Is the Case Law of ECtHR Ready to Prevent the Expansion of Mass Surveillance in the Post-Covid Europe?

Lusine Vardanyan*
Václav Stehlík**

Summary: The COVID-19 may become a new opportunity for expanding mass surveillance by states. It is already called a security threat, and states are taking appropriate measures to prevent it, including restricting human rights. Abandoning surveillance technology will not be easy after a pandemic and mass surveillance can become the standard for preventing threats. To prevent such a scenario, the approach of the European Court of Human Rights (ECtHR) may be a turning point in the expansion of mass surveillance. The research examines the current case-law of the ECtHR in order to analyse the attitude of ECtHR to mass surveillance. The research is focused on the question whether it can help to prevent the mass surveillance to be the norm for the post-pandemic world. The research reveals an increasing bias in case law of the ECtHR towards legalizing mass surveillance and the lack of updating the new criteria for the legality of mass surveillance. The ECtHR is likely to agree with most of the measures that states have introduced to prevent the COVID-19. Authors note that a due attention should be paid to human rights as potentially an effective tool to prevent widespread legalization of mass surveillance. The issue of using invasive tools to regulate mass surveillance, which are now used to resolve the COVID-19 situation, may become even more significant in the future.

Keywords: European Court of Human Rights, COVID-19, privacy, mass surveillance

* Lusine Vardanyan is a Ph.D. researcher at Palacky University in Olomouc, Law Faculty, Department of International and European Law, Czech Republic, e-mail: lucyrossetti77@gmail.com

** Václav Stehlík is an associate professor of EU law, at Palacky University in Olomouc, Law Faculty, Department of International and European Law, Czech Republic, e-mail: vaclav.stehlik@upol.cz. Václav Stehlík participated on the creation of this paper on behalf of project no. 20-27227S "The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union" funded by the Czech Science Foundation (GAČR).

1. Introduction

The term "mass surveillance" is used to describe the scope of data collection measures and can be applied within both the criminal legal paradigm and the paradigm related to the extraction of intelligence data in the protection of state security. However, digital surveillance has also become a "new type" of disease prevention. The pandemic made it possible to legalize mass surveillance as a method to fight against COVID-19. The World Health Organization (hereafter-WHO) mentions "tracing and quarantine of contacts" as one of core public health measures that breaks the chains of transmission[1] and as one of basic components it should be central to every national COVID-19 response.[2]

More and more countries (such as Spain, France, the United Kingdom, Italy, Germany, Switzerland, Israel, Estonia, Armenia or Latvia) have started using technologies to track the movement of citizens in order to monitor quarantine measures and establish contacts of patients. The impact of the pandemic on the level of human rights protection is undeniable. Ten of the forty-seven member countries of the Council of Europe have already notified about derogations from their obligations in emergency situations under article 15 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereafter ECHR) in connection with coronavirus infection. A more accurate assessment of this impact of COVID-19 in human rights will be seen when measures taken by the Governments will be analysed in judgments of the European Court of Human Rights (hereafter ECtHR). But at present the question arises: what is the attitude to mass surveillance in case-law of ECtHR and can it helps to prevent the mass surveillance to be the norm for the post-pandemic world?

2. Possible issues that COVID-19 may raise with ECtHR

The privacy or security debate has been going on for many years. With the development of digital technologies it has become one of the main moral, ethical and legal dilemmas. Yuval Noah Harari warns that humanity can lose freedom at a time when many are willing to sacrifice everything for the sake of a sense

[1] Considerations for quarantine of contacts of COVID-19 cases Interim guidance World Health Organization; 2020. 19 August 2020, p. 1.

[2] Critical preparedness, readiness and response actions for COVID-19. Geneva: World Health Organization, 2020. [online]. Available at: https://apps.who.int/iris/bitstream/handle/10665/332665/WHO-COVID-19-Community_Actions-2020.4-eng.pdf

of security in the uncertain future.[3] So the main question that always comes up in terms of choosing between these categories sounds like this: how much freedom are we willing to give up for keeping our security? COVID-19 re-actualizes this question. It has caused a new wave of increasing control over everyone. Against the background of the pandemic geo-location tracking, face recognition system deployment, software pre-installation obligations, and phone tracking are taking place. For example, mobile operators in Italy, Germany, Belgium and Austria provide officials with generalized data for monitoring compliance with the quarantine. This information is officially collected in the general databases, created in the context of panic over the COVID-19.

However, it would be naive to believe that these technologies have only just begun to be developed. Technologies that allow tracking persons and collecting data from them have long existed and are used by many states. Nick Srnicek in "Platform Capitalism"[4] shows, that for some of the modern digital platforms, the main business model is the collection of user data and their capitalization.

The legality of the use of these technologies has already been the subject of consideration by the ECtHR and it already has developed some criteria for evaluating the protection of digital rights. But the pandemic has opened new horizons for mass surveillance, made it easier and expanded the possibilities of collection of information about a person. Mass surveillance is evaluated as a means of ensuring security and even approved by the data subject itself, which no longer grabs its privacy, even if it transmits a larger volume of personal data.

