

BULK SURVEILLANCE BETWEEN NATIONAL SECURITY AND RIGHT TO PRIVACY

Veljko Turanjanin, PhD¹

Faculty of Law, University of Kragujevac, Serbia

Abstract: An author deals with the bulk surveillance and its relationship with right to privacy. Intensive ICT development enables various modern techniques and methods of crime investigation but also results in some new types of criminal offences that could be committed using ICT. Expansion of the fundamental rights and their protection, especially in Europe, raised global awareness about right to privacy and the need to protect it. Having that in mind it seems that the main question that should be answered by legislator is: Where is the borderline between the right to privacy and the public interest to investigate or prevent crime and collect evidence. European Court of Human Rights deeply examined this issue and developed criteria earlier established in famous judgement in a case Weber and Saravia. States enjoyed a wide margin of appreciation in deciding what type of interception regime was necessary to protect national security, but considered that the discretion afforded to states in operating an interception regime would necessarily be narrower. The ECtHR had identified six “minimum safeguards” which should be set out in law to avoid abuses of power: the nature of offences which 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, and the circumstances in which intercepted data may or must be erased or destroyed. The author in this paper explains international legal instrument that authorize surveillance of communication as well as its boundaries.

Keywords: bulk surveillance, the right to privacy, national security, ECtHR's jurisprudence

1 vturanjanin@jura.kg.ac.rs



INTRODUCTION

The relationship between technology and society has been a notoriously complex and slippery area of scholarship for decades. In the modern time it is getting a new form (Kiernan & Mueller, 2021: 22). Besides numerous changes, the technology changed the way we relate to another and to government (Leavens, 2015: 709). George Orwell's distant and dark *1984* would probably agree that one of the most effective ways in which an oppressive government can eliminate the personal liberties of its citizens is to deprive them of their privacy (Weber, 1971; Turanjanin, 2020: 268). In ideal world, government surveillance has to be driven by public security and enforcement interests and checked by individual privacy rights, but in recent years this balance has been gradually shifting as a result of growing national and global unrest, developing surveillance capabilities, and the erosion of privacy protections (Yadin, 2017: 709). Our communications and activities today routinely leave rich digital traces that can be collected, analyzed, and stored at low cost (Wong, 2015). Government surveillance of cyberspace is, unfortunately, unreasonably extensive and constant, mostly unhindered by legal restrictions; surveillance of physical spaces is not as prevalent or as unrestrained (Yadin, 2017: 709). In the United States, 11 September 2001 significantly altered the rules of privacy (Heymann, 2016: 428), while the globalisation of crime and terrorism justified the creation of an *Orwellian state* (Robis, 2014: 203), but we could say that is a problem in the rest of the world that is going toward totalitarian society (Nomikos, 2017; Jacobs, 2009). Although surveillance is not a new phenomenon, mass surveillance is (Franks, 2017). In the United States, surveillance that people cannot feasibly escape receives more Fourth Amendment scrutiny, while surveillance that can be avoided receives less, or none (Tokson, 2021).

Tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on law that is particularly precise (Jayawickrama, 2002: 629). Also, property rights are not excluded (Woodburn, 2016). This is, in addition, a very sensitive area due to the protection of the data (Norris, Hert, L'Hoiry, & Gletta, 2017; Flaherty, 1989: 371-377).² So, societies directed by the rule of law consider that governments should only gather information about us when it is useful to reach a goal more important than our personal right to be a manager of what gets known about us (Moonen, 2010: 98). Significant contribution in this field arising from the European Court of Human Rights (hereinafter: the ECtHR) standpoint (more than 20 years old) that legislators should clearly recognize circle of subjects who could be exposed to this measure but also nature (types) of crime where it is applicable; time limitations of its application; conditions for taking the record on the measure; methods of controlling these records and reasons for destroying collected material.³ These standpoints could be seen as the steps towards unification, which is the milestone and essential starting point of the idea to establish a united Europe. Interception of communications is a very complex issue (Rona & Aarons, 2016: 512) and the ECtHR has, from the *Leander* case onwards, always moved towards a progressive extension of the scope of Article 8 (Sicurella and Scalia, 2013: 434-435).

