P-ISSN 2233-3746 / E-ISSN 2720-782X
https://doi.org/10.60131/jlaw.2.2023.7711

Ketevan Kukava*

Balancing the Right to Privacy and National Security Interests in the Digital Age

In order to protect national security, the states widely use secret surveillance measures and monitor electronic communications, which poses high risks of arbitrariness and abuse of power. Modern technologies enable the states to collect and process personal data on an unprecedented scale. Therefore, the most important challenge in today's world is to determine how to protect national security and prevent serious crimes without violating human rights.

The judgments of the European Court of Human Rights provide guidance in terms of balancing the right to privacy and security interests. The present article aims to discuss the development of the case law of the European Court and the legal safeguards for protecting the right to privacy when the state carries out secret surveillance measures.

Keywords: *secret surveillance, personal data, national security, international communications, bulk interception.*

1. Introduction

In parallel with rapid technological development, society has witnessed the normalization of secret surveillance. With the passage of time, methods of surveillance change, develop and become more sophisticated. It can be asserted that forgoing privacy and individual liberty is the price society pays in exchange for security and public order.

Respect for private life is a precondition for a free and democratic society. At the same time, this right is not absolute and it can be restricted to pursue certain legitimate aims when it "is necessary in a democratic society." Protection of national security is among such legitimate aims.

Digital technologies significantly increased the scale of secret surveillance. The interests of security require certain restriction of rights and the implementation of covert measures. At the same time, the absence of efficient oversight over such methods poses a threat to democratic values. Such a threat exists especially in such circumstances when covert measures are directed towards every person, regardless of the existence of a reasonable suspicion.

The use of measures that have a proactive nature gives rise to controversy. The state interferes in individuals' freedom, privacy, and communications not because of what they have actually done, but because of the danger that might emerge later on.[1]

* Ph.D. student of Ivane Javakhishvili Tbilisi State University Faculty of Law. https://orcid.org/0000-0003-3956-5730.

1 *Fenwick H.,* Proactive Counter-Terrorist Strategies in Conflict with Human Rights, International Review of Law, Computers & Technology, Vol. 22, No. 3, 2008, 259-260.

Protection of national security and the prevention of crimes are among the most important obligations of a state. However, when fulfilling this obligation, the risk of arbitrariness and abuse of power is considerably high. These risks are exacerbated by the covert nature of the implemented measures, which decreases the degree of accountability of security services. Therefore, the most important challenge in today's world is to determine how to protect national security and prevent serious crimes without violating human rights.

The judgments of the European Court of Human Rights (hereinafter – "Court" or "European Court") provide guidance in terms of balancing the right to privacy and security interests. Considering the threats emerging from terrorism and transnational crimes, the present article aims to discuss the development of the case law of the European Court and the legal safeguards for protecting the rights to privacy when the state carries out secret surveillance measures.

2. Monitoring of Electronic Communications and the Right to Privacy – Which Direction Does the Case Law of the European Court of Human Rights Develop?

According to Article 8 of the European Convention on Human Rights (hereinafter –"Convention"),

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[2]

Technology significantly changes the way people communicate and live, which also changes surveillance practices and our perception and expectation of privacy.[3] Technological progress greatly affected the development of the European Court's case law as well.

The Court had to consider the compliance of secret surveillance regimes with the Convention on several occasions. Notably, the mere storage of data relating to the individual's private life constitutes interference within the meaning of Article 8.[4] "The fact that the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons, can have no bearing on that finding."[5]

---

2 European Convention on Human Rights, Article 8, Council of Europe, 1950.

3 *Stepanovic I.,* Preventing Terrorism or Eliminating Privacy? Rethinking Mass Surveillance after Snowden Revelations, Strani Pravni Zivot (Foreign Legal Life), 2015(4), 236.

4 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 244.
Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 330.
Amann v. Switzerland, [2000], ECtHR, N 27798/95, § 69.
S. and Marper v. the United Kingdom, [2008], ECtHR, N 30562/04, 30566/04, § 67.