Nevertheless, such technological measures introduced to prevent the spread of the coronavirus can be used as methods of mass surveillance. The human rights organization Amnesty International's Security Lab have released a report mentioning the contact tracing applications to track infections developed by several countries and have found some of them as most dangerous for privacy.[5] Therefore, the emergence of new tools for digital surveillance raises questions about the protection of digital rights, especially in unequal conditions of the state, business and users. The ECHR, as a guarantor of human rights, may prevent to some extent the use of the contract tracking apps as mass surveillance methods. This implies the need to adapt case law of the ECtHR to these kinds of modern challenges to privacy.

---

3 HARARI, Yuval, Noah. *The world after coronavirus 20 March 2020*. "The Financial Times". [online]. Available at: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

4 See more: SRNICEK, N. Platform Capitalism. **Cambridge**: Polity, 2016.

5 *Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy*. 16 June 2020. [online]. Available at: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

Contact tracking apps are used in about twenty eight countries, fourteen of them in Europe. Apps in Russia and Armenia were compulsory to download. In Germany, Austria, Italy mobile operators are sharing location data with health ministries. Another issue that will be considered in the near future is the possible revision of the limits of the right to privacy, which may change after the pandemic. It is difficult to say what these changes will be. But there is no doubt that issues of privacy can become even more significant and cause more controversy, and the processes of its contestation and approval are even more visible. In the context of a broad focus on privacy and digital surveillance, it is important to remember that privacy is the result of a challenge process involving different groups: business, the state, and many civic associations. There is no unambiguous concept of privacy taken abstractly and regardless of the society in which it exists. Helen Nissenbaum expresses the idea of contextual integrity,[6] according to which the concept of privacy varies depending on the context, the potential threats we perceive, and ethical considerations.

In this regard, it may be necessary for the ECtHR to re-examine the scope of article 8 of the ECHR, especially the right to informational self-determination in the context of the definitely new role of technologies in society, to outline new contours of other human rights, to consider the relationship between them and technologies, and to find new balances between individual and collective interests. Digital surveillance and special programs will be very difficult to stop when the pandemic ends, because it is a unique tool for censoring and monitoring the mood of ordinary citizens. Therefore, the fight for privacy gets a new impetus and quarantine restrictions can become a new additional reason for appeals to the ECtHR. According to the report of the Council of Europe a number of measures taken by the authorities in the context of coronavirus "*will inevitably encroach on rights and freedoms which are an integral and necessary part of a democratic society governed by the rule of law*".[7]

The ECtHR may once again face a wave of complaints from public organizations that will challenge the use of mass surveillance technologies by authorities not only during the pandemic, but also after it, with the "screwing in" of the surveillance mechanism through a facial recognition system or software. That measure brought in to protect citizens, when most people accept that they are needed, could outlast the current crisis. Joseph Cannataci, the UN special rapporteur on the right to privacy, warns against that threat to privacy when using

[6] NISSENBAUM, Helen. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Standford: Stanford University Press, 2009.

[7] Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. SG/Inf(2020)11, 7 April 2020, p. 2.

surveillance to track people who have survived the epidemic.[8] It is a global pandemic that can become a cover for future invasive electronic spies. Without a proper, especially supranational monitoring, there is a risk that these tough new measures will become the norm around the world. The practice of the ECtHR can both facilitate and hinder their legitimization. Therefore, in the near future, it may not face the question of defining the fine line between data collection and total control. Modern reality can become the test for the Europe and for the ECtHR readiness to protect human rights in the digital age.

3. The mass surveillance in the case law of the ECtHR before the case Big Brother Watch v. UK

Before 2016 the ECtHR formed fairly rigid criteria for ”strict necessity” of surveillance, which were applied not only within the framework of the criminal legal paradigm, but also in the framework of protecting national security. The approach to assessing mass data interception in the ECtHR began to take shape with the case of Weber and Saravia v. Germany.[9] There the ECtHR checked the compatibility of the German legislation with the ECHR, which allowed interception of telecommunications for the purpose of detecting and preventing such dangers as an armed attack on Germany or a terrorist act.[10] The ECtHR summarized the criteria that should be applied to assess the predictability of the legal framework governing surveillance, which were later confirmed in Liberty and others v. United Kingdom.[11] The Court developed six safeguards (called the Weber criteria) that must be introduced into national legislation to avoid abuse of power, namely: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; 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 recordings may or must be erased or the tapes destroyed.[12]

8 BACCHI, Umberto. *Coronavirus surveillance poses long-term privacy threat, U.N. expert warns* [online]. Available at: https://www.reuters.com/article/us-health-coronavirus-privacy/coronavirus-surveillance-poses-long-term-privacy-threat-un-expert-warns-idUSKBN21I1XG

9 ECtHR. Weber and Saravia v. Germany (Application no. 54934/00). Judgement of 29 June 2006.

10 Ibid., p. 4.

11 ECtHR. Liberty and Others v. the United Kingdom (Application no. 58243/00). Judgment of 1 July 2008.

12 Ibid., p. 95.

The ECtHR took an even stricter approach to privacy violations in Zakharov v. Russia.[13] To Weber's criteria listed above, the Court added the standard of "reasonable suspicion" when considering surveillance cases. Moreover, this standard is beginning to be considered in relation to a broader scope of law, and not only in the field of criminal investigation and search for missing persons, as was done, for example, in Iordachi and Others v. Moldova.[14] In Zakharov v. Russia the Court tried to apply this standard to the sphere related to the collection of intelligence data in the framework of protecting state security. The ECtHR considered the legality of the provision of the Federal Law of the Russian Federation on operational-search activities, which made possible to use surveillance and to obtain information about events or actions (inaction) that pose a threat to the state, military, economic, information or ecological security.[15] Due to uncertainty and vastness of the "*events or actions (inaction) that pose a threat to the state, military, economic, information or ecological security"* the Court concluded that such a law *"does not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national, military, economic or ecological security*".[16]