² The mass surveillance is a very interesting issue in time of coronavirus (Ram & Gray, 2020). Our protection, however, can be improved by surveillance intermediaries (Rozenshtein, 2018: 99).

³ *Huvig v. France*, ECtHR, Application no. 11105/84, April 24, 1990 and *Kruslin v. France*, ECtHR, Application no. 11801/85, April 24, 1990.



THE BULK INTERCEPTION OF COMMUNICATIONS

The bulk interception of cross-border communications,⁴ which is usually implied within the broader term of digital surveillance (Ünver, 2018), by the intelligence services faces specific difficulties.⁵ The Grand Chamber of the ECtHR reached decision in two important cases: *Big Brother Watch and Others v. the United Kingdom* and *Centrum för Rättvisa v. Sweden*. Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and states enjoy a wide margin of appreciation in deciding what type of interception regime is necessary. However, such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present in a case of bulk surveillance.

During the years, the ECtHR established certain minimum safeguards which should be set out in law to avoid abuses of power: the nature of offences which 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 parties⁶, and the circumstances in which intercepted data may or must be erased or destroyed.⁷ Additionally, the ECtHR takes care of the arrangements for supervising the implementation of secret surveillance measures, the existence of notification mechanisms and any remedies provided for by national law.⁸

According to the ECtHR, the stages of the bulk interception process which fall to be considered can be described as follows:

- (a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);
- (b) the application of specific selectors to the retained communications/related communications data;
- (c) the examination of selected communications/related communications data by analysts; and
- (d) the subsequent retention of data and use of the “final product”, including the sharing of data with third parties.⁹

At the first stage, electronic communications will be intercepted in bulk by the intelligence services. Normally, these communications will belong to a large number of individuals and some communications may be filtered out at this stage.¹⁰ The initial searching takes place at the second stage, when different types of selectors, including “strong selectors” (such as an email address) and/or complex queries are applied to the retained packets of communications and related communications data. This may be the stage where the process begins to target individuals through the use of strong selectors.¹¹ At the third stage, intercept material is examined for the first time by an analyst.¹² The final stage is when the intercept material is actually used by the intelligence services. This may involve the creation of an intelligence report, the disseminating of the material to other intelligence services within the intercepting State, or even the transmission of material to foreign intelligence services.¹³ At the end of this process, the need for safeguards will be at its highest,¹⁴ whose approach is in line with the finding of the Venice Commission. Particularly important is the fact that the ECtHR believes that the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference.



In assessing whether the state acted within its margin of appreciation, the ECtHR started to develop a new, wider range, of criteria than the six *Weber* safeguards – in addressing jointly *in accordance with the law* and *necessity* as is the established approach in this area, the ECtHR added eight criteria:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
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.¹⁵

Some states today share material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. Unfortunately, the ECtHR has not provided specific guidance regarding the precautions to be taken when communicating intercept material to other parties. The ECtHR considers that the transmission by one state to a foreign state(s) or international organization(s) of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself.

The ECtHR in *Big Brother Watch and Others* emphasized four important rules that have to be followed in these cases. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring state must ensure that the receiving state, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving state must have comparable protection to that of the transferring state; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred. Finally, the ECtHR considers that the transfer of material to foreign intelligence partners should also be subject to independent control.¹⁶

THE RECEIPT OF INTELLIGENCE FROM FOREIGN INTELLIGENCE SERVICES

The second problem in this field is the receipt of intelligence from foreign intelligence services. In *Big Brother Watch and Others* we have the receipt by the United Kingdom authorities of material from foreign intelligence services, more specifically the receipt of material intercepted by the NSA under PRISM and Upstream. The question is was it in breach of the rights under Article 8 of the Convention.