5 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 244.

Important information about individuals may be revealed not only by the content of the communication but also by metadata. Those data, taken as a whole, may allow the creation of a portrait of a person and the drawing of precise conclusions concerning the individual's private life.[6]

Any use of computer systems by individuals leaves a digital footprint. Considering the increasing capabilities of modern technologies (for example, linkage and extracting completely new information), it can be declared that "insignificant" or "irrelevant" data no longer exist.[7] In the era of big data, "all personal data processing potentially affects privacy in the broad sense."[8]

An effective fight against terrorism and organized crime is essential for protecting national security. To achieve this aim, the states widely use secret surveillance measures and monitor electronic communications, which pose a high risk of arbitrariness and abuse of power.

In the Internet age, the distinction is made between mass surveillance and targeted surveillance as well as internal and foreign surveillance.[9] Notably, the European Court sets different standards with respect to monitoring of communications of the individuals on the state's territory, on the one hand, and the individuals beyond its jurisdiction, on the other.

In 2006, the European Court confirmed the compliance of strategic monitoring of international communications with the Convention in the case of *Weber and Saravia v. Germany.*[10] The Court declared the application inadmissible because the interference in the applicants' rights was "necessary in a democratic society" and considerable safeguards against abuse were provided.[11] The legislation laid down strict conditions with regard to the transmission of data obtained by means of strategic monitoring[12] and provided for the destruction of personal data as soon as they were no longer needed to achieve the lawful purpose.[13] Besides, it was mandatory to inform relevant individuals as soon as notification could be carried out without jeopardizing the purpose of monitoring.[14]

In 2008, the European Court unanimously found the violation of Article 8 in the case of *Liberty and Others v. the United Kingdom*[15] due to a wide discretion conferred by the national legislation on the executive branch to intercept and examine external communications. According to the Court's assessment, the domestic law did not indicate with sufficient clarity the scope or manner of exercise of the State's wide discretion and did not ensure adequate protection against abuse of power. In

---

Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 330.

6 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, [2014], CJEU, C-293/12, C-594/12, § 27.

7 *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds), Springer International Publishing AG, 2017, 45.

8 *Hijmans H.,* The European Union as Guardian of Internet Privacy, The Story of Art 16 TFEU, Law, Governance and Technology Series, Vol. 31, Springer International Publishing Switzerland, 2016, 70.

9 Ibid, 104.

10 Weber and Saravia v. Germany, [2006], ECtHR, N 54934/00.

11 Ibid, §§ 117-118.

12 Ibid, § 122.

13 Ibid, § 132.

14 Ibid, § 136.

15 Liberty and Others v. the United Kingdom, [2008], ECtHR, N 58243/00.

particular, the legislation did not set out in an accessible manner the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.[16]

The case law of the European Court also includes judgments that focus on the surveillance of the communications of individuals within the territorial jurisdiction of the state. In 2015, in the case of *Roman Zakharov v. Russia*[17] the Grand Chamber unanimously found the violation of Article 8 because the Russian legislation did not lay down effective safeguards against arbitrariness and the risk of abuse. Such risks are inherent to secret surveillance and they are "particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile-telephone communications.[18]

According to the Court's assessment, the circumstances in which the public authorities could resort to secret surveillance measures were not determined with sufficient clarity; provisions on discontinuation of surveillance did not provide sufficient guarantees against arbitrariness; the legislation permitted the automatic storage of clearly irrelevant data and did not clearly determine the circumstances in which the intercepted material was stored and destroyed after the end of a trial; the authorization procedures did not ensure the use of surveillance measures only when "necessary in a democratic society;" the supervision of interceptions did not comply with the requirements of the independence and was not sufficient to exercise an effective and continuous control; the effectiveness of the remedies was undermined by the absence of notification and adequate access to documents relating to interceptions.[19]

Notably, in this case, the Grand Chamber reiterated the importance of the verification of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that endanger national security.[20]

The European Court of Human Rights discussed the issue of striking a balance between national security and the right to privacy in the case of *Szabó and Vissy v. Hungary*. In its judgment of 2016, the Court pointed out that according to the legislation of Hungary, the scope of the surveillance measures could include virtually anyone; they were carried out by the executive branch and without an assessment of strict necessity; new technologies allowed the state to intercept masses of data and there was no any effective remedy, let alone the judicial one.[21] Consequently, in this case, the European Court found a violation of Article 8.