The ECtHR found that without access to relevant materials Russian courts were unable to verify whether there was a "substantial factual basis" to suspect the person being monitored.[17] The ECtHR recognized that, although signatory states have a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security, judges must ensure adequate and effective guarantees against abuse.[18] The fact that these measures were ordered by a judge is an important guarantee against arbitrariness. At the same time, the Court pointed out that the issue of permits for surveillance by a non-judicial service may be compatible with the ECHR. The Court emphasized the need for an authorization procedure independent from the executive, while accepting that non-judicial authorities may be competent to authorize interception if they are capable of verifying the existence of a reasonable suspicion.[19]

Besides, according to this judgment, the ECtHR will assess the accessibility of the domestic law, the scope and duration of the secret surveillance measures,

[13] ECtHR. Roman Zakharov v. Russia. (Application no. 47143/06 [GC]). Judgment of 4 December 2015, p. 10.

[14] See also ECtHR. Iordachi and Others v. Moldova. (Application no. 25198/02). Judgment of 10 February 2009, p. 51.

[15] Пункт 2 статьи 7 ФЗ «Об оперативно-розыскной деятельности» от 12 августа 1995 года N 144-ФЗ с посл. изм. и доп. // Собрание законодательства РФ. 1995. N 33. Ст. 3349.

[16] Ibid., p. 248.

[17] Ibid., p. 261–262.

[18] Ibid., p. 232.

[19] Ibid., p. 260.

the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, and, any notification mechanisms and the remedies provided for by national law.[20]

Afterwards in Szabó and Vissy v. Hungary the ECtHR tested Hungarian legislation for compliance with the ECHR to the extent that it allows this measure to be used to collect information in order to prevent terrorist acts or preserve national security.[21] The ECtHR stated that "*it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents*"[22] and that the priority now is to establish effective control over these laws.

The ECtHR interpreted the category of "necessary in a democratic society" as requiring "strict necessity," in the light of the particular character of the interference and the potential for mass surveillance. Surveillance must be strictly necessary in two senses: as a general consideration for the safeguarding of democratic institutions[23] and as a particular consideration for the obtaining of vital intelligence in an individual operation.[24]

The ECtHR also highlighted the need for authorization by the national courts (only in exceptional circumstances it is permissible to do so by the executive authorities, but only subject to subsequent judicial control).[25] The Court referring to Zakharov v. Russia held that "*in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny*".[26] Thus, we can see a tightening of the requirement of judicial control in comparison with Zakharov v. Russia. Hungarian legislation was strongly criticized by the ECtHR as not conforming to the principle of strict necessity. The ECtHR referring to the Zakharov case indicated that "*a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure – and this on the basis of an individual suspicion regarding the target*

[20] Roman Zakharov v. Russia. p. 238.

[21] Comp. ECtHR. Szabó and Vissy v. Hungary (Application no. 37138/14). Judgment of 12 January 2016, p. 7, 10 - 11. For an analysis of the judgment see also CARPENTER, Christine. *Privacy and Proportionality: Examining Mass Electronic Surveillance under Article 8 and the Fourth Amendment*. International and Comparative Law Review, 2020, vol. 20, no. 1, p. 37.

[22] Ibid., p. 68.

[23] Ibid., p. 54.

[24] Ibid., p. 73.

[25] Ibid., p. 77, 80, 81.

[26] Ibid., p. 77.

person".[27] The use of the "individual suspicion" standard instead of "reasonable suspicion" was criticized in concurring opinion of Judge Pinto de Albuquerque according to whom the ECtHR in the judgment chose the lower standard of an unqualified "individual suspicion". This "*diminishes significantly the degree of protection set out in Zakharov and previously in Iordachi and Others*".[28] Such an approach required national authorities to check whether there are sufficient grounds to intercept certain communications in each case.

The imposition of quite a strict framework on surveillance which was formed in the practice of the ECtHR until 2016 complicated the use of mass surveillance by states. The ECtHR welcomed only targeted surveillance and only if a set of Weber criteria against possible abuse were met.

4. The judgment of the ECtHR in Big Brother Watch v. UK and in Breyer v Germany: shift of approach

Judgment in Big Brother Watch v. UK

Following Snowden's revelations about the USA-UK surveillance and information exchange program, three applicants sued the UK.[29] They considered that several articles of ECHR were violated and tried to persuade the ECtHR to take into account the qualitative leap in the technical capabilities of state to intercept, store and process big data. In this case, the ECtHR considered the compliance of three main aspects of UK law governing mass electronic surveillance with the ECHR: the interception of communications, the exchange of intelligence, and the collection of metadata by telecommunications service providers.[30] Immediately after the trial Snowden announced: "*today we won*".[31] However, can this decision be considered as a victory of privacy?

---

[27] Ibid., p. 71.

[28] Concurring opinion of Judge Pinto de Albuquerque. p.18.