The Chamber took the position that there is no violation of Article 8. The Chamber applied a modified version of the six minimum safeguards, because the first two requirements could not apply to the act of requesting intercept material from foreign governments. The Chamber instead asked whether the circumstances in which intercept could be requested was circumscribed sufficiently to prevent States from using the power to circumvent domestic law or their Convention obligations. It then applied the final four requirements to the treatment of intercept material once it had been obtained by the United Kingdom intelligence services. The Chamber considered that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicated with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence services. Moreover, the Chamber found no evidence of any significant shortcomings in the application and operation of the regime. In the Chamber's view, the interception of communications by foreign intelligence services could not engage the responsibility of a receiving State, or fall within that State's jurisdiction within the meaning of Article 1 of the Convention, even if the interception was carried out at that State's request.

The ECtHR developed another applicable test. First of all, the Chamber considered that these would only be relevant if the foreign intelligence services were placed at the disposal of the receiving State and were acting in exercise of elements of the governmental authority of that State; if the receiving State aided or assisted the foreign intelligence services in intercepting the communications where that amounted to an internationally wrongful act for the State responsible for the services, the receiving State was aware of the circumstances of the internationally wrongful act, and the act would have been internationally wrongful if committed by the receiving State; or if the receiving State exercised direction or control over the foreign Government. Secondly, according to the ECtHR's case-law the interception of communications by a foreign intelligence service could only fall within the receiving State's jurisdiction if that State was exercising authority or control over the foreign intelligence service.¹⁷ The Grand Chamber agreed with the Chamber that none of these elements were present in the situation under consideration. Therefore, any interference with Article 8 of the Convention could only lie in the initial request and the subsequent receipt of intercept material, followed by its subsequent storage, examination and use by the intelligence services of the receiving State.¹⁸

Furthermore, where a request is made to a non-contracting State for intercept material the request must have a basis in domestic law, and that law must be accessible to the person concerned and foreseeable as to its effects.¹⁹ It will also be necessary to have clear detailed rules which give citizens an adequate indication of the circumstances in which and the conditions on which the authorities are empowered to make such a request²⁰ and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention. Upon receipt of the intercept material, the ECtHR considers that the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards, first developed by the ECtHR in its case-law on the interception of communications by Contracting States, are equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If States do not always know whether material received from foreign intelligence services is the product of interception, then the ECtHR considers that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept.²¹ Finally, the ECtHR considers that any regime permitting the intelligence services to request either interception or intercept material from non-Contracting

21 *Big Brother Watch and Others*, § 497.



States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review.²²

In *Big Brother Watch and Others* the ECtHR considered that the regime for requesting and receiving intercept material was compatible with Article 8 of the Convention. There existed clear detailed rules which gave citizens an adequate indication of the circumstances in which and the conditions on which the authorities were empowered to make a request to a foreign intelligence service; domestic law contained effective guarantees against the use of such requests to circumvent domestic law and/or the United Kingdom's obligations under the Convention; the United Kingdom had in place adequate safeguards for the examination, use, storage, onward transmission, erasure and destruction of the material; and the regime was subject to independent oversight by the IC Commissioner and there was a possibility for *ex post facto* review by the IPT. Accordingly, there had been no violation of Article 8 of the Convention.

CONCLUSION

To establish a balance between the protection of the right to privacy and human rights on the one hand, and the protection of society from crime and national security on the other, should be one of the key goals of the state in modern forms of state response to crime. It is definitely not an easy task to respect privacy, provide security, and protect against abuse in the contemporary, modern, digitally connected world (Daskal, 2017). As the jurisprudence of the ECtHR often shows, states very easily slip into the field of human rights violations.