Despite the judgment delivered in favor of the right to privacy, the argumentation of the Court gave rise to criticism: According to the concurring opinion of Judge Pinto de Albuquerque, in its reasoning, the Court chose the lower standard – "individual suspicion" instead of a "reasonable suspicion," which significantly diminishes the degree of protection set out in the case of *Zakharov.* According to his assessment, "any kind of "suspicion" will suffice to launch the heavy artillery of

16 Ibid, § 69.
17 Roman Zakharov v. Russia, [2015], ECtHR, N 47143/06.
18 Ibid, § 302.
19 Ibid.
20 Ibid, § 260.
21 Szabó and Vissy v. Hungary, [2016], ECtHR, N 37138/14, § 89.

State mass surveillance on citizens, with the evident risk of the judge becoming a mere rubber-stamper of the governmental social-control strategy."[22] "Individual suspicion" equates to overall suspicion and the judgment creates the impression that the Chamber condones widespread "strategic surveillance" for the purposes of national security.[23]

2.1. Normalization of mass surveillance of international communications for the purpose of safeguarding national security

The European Court's lenient approach towards large-scale surveillance was further strengthened by the Grand Chamber's two similar judgments delivered on May 25, 2021.[24] When assessing the secret surveillance regimes of the United Kingdom[25] and Sweden,[26] the Grand Chamber noted that considering current threats and sophisticated technology, bulk interception regimes are not *per se* non-compliant with Article 8 and the decision to operate such a regime in order to identify threats to national security falls within the state's margin of appreciation. Both applications concerned bulk interception of cross-border communications by the intelligence services.

The Court referred to previous cases (*Weber and Saravia v. Germany; Liberty and Others v. the United Kingdom*) and highlighted 6 minimum requirements developed in its case law that should be set out in law: the nature of offences that may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of 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; the circumstances in which intercepted data may or must be erased or destroyed.[27]

The Grand Chamber emphasized that those cases were more than 10 years old, and in the intervening years, technological developments have significantly changed the way in which people communicate.[28] Considering the development of modern communication technologies, the Court deemed it necessary to adapt the general approach towards targeted surveillance to the specificities of the bulk interception regime.

According to the Grand Chamber, the first two of the above-mentioned six "minimum safeguards" relating to the targeted interception (namely, the nature of offences that may give rise to an interception order and the categories of people liable to have their communications intercepted) are

---

22 Szabó and Vissy v. Hungary, [2016], ECtHR, N 37138/14, Concurring Opinion of Judge Pinto De Albuquerque, § 35.

23 Ibid.

24 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15.
Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08.

25 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15.

26 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08.

27 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 335.
Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 249.

28 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 341.

not readily applicable to a bulk interception regime. Similarly, the requirement of "reasonable suspicion", which can be found in the Court's case law on a targeted interception in the context of criminal investigations is less relevant for the bulk interception regime, the purpose of which is in principle preventive, rather than for the investigation of a specific criminal offence.[29]

In order to ensure the compliance of the bulk interception regime with the Convention, the Grand Chamber determined new safeguards to be defined by the domestic legal framework:

1. the grounds on which bulk interception may be authorized;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorization;
4. the procedures to be followed for selecting, examining, and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[30]