[29] ECtHR. Big Brother Watch and Others v. United Kingdom (Applications nos. 58170/12, 62322/14 and 24960/15). Judgement of 13 September 2018 (referral to Grand Chamber, 4 February 2019). For an evaluation of the judgement see also CARPENTER, Christine. *Privacy and Proportionality: Examining Mass Electronic Surveillance under Article 8 and the Fourth Amendment.* p. 41.

[30] Ibid., p. 269.

[31] Bulk Data Collection By NSA and GCHQ Violated Human Rights Charter, European Court Rules. 14 September, 2018. [online]. Available at: //https://massive.news/2018/09/14/bulk-data-collection-by-nsa-and-gchq-violated-human-rights-charter-european-court-rules/.

In Big Brother Watch v. UK the ECtHR concluded that mass surveillance per se does not violate the ECHR and confirmed that it is subject to the broad discretion that States have when choosing how best to achieve a legitimate goal of protecting national security.[32]

This approach was a repetition of the position expressed in Centrum för Rättvisa v. Sweden,[33] in which the ECtHR held that Sweden's bulk interception regime was not *per se* out of step with Article 8 of the ECHR and its operation was within the state's margin of appreciation in light of "*current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted*."[34] This re-approval delineates the position of the ECtHR, which it will adhere to when further developing its case law.

The ECtHR's recognition of mass data interception as permissible per se removes a number of key parameters of verification for "legality", "necessity in a democratic society" and "proportionality". The ECtHR identifies four stages of mass surveillance technology: data interception, filtering, selection by search criteria and verification by analysts and promises that the broad discretion of States to decide whether to use this regime will be combined with strict control in subsequent stages.[35] What exactly does the ECtHR exclude from verification?

Firstly, the ECtHR in Big Brother Watch[36] points out that the very idea of ex post facto notification of the operation of the person about his/her being under the surveillance is logically incompatible with a mass surveillance system and should, therefore, be discarded. Before that, the ECtHR held a different position, which was formed in cases Weber and Saravia v. Germany and Szabó and Vissy v. Hungary.[37] According to the Court's previous position, "*subsequent notification is inextricably linked to the effectiveness of judicial protection measures and, consequently, to the existence of effective safeguards against abuse of monitoring power, since, in principle, the individual concerned will have little recourse to the courts unless they are notified of measures taken without their consent*"; and

[32] Ibid., p. 314.

[33] ECtHR. Centrum För Rättvisa v. Sweden (Application no. 35252/08). Judgment of 19 June 2018, p. 112.

[34] Ibid., p. 112.

[35] ECtHR. Big Brother Watch and Others v. United Kingdom (Applications nos. 58170/12, 62322/14 and 24960/15). Judgement of 13 September 2018, p. 315, 329.

[36] Ibid., p. 317.

[37] Weber and Saravia p. 135, Szabó and Vissy v. Hungary, p. 86.

that notification should be sent as soon as possible after the end of surveillance when it would not undermine the purpose of the measure.[38]

Secondly, the ECtHR refused to consider it necessary to obtain prior judicial permission to conduct such operations. In Roman Zakharov v. Russia the ECtHR stated that if the competence to authorize surveillance is not vested in a judicial authority, this may be compatible with the ECHR if that authority is sufficiently independent from the executive.[39] In Szabó and Vissy v. Hungary the ECtHR specified authorization by the judicial authorities as a necessary guarantee and only in exceptional circumstances allowed authorization by the executive authorities, and then only subject to subsequent judicial review.[40] The ruling in the Big Brother Watch states that although in the United Kingdom permission to conduct mass surveillance was not issued by either a judge or an independent administrative authority, there are no problems because several indications show that there is no abuse of executive power.[41] In this part, the ECtHR agrees with the report of the Venice Commission that independent supervision may be able to compensate for the lack of a court-issued permit.[42] The removal of this procedural requirement indicates the creation of a different approach depending on states: what was criticized for Hungary, Russia, Croatia, and Bulgaria is acceptable for Sweden and the UK.

Thirdly, regarding the nature of the offences that give rise to mass surveillance, the ECtHR pointed out that the focus should shift to the stage of selecting the information received for verification.[43] At the same time, the ECtHR recognizes that the general mention of threats to national security in the applicable legal acts is already sufficient to meet this requirement for verification. Using such a broad concept to define the reason for mass surveillance makes it possible for states to justify it broadly. As an argument for the correctness of its judgment, the Court indicates that national security constituted one of the legitimate aims to which national law referred.[44]

Fourthly, the ECtHR did not impose strict requirements for the formulation of a range of offences in acts on specific operations, although it noted that the use of clear expressions would be highly desirable.[45] For example the Big Brother

[38] Ibid. p. 86.
[39] Ibid., p. 258.
[40] Ibid., p. 77, 80, 81.
[41] See ibid., p. 381.
[42] Ibid., p. 318.
[43] ECtHR. Big Brother Watch and Others v. United Kingdom.(Applications nos. 58170/12, 62322/14 and 24960/15) Judgement of 13 September 2018 (referral to Grand Chamber, 4 February 2019).
[44] Ibid., p. 333.
[45] Ibid., p. 342.

Watch concerned phrases such as "*material providing intelligence on terrorism (...) including, but not limited to, terrorist organizations, terrorists, active sympathizers, attack planning, fund-raising*".[46] Recognizing such uncertainty as acceptable can also be interpreted as a sign of agreement for the broadest possible discretion of states to use mass surveillance.