REFERENCES

1. *Big Brother Watch and Others v. the United Kingdom*, Application nos. 58170/13, 62322/14 and 24960/15 (ECtHR May 25, 2021).
2. *Centrum för Rättvisa v. Sweden*, Application no. 35252/08 (ECtHR May 25, 2021).
3. Flaherty, D. H. (1989). *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. University of North Carolina Press.
4. Franks, M. A. (2017). Democratic Surveillance. *HARV. J. L. & TECH.* 30, no. 2, 425-489.
5. Freiwald, S. (2008). Electronic Surveillance at the Virtual Border. *Miss. L.J.*, 78, 333-368.
6. Heymann, P. B. (2016). An Essay on Domestic Surveillance. 8 *J. NAT'l Sec. L. & POL'y*, 421-435.
7. *Huvig v. France*, Application no. 11105/84 (ECtHR April 24, 1990).
8. Jacobs, B. (2009). Keeping Our Surveillance Society Non-Totalitarian. *Amsterdam L.F.*, 1, 19-34.
9. Kiernan, C. J., & Mueller, M. L. (2021). Standardizing Security: Surveillance, Human Rights, and the Battle Over Tls 1.3. *Journal of Information Policy*, 11, 1-25.
10. *Kruslin v. France*, Application no. 11801/85 (ECtHR April 24, 1990).
11. Landau, S. (2016). Choices: Privacy & Surveillance in a Once & Future Internet. *Daedalus*, 145, 54-64.

²² *Id.*, § 498.



12. Leavens, A. (2015). The Fourth Amendment and Surveillance in a Digital World. *J. C.R. & ECON. DEV.*, 27, 709-746.
13. Nomikos, L. (2017). Are We Sleepwalking into a Surveillance Society. *BLR*, 2017, 111-122.
14. Norris, C., Hert, P. d., L'Hoiry, X., & Gletta, A. (2017). *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*. Cham: Springer.
15. Ram, N., & Gray, D. (2020). Mass Surveillance in the Age of COVID-19. 7 *J.L. & Biosciences*.
16. Robis, L. A. (2014). When Does Public Interest Justify Government Interference and Surveillance. 15 *Asia-PAC. J. oN HUM. Rts. & L.*, 203-218.
17. Roman Zakharov v. Russia, Application no. 47143/06 (ECtHR December 04, 2015).
18. Rozenshtein, A. Z. (2018). Surveillance Intermediaries. *Stan. L. REV.*, 70.
19. S. and Marper, Applications nos. 30562/04 and 30566/04 (ECtHR December 04, 2008).
20. Schweda, S. (2015). UK surveillance under judicial scrutiny: GCHQ intelligence sharing with NSA contravened human rights, but is now legal. *Eur. Data Prot. L. Rev.*, 1, 61-69.
21. Scott, P. F. (2017). General Warrants, Thematic Warrants, Bulk Warrants: Property Interference for National Security Purposes. *N. IR. LEGAL Q.*, 68, 99-121.
22. Squires, D. (2006). The Problem with Entrapment. *Oxford Journal of Legal Studies*, 26(2), 351-376.
23. Tokson, M. (2021). Inescapable Surveillance. *CORNELL L. REV.*, 106, 409.
24. Turanjanin, V. (2020). Video Surveillance of the Employees Between the Rights to Privacy and Rights to Property after Lopez Ribalda and Others v. Spain. *University of Bologna Law Review*, Vol. 5, no. 2, 268-293.
25. Ünver, H. A. (2018). Politics of Digital Surveillance. *National Security and Privacy* 5 .
26. Yadin, G. (2017). Virtual Reality Surveillance. 35 *CARDOZO Arts & ENT. L.J.*, 707-743.
27. Weber, S. J. (1971). Habeas Data: The Right of Privacy Versus Computer Surveillance. *U.S.F. L. REV.*, 5 , 358.
28. Wong, C. M. (2015). Internet at a Crossroads: How Government Surveillance Threatens How We Communicate. *World report, HUMAN RIGHTS WATCH*, 1-13.
29. Woodburn, N. (2016). NSA Surveillance and Interference with Citizens' Property Rights. *FAULKNER L. REV.*, 7, 287-299.