According to the Court's assessment, the Swedish bulk interception system was based on detailed legal rules, was delimited in scope, and provided for safeguards.[31] The main features of the interception regime met the Convention requirements and in most aspects were "necessary in a democratic society."[32] At the same time, the Grand Chamber identified the following three shortcomings: the absence of a clear rule regarding the destruction of the intercepted material that did not contain personal data;[33] the absence of a legal requirement that consideration be given to the privacy interests of the individual concerned when making a decision to transmit intelligence material to foreign partners;[34] the absence of an effective *ex post facto* review.[35]

The Grand Chamber highlighted the importance of additional safeguards when transmitting material obtained by bulk interception to foreign states.[36] According to the Court, the absence of a requirement in the Swedish legislation to assess the necessity and proportionality of intelligence sharing was a significant shortcoming.[37] Furthermore, there was no obligation to analyze and

---

29 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 348.
Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 262.

30 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 275.
Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 361.

31 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 367.

32 Ibid, § 373.

33 Ibid, § 342.

34 Ibid, §§ 326-330.

35 Ibid, §§ 359-364.

36 Ibid, § 276.

37 Ibid, § 326.

determine whether the foreign recipient of intelligence offered an acceptable minimum level of safeguards.[38]

The Grand Chamber took into account the unpredictability of situations that may warrant cooperation with foreign intelligence partners. Therefore, the law cannot provide an exhaustive and detailed list of such situations when the transmission of data is permissible.[39] At the same time, the legal regulation and practice must limit the risk of abuse and disproportionate interference with Article 8 rights.[40]

Ultimately, the Grand Chamber considered that the Swedish bulk interception regime was not in compliance with Article 8 of the Convention as it did not provide sufficient safeguards against arbitrariness and abuse of power.

As for the bulk interception in the United Kingdom, the Court identified the following fundamental deficiencies in this regime: the absence of independent authorization, the failure to include the categories of selectors[41] in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorization.[42]

Furthermore, the Grand Chamber assessed the compliance of the interception regime with Article 10 of the Convention – freedom of expression. According to the Court, before the intelligence services used selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, authorization by a judge or other independent and impartial decision-making body was necessary.[43] The legislation of the UK did not lay down this requirement.[44]

As for requesting and receiving intelligence from non-contracting states, according to the Court's assessment, it had a clear legal basis and pursued legitimate aims. The legislation clearly regulated the circumstances and conditions on which the authorities could request material from a foreign state. The procedures for storing, accessing, examining, using, and communicating the material to other parties, and the erasure and destruction of the material obtained were sufficiently clear and provided adequate safeguards against abuse.[45]

Ultimately, the Grand Chamber found a violation of Articles 8 and 10 of the Convention with respect to the bulk interception regime and acquisition of communications data from Communications Service Providers. As for requesting and receiving intelligence from foreign intelligence services, the Court considered that this regime was compliant with the Convention.

Despite the fact that the violation of the right to privacy was found in both cases, the European Court identified such shortcomings that "require comparably easy fixes."[46] Due to the lenient approach towards strategic surveillance, these judgments of the Grand Chamber gave rise to criticism.

---

38 Ibid.
39 Ibid, § 323.
40 Ibid.
41 Selector means specific identifier, for example, name, email address, etc.
42 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15.
43 Ibid, § 448.
44 Ibid, § 456.
45 Ibid, §§ 501-508.
46 *Milanovic M.,* The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa, EJIL:Talk! 2021, <https://www.ejiltalk.org/the-grand-

According to the partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque, the judgment delivered in the case of *Big Brother Watch and Others* fundamentally alters the existing balance between the right to respect for private life and security interests, as it admits non-targeted surveillance of electronic communications. He concludes that with this judgment the Strasbourg Court opened the gates for an electronic "Big Brother" in Europe.[47]

Furthermore, Judge Albuquerque disagreed with the majority's opinion on the point that the exchange of intercept material with foreign intelligence services did not violate Articles 8 and 10. The Court's judgment indicates that the transfer of bulk material to foreign intelligence services should be subject to "independent control", but the receipt of such material should not be. According to Albuquerque's assessment, if the safeguards are not sufficient with regard to direct surveillance carried out by the United Kingdom, they should be considered inadequate for indirect surveillance as well, resulting from the receipt of third-party intercept material, even more so where this party is not a signatory to the Convention.[48]