There is also no requirement to determine the individuals whose data can be intercepted by the state. What is surprising is quite a naive claim that "*it is clear that the intelligence services are (not) exercising an unfettered discretion to intercept whatever communications they wish*".[47] In terms of the limits of this discretion, the ECtHR points to the need to comply with national legislation, as well as the proportionality of mass interception of data for the purpose being pursued.[48]

Rather unlimited nature of the mass surveillance regime is also reflected in the fact that the ECtHR refuses to apply the rule previously deduced in the decision of the case Weber and Saravia,[49] that the search criteria applied to intercepted data must be specified in the operation order. As the Court mentioned it would "*unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic*".[50] The guarantee of protection from arbitrariness, according to the ECtHR, should be that these search words and so-called "selectors" should be subject to independent supervision.[51] Thus, by recognizing mass surveillance as permissible per se, the ECtHR further restricts the right to respect for privacy.

The ECtHR did not create new criteria for the mass surveillance regime, but relied on a list of criteria stated in case Weber and Saravia v. Germany. For some reason, the Court did not pay attention to the fact that technological and information development has undergone both quantitative and qualitative changes since 2006, and the criteria already developed by the Court's practice are insufficient for an adequate assessment of modern surveillance regimes. The problem is the comprehensive coverage of modern digital surveillance without any restriction or exception for individuals who have no connection to terrorism or serious crime.

Criticism of this approach was expressed by Judge Koskelo. In a partly concurring, partly dissenting separate opinion in Big Brother Watch, ECtHR Judge Koskelo, joined by Judge Turković, suggested that the ECtHR's case law assessing the minimum safeguards that should apply to bulk interception regimes in the context of national security was insufficient and in need of clarification: "*It*

[46] Ibid., p. 342, 156.
[47] Ibid., p. 337.
[48] Ibid.
[49] ECtHR. Weber and Saravia, p. 32.
[50] ECtHR. Big Brother Watch and Others v. United Kingdom, p. 340.
[51] Ibid., p. 340.

is obvious that such an activity – an untargeted surveillance of external communications with a view to discovering and exploring a wide range of threats – by its very nature takes on a potentially vast scope, and involves enormous risks of abuse. The safeguards against those risks, and the standards which under the Convention should apply in this regard, therefore raise questions of the highest importance. I am not convinced, in the light of present-day circumstances, that reliance on the Court's existing case-law provides an adequate approach to the kind of surveillance regimes like the one we are dealing with here."[52]

As for the advantages of this decision, however, it is worth mentioning the expansion of the range of information that could be intercepted in violation of article 8 ECHR: from the content of messages to related communications data (metadata). The Regulation of Investigatory Powers Act allowed the UK's intelligence services to search and examine, without restriction, "linked communications data" of all intercepted communications on the grounds that metadata is less intrusive than content data, and it was necessary to determine whether a person was or was not in the British Isles. The Court took a slightly different approach to this issue, considering that shared access to the content of messages violates the essence of the right to privacy, although this does not apply to metadata, hence revealing the difference between them. This approach explicitly ignores that this distinction between access to message content or metadata is very problematic: metadata can often reveal more confidential information about the data subject and mass surveillance of metadata is much more effective than accessing content.[53] For example, the content of message may not reveal anything remarkable about the sender/recipient. But metadata could reveal for example the identity of the sender/recipient or his geographic position.

The Court recognizes that metadata is one of main tools for the intelligence services, but does not believe that the authorities did the right thing by completely exempting them from the safeguards applicable to the search and study of content. The ECtHR held that national law concerned did not provide real guarantees for the selection of metadata for verification and, thus, violated article 8 ECtHR, since it did not meet the quality requirements of the law and was unable to deter interference in what is necessary in a democratic society.

Refusal to recognize the acquisition of related communications data "*necessarily less intrusive than the acquisition of content*"[54] does not mean that the Court's

[52] Big Brother Watch partly concurring, partly dissenting separate opinion of Judge Koskelo, joined by Judge Turković, p. 3.

[53] For more see for example Bernal, Paul. Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 2016, vol. 1, no. 2, pp. 243–264.

[54] Big Brother Watch partly concurring, partly dissenting separate opinion of Judge Koskelo, joined by Judge Turković, p. 3, ibid., p. 356.

approach to the equality of these categories of information is already established. The ECtHR will be forced to formulate a clearer position in the near future and it is possible that a number of cases will challenge the legality of collecting or sufficient guarantees for collecting and storing information (especially metadata) through applications that were designed to prevent the spread of COVID-19. Yet the ECtHR has not equalized the modes of verification of interception of the content of messages and their metadata, did not reach the applicability of Weber's criteria to metadata and did not recognize metadata interception as the same as gaining access to the content of messages. But even this "rudimentary" position of the Court regarding the protection of metadata should definitely be considered a significant step towards ensuring comprehensive protection of privacy.

