the cases mentioned, provided that the Grand Chamber does not reverse the approach on the compatibility of mass surveillance *per se* with the Convention, will to a greater or lesser degree influence the ECJ position so that the latter would finally realize that its previously chosen way was 'too progressive'. The voices of the UN Human Rights Committee and UN Special Rapporteurs, notwithstanding their very critical attitude towards 'mass surveillance', has been neglected because of its lack of binding force. Besides this, a long-awaited General Comment to Article 17 of the International Covenant on Civil and Political Rights has not yet been adopted[130].

Finally, protection provided to citizens of democratic states by their constitutions can be rendered insufficient. It can be demonstrated using the example of the judgment of the German Federal Constitutional Court of 2016, where it found that a refusal to disclose to the special parliamentary commission the selectors and search words applied by bulk interception in co-operation of German and US intelligence agencies (BND and NSA), when, probably, the communications of German citizens were intercepted, does not qualify as a violation of the Constitution *(Grundgesetz)* [131]. The basic tenet of this decision is the interest in maintaining the ability of governments to pursue foreign policy and policy in the field of security which 'overrides' the right of the parliamentary commission to get acquainted with the list of selectors and search words[132]. Even provided that the mass surveillance programs of democratic states exclude their own citizens, constitutional protection can still be illusory, as 'we are all foreigners'[133], because a prohibition on the surveillance of a state's own citizens can be easily circumvented by means of international co-operation of intelligence agencies.

---

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

[129] Lubin, Op. cit. at 545-546, Milanovic, Op. cit. at 82, 132, Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2014) 82 Fordham Law Review 2137 at 2166; Georgieva, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 Utrecht Journal of International and European Law 104 at 128; Verbruggen, Royer, Severijns, Op. cit.

[130] Joyce, 'Privacy in the Digital Era: Human Rights Online?' (2015) 16 *Melbourne Journal of International Law* 1 at 7.

[131] Bundesverfassungsgericht, Beschluss des Zweiten Senats vom 13. Oktober 2016, 2 BvE 2/15, http://www.bverfg.de/e/es20161013_2bve000215.html

[132] Ibid. at para 5 (Leitsätze).

[133] Cole, 'We Are All Foreigners: NSA Spying and the Rights of Others', *Just Security Blog* (29 October 2013), https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/

Reading the ECHR Chamber judgments on both *Centrum för Rättvisa v. Sweden* and *Big Brother Watch and Others v. United Kingdom* exposes how with 'eyes wide shut' society is moving towards a 'global panopticon', word for word substantiating a scenario described by Foucault. In particular, in 'Discipline and Punish: The Birth of a Prison', published in 1975, he was very precise in characterizing the role played by states in surveillance over their citizens: 'We must cease once and for all to describe the effects of power in negative terms: it 'excludes', it 'represses', it 'censors', it 'abstracts', it 'masks', it 'conceals'. In fact power produces; it produces reality; it produces domains of objects and rituals of truth. The individual and the knowledge that may be gained of him belong to this production'[134]. The opinion of the ECHR Grand Chamber on both cases, should judges prefer efficiency to integrity and lower the threshold of the requirements on protection of privacy, might well become fatal.

[134] Foucault, *Discipline and Punish: the Birth of a Prison* (1991) at 194.

References

Cohen J. (2015) Studying Law Studying Surveillance, *Surveillance & Society*, vol. 13(1). pp. 91-101.

Crawford J. (2002) The International Law Commission's Articles on State Responsibility. Introduction, Text and Commentaries. Cambridge: Cambridge University Press.

de Londras F., Dzehtsiarou K. (2017) Mission Impossible? Addressing Non-Execution Through Infringement Proceedings in the European Court of Human Rights. *International and Comparative Law Quarterly,* vol. 66, no. 2. pp. 467-490.

Foucault M. (1991) Discipline and Punish: the Birth of a Prison. London: Penguin.

Franck Th. (1998) Fairness in International Law and Institutions. Oxford: Oxford University Press.

Georgieva I. (2015) The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR. Utrecht Journal of International and European Law, vol. 31 (80), pp.104–130.

Golubok S. (2015) Roman Zakharov v. Russia: Big Brother Under Control? Journal for Constitutionalism and Human Rights, no. 3-4(8). pp. 20-26.

Janneke G. (2018) Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights', Human Rights Law Review, vol. 18, pp. 495–515.

Joyce D. (2015) Privacy in the Digital Era: Human Rights Online? Melbourne Journal of International Law, vol. 16, pp. 1-16.

Koskenniemi M. (2011) The Politics of International Law, Oxford: Oxford University Press.

Letsas G. (2007) A Theory of Interpretation of the European Convention on Human Rights, Oxford: Oxford University Press.

Lubin A. (2018) "We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance. Chicago Journal of International Law, vol. 18, no. 2. pp. 502-552.

Lyon D. (2001) Surveillance Society: Monitoring Everyday Life, Cambridge, MA: MIT Press.

Madsen M. R. (2016) 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, vol. 79, no. 1, pp. 171-178.

Maras M.-H. (2012) The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'? International Journal of Law, Crime and Justice, vol. 40, pp. 65-81.

Margulies P. (2014) The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism. Fordham Law Review, vol. 82, no. 5, pp. 2137-2167.

Milanovic M. (2015) Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. Harvard International Law Journal, vol. 56, no. 1, pp. 81-146.

Nollkaemper A., Jacobs D. (2013) Shared Responsibility in International Law: A Conceptual Framework. Michigan Journal of International Law, vol. 34, no. 2, pp. 359-438.

Pásztor E. (2017) Secret Intelligence Gathering — a Low Threshold Still Too High to Reach. ELTE Law Journal, no. 1, pp. 99-112.

Vera Rusinova

Professor of Public International Law at the Department of general and inter-branch legal disciplines of the Law Faculty, the National Research University Higher School of Economics. (E-mail: vrusinova@hse.ru).