A different legal regime with regard to the receipt of material from foreign intelligence services poses the risk that, in order to circumvent the strict supervision in Europe, European intelligence agencies may ask foreign counterparts to collect the information they are not allowed to gather themselves and request to transfer this material to them.[49]

In this case, finding the violation of the right to privacy was also considered a "pyrrhic victory",[50] as there is "no longer a question about the *legality* of mass surveillance policies, but rather a question relating to *how* to operate it."[51] Moreover, this judgment is considered not a "landmark victory" but rather a definitive normalization of mass surveillance by the Grand Chamber,[52] which raises questions about a certain "fragmentation" of European data protection law. [53]

---

normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> [31.07.2023].

47 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, §§ 59-60.

48 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, § 51.

49 *Sloot B.v.d.,* Big Brother Watch and Others v. the United Kingdom & Centrum for Rattvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases? European Data Protection Law Review (EDPL), Vol. 7, No. 2, 2021, 325.

50 *Christakis T.,* A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment, European Law Blog, 2018, <https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/> [31.07.2023].

51 Ibid.

52 *Milanovic M.,* The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa, EJIL:Talk! 2021, <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> [31.07.2023].

53 *Christakis T.,* A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment, European Law Blog, 2018, <https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/> [31.07.2023].

3. Different legal standard with regard to international communications – "electronic big brother" or reinforced national security regime?

The recent case law of the European Court of Human Rights demonstrates that in the interests of national security, the existence of different legal standards with respect to cross-border communications is justified. In this case, the state has broad power in terms of bulk interception of communications, but a further examination of collected data should be subject to strict requirements.

Mass surveillance implies large-scale data collection with the hope of obtaining useful information. Considering the potential of big data, the targeted collection that aimed to avoid searching for "the needle in the haystack" was changed by a new paradigm, according to which "finding a needle in a haystack is not only possible but also practical: in order to find the needle you have to have a haystack."[54] Such an approach raises legitimate questions in terms of human rights protection as it gives the impression that the mass surveillance practice treats ordinary people as potential suspects.[55]

Notably, this approach has supporters as well. Lubin discusses in detail the arguments, which justify different standards with respect to international communications:

1) The state has myriad options for conducting investigations within its jurisdiction. Therefore, the need to carry out covert, let alone bulk interception of communications, is innately reduced. The state can use less intrusive methods to achieve the same legitimate aim. On the other hand, the abilities of a state beyond its jurisdiction are significantly limited.[56]
2) The state has more technological capacities to carry out surveillance of electronic communications in its jurisdiction than abroad. In other words, the states often have statutory access to the communications grid for conducting warranted interceptions. It can also compel telecommunication companies to provide it with additional access to their networks or disclose certain user information from their database. The state does not possess such abilities with respect to international communications.[57]

Ultimately, Lubin recognizes the legitimacy behind certain limited legal differentiations with regard to domestic and foreign surveillance and declares that in fighting for a universal and unified standard of privacy the human rights defenders are losing the far bigger war.[58]

A similar approach is reflected in the 2018 judgment of the Chamber: The Government has considerable powers and resources to investigate persons within the British Islands, however, they do not have the same powers with regard to persons outside the territorial jurisdiction of the United Kingdom.[59]

---

54 *Hijmans H.,* The European Union as Guardian of Internet Privacy, The Story of Art 16 TFEU, Law, Governance and Technology Series, Vol. 31, Springer International Publishing Switzerland, 2016, 100.

55 *Stepanovic I.,* Preventing Terrorism or Eliminating Privacy? Rethinking Mass Surveillance after Snowden Revelations, Strani Pravni Zivot (Foreign Legal Life), 2015(4), 239.