Follow-up of Big Brother Watch: case Breyer v. Germany

The decision in Big Brother Watch can be considered as one of the significant decisions that will determine the approach for further case law of the ECtHR for a long time to come. And this is far from an assumption: already on 30 January 2020 in Breyer v. Germany[55] the ECtHR held that the indiscriminate storage of subscriber information by telecommunications service providers did not violate article 8 of the ECHR. The applicants claimed that the obligation to keep their data under article 111 of the Telecommunications Act (hereinafter – TA) violated their right to privacy, "*as it forced them to disclose their personal data, which was subsequently stored*".[56] In their opinion, the violations were very serious because the storage of subscriber information by telecommunications service providers is possible without providing preliminary requirements. The article 111 of the TA did not contain any preliminary requirements for storage. Moreover, the law allows the storage of information not for a targeted subscriber, but for all mobile-telephone users. This regulation practically makes it possible to store information about those subscribers, which do not pose any danger or risk for public safety or national security.[57]

The ECtHR first held that "*Article 8 of the Convention (...) provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such form or manner that their Article 8 rights may be engaged*".[58] After that it pointed out that the mere storage

[55] ECtHR Breyer v. Germany (Application no. 50001/12). Judgement of 30 January 2020.
[56] Ibid., p. 66.
[57] Comp. ibid., p. 67.
[58] Ibid., p. 75.

of data relating to a person's private life, and therefore section 111 of the TA, constituted interference within the meaning of article 8 of the Convention.[59] As for its justification, it repeated that " [*I]n the context of, inter alia, storage of personal information it is essential to have clear, detailed rules governing minimum safeguards concerning amongst other things duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction*".[60]

ECtHR found that the intervention is pursuing the legitimate aims of public safety, prevention of disorder or crime and the protection of the rights and freedoms of others.[61] For this measure to be necessary in a democratic society, it must meet urgent social needs and be proportionate.[62] According to the Court, fighting crime, ensuring public safety and protecting citizens were indeed urgent social needs. In order to assess the proportionality of the measure, the Court subsequently determined the level of interference with the applicants' right to privacy. Agreeing with the German Constitutional Court, it stated that this data does not include any personal information, does not allow creating personal profiles or tracking the movements of mobile phone subscribers, and also relates to individual communication events.[63]

The ECtHR also came to the conclusion that the interference was, while not trivial, of a rather limited nature.[64] With regard to the rules for future access and use of collected data, the Court found that sections 112 and 113 of the TA contained sufficient limiting factors to make the interference proportionate. It was also noted that the collected data was "*further protected against excessive or abusive information requests by the fact that the requesting authority requires an additional legal* basis to retrieve the data".[65] The exemptions were limited to the requirement of necessity, which in the context of prosecution for offences meant "*that there must be at least an initial suspicion*".[66]

The ECtHR concluded that the retention of subscriber data for government purposes, without discrimination and regardless of whether there is a reasonable suspicion of the concerned person does not violate the ECHR. This is an extension of the already selected trend of the ECtHR, which was already in the case of Big Brother Watch. The permissibility of mass surveillance per se is not

[59] Ibid., p. 81.
[60] Ibid., p. 83.
[61] Ibid., p. 86.
[62] Ibid., p. 88.
[63] Ibid., p. 92.
[64] Ibid., p. 95.
[65] Ibid., p. 100.
[66] Ibid., p. 100.

inconsistent with the ECHR and does not exceed the broad discretion that governments have when choosing the means to achieve the legitimate goal of protecting national security. If inappropriate collection of such information can be allowed, then the storage of subscriber data is not extraordinary. In his dissenting opinion, Judge Ranzoni criticized the decision in Breyer. According to him, the ECtHR, as well as the German Constitutional Court, overlooked the fact that the data in question, admittedly, is not sensitive in itself, "*It ... facilitates the identification of the parties to every telephone call or message exchange and (consequently) the attribution of possibly sensitive information to an identifiable person*".[67]

Judge Ranzoni also disagreed with the majority regarding the assessment of safeguards and whether the existing ones are sufficient in order to effectively prevent the misuse and abuse of personal data.[68] In particular, he argued that, in the circumstances, the concept of a "double lock" could not be considered an effective protection from the moment the data was received, although it was based on broad and general provisions that might be sufficient as legitimate door keys that do not require an order from a judicial or other independent authority. In addition, since individuals are not notified after their data has been received, "*the victim of the interference has no knowledge and cannot seek a review of the information retrieval*".[69] The observation that compensation may nevertheless be required together with judicial proceedings for damages in respect of final decisions of the authorities, moreover "*only applies to information requests that have led to further telecommunication surveillance or other investigative measures*".[70]

Based on the above, we can conclude that the modern approach of the ECtHR to mass surveillance gives broad discretionary powers to states, opening the possibility for extensive use of mass surveillance technologies by states.

5. Why did the ECtHR choose this approach?

It may be argued that the acceptable recognition of mass surveillance per se is in fact a legalisation of current European national policies in this area. The same approach is more likely to be followed by the ECtHR in its case law in the near future. The ECtHR stated that "*the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within states' margin of appreciation*", adding that such regimes

[67] Dissenting Opinion of Judge Ranzoni (Breyer v. Germany), p. 5.
[68] Ibid., p. 18.
[69] Ibid., p. 23.
[70] Ibid., p. 24.

are "*valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime*".[71] But the real reason for this legitimization still lies in another plane: states always seek to get and use the data of their citizens and any change that can be adjusted to national security will most probably be used to get this data.

After the terrorist attacks that have occurred in Europe since 2015, Germany,[72] France,[73] United Kingdom,[74] Austria,[75] Italy,[76] Sweden[77] and many other states passed almost identical laws that give their national surveillance agencies very broad ability to conduct mass surveillance. Detailed consideration of these laws is beyond the scope of this study. But even a superficial analysis of these legal acts shows their inconsistency with the case law of the ECtHR already developed at the time of their adoption.