56 *Lubin A.,* We Only Spy on Foreigners: The Myth of Universal Right to Privacy and the Practice of Foreign Mass Surveillance, Chicago Journal of International Law, Vol. 18, No. 2, 2018, 530-531.

57 Ibid, 532-533.

58 Ibid, 551.

59 Big Brother Watch and Others v. the United Kingdom, [2018], ECtHR, N 58170/13, 62322/14, 24960/15, § 518.

According to the judgment of the Grand Chamber in this case, while the interception and even examination of communications of persons within the surveilling state might not be excluded, the stated purpose of bulk interception is to monitor the communications of persons outside the state's territorial jurisdiction, which can not be monitored by other forms of surveillance.[60]

Siofra O'Leary's opinion with regard to striking a fair balance between competing interests is also noteworthy: "The quite legitimate ascendancy of data protection as a fundamental right, and its increased and indeed fundamental importance in this digital age, should not obscure the fact that balancing means just that – the careful weighing and consideration of two competing rights and interests. Just as the interests of public safety and law enforcement will sometimes have to give way to the right to privacy, so the right to privacy may on occasion need to yield to competing considerations."[61]

On the other hand, when operating the bulk interception system, there will always be a temptation to exceed powers, because "if the boundaries of state discretion are wide, even the most stringent policing of them does little to safeguard against abuse."[62] Therefore, there is a high risk that "a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it."[63] When people can not know whether their communications are being targeted, but are aware that there is a strong probability that the monitoring is being carried out, they may adapt their behavior.[64] This may have a "chilling effect" on the realization of fundamental rights, which poses a serious threat to the rule of law and democratic values.

4. Authorization of Secret Surveillance Measures by Independent Body

When secret surveillance measures are carried out, independent supervision constitutes one of the most important safeguards against arbitrariness and abuse. Supervision is necessary at all stages: when the surveillance is ordered, while it is being carried out, and after it has been terminated.[65] When assessing the authorization procedures, the Court takes into account the following factors: the authority competent to authorize the surveillance, its scope of review and the content of the interception authorization.[66]

It has been suggested that in the sphere of mass surveillance, the key shortcoming is the Court's reticence to make judicial authorization mandatory.[67] According to the European Court, "in a field

---

60 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 344.

61 *O'Leary S.,* Balancing Rights in a Digital Age, Irish Jurist, Vol. 59, 2018, 92.

62 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, Partly Concurring and Partly Dissenting Opinion of Judge Pinto de Albuquerque, § 33.

63 Szabó and Vissy v. Hungary, [2016], ECtHR, N 37138/14, § 57.

64 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, Joint Partly Concurring Opinion of Judges Lemmens, Vehabović and Bošnjak, § 11.

65 Roman Zakharov v. Russia, [2015], ECtHR, N 47143/06, § 233.

66 Ibid, § 257.

67 *Watt E.,* The Right to Privacy and the Future of Mass Surveillance, International Journal of Human Rights, Vol. 21, No. 7, 2017, 789.

where abuse is potentially so easy in individual cases and could have such harmful consequences for a democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."[68] Judicial authorization is an important safeguard but it is not mandatory.[69] The case law of the European Court demonstrates that authorization of surveillance by the other independent body meets the requirements of the Convention.[70] What matters most is that this body should be independent of the executive.[71]

For example, the Court considered that the combination of oversight mechanisms in Germany was in compliance with the Convention, although the judicial authorization of the surveillance was not ensured. In this case, the supervision was carried out by G 10 Commission, chaired by the person qualified to hold judicial office.[72]

In the case of *Zakharov,* the Grand Chamber pointed out that according to Russian legislation, authorization was granted by the judge, however, the scope of the review was limited. The courts were not required by the domestic legislation and in practice, they did not verify whether there was a "reasonable suspicion" against the person concerned and did not apply the "necessity" and "proportionality" test.[73]

Swedish legislation required the authorization of surveillance by the Foreign Intelligence Court, which according to the European Court's assessment, met the requirement of independence. The president and vice-president of the Foreign Intelligence Court were permanent judges. All members were appointed by the Government, and they had four-year terms of office.[74] Except in urgent cases, a privacy protection representative also participated in the court sessions, who was a judge, a former judge, or an attorney. This person acted independently and in the public interest and had access to all the case documents.[75]

Notably, in his concurring opinion, Judge Pinto de Albuquerque highlighted the fact that the Swedish Foreign Intelligence Court was not an ordinary court. The Government appointed its members for a four-year mandate and their appointment was renewable, which strengthened their political ties to the Government.[76] The privacy protection representative, who acted in the public interest and not in the interest of any affected individual, was also appointed by the Government with a

---

68 Klass and Others v. Germany, [1978], ECtHR, N 5029/71, § 56.
Szabó and Vissy v. Hungary, [2016], ECtHR, N 37138/14, § 79.

69 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 351. Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 265.

70 Klass and Others v. Germany, [1978], ECtHR, N 5029/71, § 51.
Weber and Saravia v. Germany, [2006], ECtHR, N 54934/00, § 115.

71 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 265.
Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 351.

72 Klass and Others v. Germany, [1978], ECtHR, N 5029/71, § 56.

73 Roman Zakharov v. Russia, [2015], ECtHR, N 47143/06, §§ 262-263.

74 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, § 296.

75 Ibid, § 297.

76 Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08, Concurring Opinion of Judge Pinto de Albuquerque, § 9.

renewable mandate.[77] Therefore, the Foreign Intelligence Court was more akin to a political body than to a truly independent judicial authority.[78]

When assessing the legislation of the United Kingdom, the Grand Chamber considered that the major shortcoming was the authorization of the bulk interception by the Secretary of State and not by a body independent of the executive.[79]

In summary, the case law of the European Court demonstrates that the states are afforded certain discretion in terms of selecting oversight mechanisms. In order to prevent human rights violations, the degree of independence of the supervisory authority and the exercise of genuine control is decisive, which implies the assessment of the necessity and proportionality of secret surveillance measures.

5. Conclusion

The development of digital technologies created an unprecedented opportunity for secret surveillance. Considering the threats derived from terrorism and transnational crimes, the states use sophisticated technologies to protect national security." The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen."[80]

Modern technologies enable States to collect and process personal data on an unprecedented scale. The relevant bodies monitor the communications that may include information about the imminent threat.

The recent judgments of the European Court demonstrate that the aim of fighting terrorism and protecting national security justifies the large-scale processing of data and mass monitoring of international communications. The Court's case law reveals different legal standard with respect to the interception of communications of individuals outside the state's jurisdiction. "The court is tolerant of an argument that different forms of surveillance activities might justify different frameworks of privacy regulations."[81]

The States are afforded certain discretion in terms of selecting the means to protect national security. The European Court explicitly recognized the importance of mass surveillance for protecting national security and considered the bulk interception of international communications to be a legitimate state practice.

Unlike the targeted interception, bulk interception is used for foreign intelligence gathering and the identification of new threats. The recent case law of the European Court demonstrates that the requirement of a "reasonable suspicion" is not relevant in the context of bulk interception of cross-border communications, which serves preventive purposes rather than the investigation of a specific criminal offence.

---

77 Ibid.

78 Ibid.

79 Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15, § 377.

80 Szabó and Vissy v. Hungary, [2016], ECtHR, N 37138/14, § 68.

81 *Lubin A.,* We Only Spy on Foreigners: The Myth of Universal Right to Privacy and the Practice of Foreign Mass Surveillance, Chicago Journal of International Law, Vol. 18, No. 2, 2018, 536.

In order to ensure the compliance of the bulk interception regime with the Convention, in 2021 the Grand Chamber laid down the new safeguards to be provided by the domestic legislation, however, some of them require clear interpretation in the national law.