First, in Zacharov the ECtHR was sceptical of broad definitions in the context of "*national, military, economic or ecological security*" that provide "*an almost unlimited degree of discretion*."[78] In case Kennedy v. the UK the ECtHR noted that "*the condition of foreseeability does not require states to set out exhaustively by name the specific offences which may give rise to interception*",[79] "*it obliges them to provide sufficient details about the nature of the offences in question*".[80] This suggests that surveillance laws should be precise enough to give citizens an

71 Ibid., p. 386.

72 Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes Vom 23 Dezember 2016. [online]. Available at: https://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/18_wp/BND-Gesetz/bgbl.pdf;jsessionid=03D24BF37F441A72BF4E5FB3E0F5AC73.2_cid294?__blob=publicationFile&v=1

73 LOI n. 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (1) NOR: DEFX1521757L. [online]. Available at: https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte.

74 The UK Investigatory Powers Act 2016. [online]. Available at: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

75 Sicherheitspolizeigesetz, BGBl Nr. 662/1992, last amended by BGBl I Nr. 44/2014. [online]. Available at: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792.

76 *D.L. 18 febbraio 2015, n. 7 1 2, Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione (15G00019) (GU Serie Generale n.41 del 19-02-2015).*

77 Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet. SFS 2018:1918. [online]. Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717.

78 Ibid., p. 248.

79 Ibid., p. 159.

80 Ibid.

indication of the circumstances that may warrant surveillance. But the national legal acts may tend to allow mass surveillance on broad grounds.

Second, almost all the laws have a lack of adequate legal guarantees for data subjects. For example in the UK the Investigatory Powers Act 2016[81] introduced the double-lock mechanism requiring judicial approval.[82] But the law limits the scope of review by the Judicial Commissioners and they do not have full authority to assess the merits of surveillance measures. In France the Intelligence Act 2015 on the basis of article L. 811-3, expanded the number of purposes that can justify extra-judicial surveillance, at the same time does not establish any mandatory judicial pre-authorization process. Marc Trévidic mentions this situation as "*a total absence of control in this law*" with regard to the interception of calls, text messages and emails by the security services, "*extra-judicial surveillance with the approval of the Prime Minister, which also provides for the creation of 'black boxes' that track data on the connection of all Internet users*".[83] But as we mentioned before, these criteria were of importance for the ECtHR: in Roman Zakharov v. Russia the Court accepts that the requirement of prior judicial authorization constitutes an important safeguard against arbitrariness.[84]

Third, most of laws do not restrict protection from the collection and analysis of privileged communications, including foreign public officials, parliamentarians both inside and outside the borders of Europe. In Kennedy v. the United Kingdom, which concerns the Swiss government's use of the telephone lines of a lawyer, the ECtHR explicitly noted the need to establish clear rules and guarantees under the law for such privileged communications.[85]

Against the background of this situation, having changed its attitude to mass surveillance in cases such as Centrum för Rättvisa and Big Brother Watch, the ECtHR expresses the general approach of European states after 2015. To strengthen its position in the Big Brother Watch case, the ECtHR regularly refers to the report of the Venice Commission.[86] The report recognizes that "*the main*

---

[81] See article 140 of the Investigatory Powers Act 2016. [online]. Available at: https://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.

[82] A dual executive-judicial pre-authorization process for its foreign bulk warrants.

[83] *Loi renseignement: "Une arme redoutable entre de mauvaises mains", s'inquiète Marc Trévidic*. [online]. Available at: https://www.rtl.fr/actu/debats-societe/la-loi-sur-le-renseignement-entre-de-mauvaises-mains-est-une-arme-redoutable-estime-le-juge-marc-trevidic-7777296541

[84] Ibid., p. 249.

[85] ECtHR. Kopp v. Switzerland (Application - 23224/94). Judgment of 25 March 1998, p. 71–75.

[86] *Report on the Democratic Oversight of Signals Intelligence Agencies*. Strasbourg, 15 December 2015 Study No. 719/2013 CDL-AD(2015) 011 Or. Engl. European Commission for Democracy through Law (Venice Commission) Adopted by the Venice Commission At Its 102nd Plenary Session (Venice, 20-21 March 2015). [online]. Available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

interference with privacy occurred when stored personal data was accessed and/or processed by the agencies."[87] As we can see, the data collection stage is not mentioned here, which means that the data collection can be considered per se consistent with the ECHR.

6. Conclusions

The ECtHR has already formulated an approach to the legal acts regulating mass surveillance for compliance with the ECHR. Most probably the situation will further strengthen the position formed after Big Brothers Watch and Centrum för Rättvisa cases. Despite the fact that Big Brother Watch case is currently being considered by the Grand Chamber of the ECtHR, it seems improbable to have a change in the approach of the ECtHR especially with the emergence of COVID-19, which becomes the turning point in the issue of expanding mass surveillance.

In the situation when COVID-19 is already considered a threat to security, the states take appropriate measures, including restricting human rights. To abandon surveillance technology will not be easy after a pandemic, and mass surveillance can become the standard for preventing and managing threats. By rejecting to review the list of minimum requirements in the Big Brother Watch the ECtHR missed a chance to make its case law more adaptable to challenges in post-pandemic world.