The rule of law requires that the executive authorities' interference with an individual's rights should be subject to effective control.[82] Although judicial control offers the best guarantees of independence and impartiality,[83] the case law of the European Court demonstrates that the oversight by the other independent body also meets the requirements of the Convention. This body must be independent of the executive and ensure genuine control.

The standard set by the European Court with respect to the intelligence sharing regime is problematic as it poses the risk of "indirect surveillance" – circumventing the legislative requirements and effective supervision by receiving intelligence obtained by a third party.

In conclusion, striking a fair balance between the right to privacy and national security interests remains one of the most topical and problematic issues in European human rights law. The state's wide discretion and the covert nature of the implemented measures pose a high risk of human rights violations. Strong safeguards against abuse of power are decisive for ensuring a fair balance and effective protection of democratic values.

Bibliography:

1. European Convention on Human Rights, Council of Europe, 1950.
2. *Christakis T.,* A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment, European Law Blog, 2018, <https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/> [31.07.2023].
3. *Fenwick H.,* Proactive Counter-Terrorist Strategies in Conflict with Human Rights, International Review of Law, Computers & Technology, Vol. 22, No. 3, 2008, 259-260.
4. *Hijmans H.,* The European Union as Guardian of Internet Privacy, The Story of Art 16 TFEU, Law, Governance and Technology Series, Vol. 31, Springer International Publishing Switzerland, 2016, 70, 100, 104.
5. *Karaboga M., Matzner T., Obersteller H., Ochs C.,* Is there a Right to Offline Alternatives in a Digital World? in Data Protection and Privacy: (In)visibilities and Infrastructures, *Leenes R., Brakel R.v., Gutwirth S., Hert P.D.,* (eds), Springer International Publishing AG, 2017.
6. *Lubin A.,* We Only Spy on Foreigners: The Myth of Universal Right to Privacy and the Practice of Foreign Mass Surveillance, Chicago Journal of International Law, Vol. 18, No. 2, 2018, 530-533, 536, 551.
7. *Milanovic M.,* The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa, EJIL:Talk! 2021, <https://www.ejiltalk.org/the-grand-

[82] Klass and Others v. Germany, [1978], ECtHR, N 5029/71, § 55.
Szabó and Vissy v. Hungary, [2016], ECtHR, N 37138/14, § 77.
[83] Ibid.

normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> [31.07.2023].

8. *O'Leary S.,* Balancing Rights in a Digital Age, Irish Jurist, Vol. 59, 2018, 92.
9. *Sloot B.v.d.,* Big Brother Watch and Others v. the United Kingdom & Centrum for Rattvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases? European Data Protection Law Review (EDPL), Vol. 7, No. 2, 2021, 325.
10. *Stepanovic I.,* Preventing Terrorism or Eliminating Privacy? Rethinking Mass Surveillance after Snowden Revelations, Strani Pravni Zivot (Foreign Legal Life), 2015(4), 236, 239.
11. *Watt E.,* The Right to Privacy and the Future of Mass Surveillance, International Journal of Human Rights, Vol. 21, No. 7, 2017, 789.
12. Centrum för Rättvisa v. Sweden, [2021], ECtHR, N 35252/08.
13. Big Brother Watch and Others v. the United Kingdom, [2021], ECtHR, N 58170/13, 62322/14, 24960/15.
14. Szabó and Vissy v. Hungary, [2016], ECtHR, N 37138/14.
15. Roman Zakharov v. Russia, [2015], ECtHR, N 47143/06.
16. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, [2014], CJEU, C-293/12, C-594/12.
17. Liberty and Others v. the United Kindgom, [2008], ECtHR, N 58243/00.
18. S. and Marper v. the United Kingdom, [2008], ECtHR, N 30562/04, 30566/04.
19. Weber and Saravia v. Germany, [2006], ECtHR, N 54934/00.
20. Amann v. Switzerland, [2000], ECtHR, N 27798/95.
21. Klass and Others v. Germany, [1978], ECtHR, N 5029/71.