The ECtHR new approach to mass surveillance may serve as a guide for the development of national legislation and may provoke the adoption of such legislation in states where it is not yet available. Due to the COVID-19 mass surveillance by governments is becoming the new norm and may be expected to expand even further in the future justified by insurance of the security of people. If ECtHR delays updating the new criteria for the legality of mass surveillance in the near future, states may try to interpret such a provision as a carte blanche at the European level the expansion of the mass surveillance.

At the end, we would like to emphasise that a due attention should be paid to the potential of human rights as an effective tool to prevent widespread legalization of mass surveillance. The issue of using invasive tools to regulate mass surveillance, which are now increasingly used by governments to resolve the pandemic situation, may become even more significant in the future. Even without derogations under article 15 of the ECHR, the ECtHR might agree with most of the measures that states have introduced to combat the pandemic. Therefore,

[87] ECtHR. Centrum För Rättvisa v. Sweden (Application no. 35252/08). Judgment of 19 June 2018, p. 69.

the answer of the main question of the research is that the modern attitude to mass surveillance in case law of ECtHR does not help much to prevent the mass surveillance to be the norm for the Post-pandemic world.

List of references

BACCHI, U. *Coronavirus surveillance poses long-term privacy threat, U.N. expert warns* [online]. Available at: https://www.reuters.com/article/us-health-coronavirus-privacy/coronavirus-surveillance-poses-long-term-privacy-threat-un-expert-warns-idUSKBN21I1XG

Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy. 16 June 2020. [online]. Available at: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

BERNAL, P. Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 2016, vol. 1, no. 2, pp. 243–264.

Bulk Data Collection By NSA and GCHQ Violated Human Rights Charter, European Court Rules. 14 September, 2018. [online]. Available at: //https://massive.news/2018/09/14/bulk-data-collection-by-nsa-and-gchq-violated-human-rights-charter-european-court-rules

CARPENTER, Ch. *Privacy and Proportionality: Examining Mass Electronic Surveillance under Article 8 and the Fourth Amendment*. International and Comparative Law Review, 2020, vol. 20, no. 1, pp. 27–57.

Critical preparedness, readiness and response actions for COVID-19. Geneva: World Health Organization, 2020. [online]. Available at: https://apps.who.int/iris/bitstream/handle/10665/332665/WHO-COVID-19-Community_Actions-2020.4-eng.pdf

HARARI, Yuval, Noah. *The world after coronavirus 20 March 2020.* "The Financial Times". [online]. Available at: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Loi renseignement: "Une arme redoutable entre de mauvaises mains", s'inquiète Marc Trévidic. [online]. Available at: https://www.rtl.fr/actu/debats-societe/la-loi-sur-le-renseignement-entre-de-mauvaises-mains-est-une-arme-redoutable-estime-le-juge-marc-trevidic-7777296541

NISSENBAUM, H. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Standford: Stanford University Press, 2009.

Report on the Democratic Oversight of Signals Intelligence Agencies. Strasbourg, 15 December 2015 Study No. 719/2013 CDL-AD(2015) 011 Or. Engl. European Commission for Democracy through Law (Venice Commission) Adopted by the Venice Commission At Its 102nd Plenary Session (Venice, 20-21 March 2015). [online]. Available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e

Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. SG/Inf(2020)11, 7 April 2020, p. 2.

SRNICEK, Nick. *Platform Capitalism*. Cambridge: Polity, 2016.

Case-law

ECtHR. Kopp v. Switzerland (Application – 23224/94). Judgment of 25 March 1998.

ECtHR. Weber and Saravia v. Germany (Application no. 54934/00). Judgement of 29 June 2006.

ECtHR. Liberty and Others v. the United Kingdom (Application no. 58243/00). Judgment of 1 July 2008.

ECtHR. Iordachi and Others v. Moldova. (Application no. 25198/02). Judgment of 10 February 2009.

ECtHR. Roman Zakharov v. Russia. (Application no. 47143/06 [GC]). Judgment of 4 December 2015.

ECtHR. Szabó and Vissy v. Hungary (Application no. 37138/14). Judgment of 12 January 2016.

ECtHR. Centrum För Rättvisa v. Sweden (Application no. 35252/08). Judgment of 19 June 2018.

ECtHR. Big Brother Watch and Others v. United Kingdom (Applications nos. 58170/12, 62322/14 and 24960/15). Judgement of 13 September 2018.

ECtHR. Breyer v. Germany (Application no. 50001/12). Judgement of 30 January 2020.

Legislation and other sources

Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes Vom 23 Dezember 2016. [online]. Available at: https://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/18_wp/BND-Gesetz/bgbl.pdf;jsessionid=03D24BF37F441A72BF4E5FB3E0F5AC73.2_cid294?__blob=publicationFile&v=1

Investigatory Powers Act 2016. [online]. Available at:
https://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf

Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet. SFS 2018:1918. [online]. Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717

LOI n. 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (1) NOR: DEFX1521757L. [online]. Available at: https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte

Пункт 2 статьи 7 ФЗ «Об оперативно-розыскной деятельности» от 12 августа 1995 года N 144-ФЗ с посл. изм. и доп. // Собрание законодательства РФ. 1995. N 33. Ст. 3349

Sicherheitspolizeigesetz, BGBl Nr. 662/1992, last amended by BGBl I Nr. 44/2014. [online]. Available at: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792

The UK Investigatory Powers Act 2016. [online]. Available at: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted