Marcin Rojszczak*

THE ECTHR'S JUDGMENT IN THE CASE OF *CENTRUM FÖR RÄTTVISA V. SWEDEN* AS A LEADING CASE FOR THE REVIEW OF DOMESTIC REGULATIONS ON SIGNALS SURVEILLANCE

DOI: 10.26106/d460-w456

PWPM – Review of International, European and Comparative Law
vol. XVII A.D. MMXIX

ARTICLE

I. Introduction

The progressing digitalisation of life is providing incentives for the development of a society based on knowledge and information; however, at the same time, it is revealing new threats and risks. In recent years, the public's attention has been increasingly attracted to the issue of constantly expanded surveillance powers of public authorities. Although these powers should be beneficial for the protection of public security, in practice there is sufficient evidence that they are also useful for applications that are contrary to the principles of democracy, including social control. As Neil Richards rightly noted, the essence of surveillance is often not the acquisition of knowledge, but the control which makes it possible to influence the decisions of others.[1] Unfettered power of that kind in the hands of the government is a way to create an undemocratic system.

This problem has been even more relevant since the scale of surveillance programmes conducted by US and UK intelligence agencies was revealed. Suffice to say, the UK signals intelligence service, the Government Communications Headquarters (GCHQ), is suspected of not only tapping a considerable portion of electronic communications transmitted through the territory of the United Kingdom (and therefore also from users from other EU countries),[2] but also of the interception of

* Ph.D. in Law; assistant professor at Warsaw University of Technology, Faculty of Administration and Social Sciences. ORCID: 0000-0003-2037-4301, e-mail: marcin.rojszczak@gmail.com.

[1] N. Richards, *The Dangers of Surveillance*, Harvard Law Review 2013, vol. 126, p. 1949.

[2] M. Rojszczak, *UK Electronic Surveillance Programmes in the Context of the Protection of EU Citizens' Rights After Brexit*, PWPM 2018, vol. XVI.

communications transmitted between Google and Yahoo data centres (the MUSCULAR programme)[3] or of bulk interception of images from webcams, without the users' knowledge and consent (the OPTIC NERVE programme).[4] The scale of surveillance activities, along with the lack of sufficient oversight mechanisms (*checks and balances*) making it possible to challenge the legality of these activities before national courts, was the reason for the initiation of a number of court cases at the European Courts: the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU).

It should be stressed that EU treaties contain an important limitation on the applicability of their provisions to intelligence activities of states. Pursuant to Article 4(2) of the TEU, "national security remains the sole responsibility of each Member State." This provision significantly limits the possibility of applying EU law to assess the legality of bulk surveillance programmes.[5] Although the CJEU has expressed its opinion on the incompatibility of the general data retention obligation with the provisions of the Charter of Fundamental Rights (CFR),[6] there is no doubt that the explicit assessment of intelligence services' activities remains outside the scope of the authority of the EU Courts. The legal obligation to retain data (data retention) refers solely to the data collection phase and it does not pertain to the powers of the security services themselves and, consequently, to the phase of the processing, analysis and further reporting of information (e.g. transferring it to foreign intelligence services). Hence, EU law may be regarded only as complementary in assessing the legality of the activities of states in respect of untargeted surveillance programmes.

The above restriction is not to be found in the ECHR, which, stipulating the protection of individuals' rights, does not set forth any exceptions to its application in the field of national security. The Convention could therefore be the basis of obtaining international protection against unauthorised state interference also in the case of bulk surveillance programmes.

The European Court of Human Rights has evaluated domestic surveillance programmes on numerous occasions and its subsequent rulings have contributed to the development of the Court's own standard in this field. Consequently, for many years, the Court upheld the interpretation that the provisions of the Convention were an obstacle for use of bulk surveillance measures by public authorities.

In the judgment of 19 June 2018 handed down in the case *Centrum för Rättvisa v Sweden* (hereinafter referred to as CfR), the ECtHR once again dealt with the analysis of domestic surveillance provisions and ruled that the Swedish legislation

---

[3] *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post, 30.10.2013, http://cli.re/g1kRDd.

[4] *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*, The Guardian, 28.02.2014, http://cli.re/Lmrj8p.

[5] *National programmes for mass surveillance of personal data In EU Member States and their compatibility with EU law*, European Parliament 2013, http://cli.re/6EWad5, p. 28.

[6] The Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, 389–405; hereinafter referred to as 'the Charter' and 'CFR'.

implementing signals surveillance mechanisms contains sufficient legal safeguards and, consequently, does not lead to a violation of the Convention.[7]

The CfR case necessitates a reassessment of whether and to what extent the use of mass surveillance may be reconciled with the provisions of the Convention. If the very fact of applying this measure does not *per se* lead to a violation of the Treaty, the question remains as to whether such an inference proves the Court's departure from its previous jurisprudence or, perhaps, it demonstrates evolution of its case-law triggered by arguments of the supporters of strengthening the state's powers in the field of national security.

This paper provides a detailed discussion of the judgment and its practical consequences, in particular for the assessment of the compatibility of other domestic provisions with the Convention. Moreover, it also highlights and delves into potential discrepancies between the existing case-law of the CJEU and the theses contained in the ECtHR's judgment in CfR.

II. Basic concepts and terminology

Due to the technical complexity and diversity of legal systems, the discussion of the topic of signals surveillance should be started from defining the most significant terms and concepts. Otherwise, without the analysis of whether these terms are not defined differently by particular legislatures, the comparative analysis of legal systems might be inconsistent and incomplete.

Signals surveillance is usually defined as obtaining, collecting, processing and reporting information from electronic communication channels. Such surveillance may be *targeted* or *untargeted*. Untargeted surveillance is also defined as *bulk* or *indiscriminate*. The purpose of targeted surveillance is to obtain information about a designated individual or group of individuals, usually associated with a given criminal event. In turn, untargeted surveillance is related to preventive measures and is aimed at forecasting the events and individuals that, given the existing correlations, may be of interest to law enforcement agencies. Untargeted surveillance may lead to the application of further operational techniques aimed at specific individuals and, therefore, be an introduction to the use of targeted surveillance measures. Hence, untargeted surveillance is often associated with the processing of metadata, whereas targeted surveillance is connected with collecting and processing the whole message (the content of data transmission). This distinction is crucial in most legal systems. While modern constitutional provisions and applicable international legal acts define measures for the protection of the secrecy of correspondence (within this meaning, also the messages exchanged through electronic communications), the issue of the limits of the protection of metadata under the same provisions is discussed in the jurisprudence.[8]

[7] The judgment of the ECtHR of 19.07.2018 in the case of *Centrum för Rättvisa v Sweden*, application no. 35252/08. As of 13.05.2019 the judgment is not final – it was referred on 4.02.2019 to the Grand Chamber.

[8] Although in the EU data protection model it is commonly accepted to provide metadata with an equivalent level of protection to the content of the message, the situation in other legal systems

Frequent misunderstandings arise as to the use of the term *mass surveillance*. It is used to define different types of activities, often related to targeted surveillance programmes. As pointed out by the Venice Commission, the adjective "mass" can indicate a wide range of surveillance activities, not infrequently affecting the whole population or a large part of it.[9] The purpose of applying this type of techniques is also important: in discussions related to the measures of social control, mass surveillance should be connected with the activities of undemocratic states. On this basis, David Anderson makes a distinction between the terms '*mass surveillance*' and '*bulk surveillance*', stressing that not every programme of bulk data collection can be regarded as mass surveillance.[10]

Programmes based on the bulk collection of metadata are usually associated with the activities of intelligence services and referred to as *signals intelligence* (SIGINT), while targeted surveillance measures are perceived as related to the activities of the police and law enforcement agencies. Because of this, the first type of surveillance activities is also sometimes referred to as *'strategic monitoring'*, especially in the case-law of the ECtHR.[11] This term is supposed to express the relationship between surveillance measures and the protection of fundamental interests of the state, such as its defence and national security.

In practice, due to the scale of the interference with the right to privacy, the most significant are bulk programmes which are based on the interception of enormous amounts of data. Thus, they often belong to the sphere of activity of intelligence services, which, in turn, are not governed by criminal procedure and the method of oversight over their functioning depends on the statutory provisions applicable in a given legal system. For many years, the lack of transparency of security services' actions has continued to be an obstacle to the effective assessment of the scale of signals surveillance programmes and their actual impact on fundamental rights, including the rights to privacy, information and freedom of expression.

---

may be different. For example, in the United States, according to a commonly accepted view, the Fourth Amendment to the US Constitution, which is the source of the right to privacy, does not include metadata. *See*: J. Mornin, *NSA Metadata Collection and the Fourth Amendment*, Berkeley Technology Law Journal 2014, vol. 29, pp. 985–1006. It should be noted that the US legal doctrine is being changed and according to a recent judgment of the US Supreme Court, mobile phone location information is protected by the Fourth Amendment (see *Carpenter v United States* ruling, 585 U.S. 2018). More information on the practical meaning of metadata as a source of information about individuals in: *NSA Collected 534 Million Call Records Metadata In 2017: 3 Times Increase From 2016*, Fossbytes 5.05.2018, http://cli.re/GyZowd; *'We Kill People Based on Metadata'*, NYR Daily 10.05.2014, http://cli.re/gXd19J.

[9] *Report on the democratic oversight of signals intelligence agencies*, European Commission for Democracy through Law 2015, CDL-AD(2015)011, http://cli.re/LAvWog, para 56.

[10] David Anderson Q.C., *Report Of The Bulk Powers Review*, The Crown 2016, http://cli.re/g4dnp4, p. 4.

[11] *See*: the decision of the ECtHR of 29.06.2006 in the case of *Weber and Saravia v Germany*, application no. 54934/00.

III. ECtHR jurisprudence

The European Court of Human Rights has heard cases instituted by individual complaints against domestic surveillance programmes on several occasions. Although not all of them pertained to untargeted surveillance, an analysis of the cases which involved electronic tapping measures may be useful for gaining insight into the standard developed in the Court's jurisprudence. Indeed, the Court itself pointed out that it "does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other".[12]

In *Klass and others v Germany,*[13] the Court held that, under certain conditions, individuals may complain against the violation of their rights guaranteed by the Convention as a result of the application of domestic provisions introducing secret surveillance techniques, even if they have failed to demonstrate that they were subject to such surveillance. In this regard, the Court found that limiting the application of the Convention may not be accepted only for the reason that the individuals concerned are unaware of the limitation of their rights.

In turn, in the ruling in the case of *Weber and Saravia v Germany*, the Court held that the term "except such as is in accordance with the law" used in Article 8(2) of the ECHR means that the recognition of an exception to the prohibition of interference with the right to privacy must not only follow from domestic law, but it also has to be compliant with the principle of the rule of law. For this reason, domestic legislation must be accessible to the individual and ensure *foreseeability*. The Court understands this concept as an individual's capability to determine what activities and in what circumstances may entail the application of surveillance measures.[14] Hence, foreseeability expresses protection against arbitrariness both on the part of state security agencies and oversight authorities. In addition, in light of the principle of the rule of law, oversight over the activities of authorised bodies exercising their powers related to surveillance must be legally grounded and may not be fully discretionary.[15]

In turn, in the case of *Kennedy v the UK*, the Court ruled that there was no violation of the Convention by the reviewed surveillance provisions i.a. due to the lack of legal possibilities of applying bulk and unlimited data interception.[16] This thesis deserves special emphasis since, *a contrario*, it can be concluded that the opposite activity, that is unlimited surveillance, would lead to a violation of the guarantees arising from the Convention.

---

[12] *Liberty and others v United Kingdom*, para. 63.

[13] The judgment of the ECtHR of 6.09.1978 in the case of *Klass and others v Germany*, 5029/71.

[14] *See*, the judgment of the ECtHR of 1.07.2008 in the case of *Liberty v the United Kingdom*, application no. 58243/00, para. 62.

[15] *Weber and Saravia v Germany*, paras. 92–94.

[16] The judgment of the ECtHR of 18.05.2010 in the case of *Kennedy v United Kingdom*, 26839/05, para 160.

In its prior jurisprudence, the Court also listed minimum legal safeguards which should be included in national laws on secret surveillance in order to prevent abuse of power. In particular, the application of surveillance techniques should be limited in terms of:

- the categories of crimes which may entail the authorisation of the application of surveillance measures;
- the categories of individuals who may be subjected to surveillance;
- a time limit on the application of the measures;
- a procedure governing the analysis, storage and use of collected data;
- precautions applied when providing collected data to third parties;
- the criteria by which collected data should be deleted or destroyed.[17]

The abovementioned test was used on numerous occasions in subsequent cases heard by the Court, including the recent rulings in *Zakharov v Russia* and *Szabo and Vissy v Hungary*, where domestic laws were deemed to violate the standard of protection arising from the Convention.

The Court also specified how to interpret exceptions "necessary in a democratic society", a term introduced in Article 8(2) of the ECHR. In particular, the considerations concerning the balance between the importance of norms governing public security and the right to privacy are interesting in this regard. The Court highlighted the principle of proportionality expressed by striking a balance between the requirements of the public interest and the interests of an individual or individuals affected by surveillance measures. Here, the domestic legislature has considerable discretion as to the choice of the means to achieve this goal. However, the Court stressed that the implementation of secret surveillance programmes justified by national security purposes carries the risk of weakening or even destroying the principles of democracy. For this reason, legal measures aimed at eliminating the risk of the abuse of power should play a significant role in assessing the proportionality of the measure taken.[18]

The above considerations in *Zakharov v Russia* led the Court to point out that Russia's enactment of an obligation enabling authorised bodies to record transmissions in telecommunication networks with regard to all users, without the possibility of tracking what data has been intercepted and by whom, prevents the implementation of effective control and oversight mechanisms that could limit the risk of abuse of power.

The latest Court rulings in the field of surveillance laws include the case of *Szabo and Vissy v Hungary,*[19] which was instituted following a complaint by two Hungarian citizens against domestic provisions granting broad powers to the anti-terrorist police service. These powers, according to the applicants, resulted in a violation of their right to privacy. In the reviewed case, the Court elaborated on its previous considerations as to the definition of necessity and introduced the term '*strict necessity*', which

[17] *Weber and Saravia v Germany*, para. 95.

[18] The judgment of the ECtHR of 4.12.2015 in the case of *Zakharov v Russia*, 7143/06, para. 232.

[19] The judgment of the ECtHR of 12.01.2016 in the case of *Szabo and Vissy v Hungary*, 37138/14.

was to be applied to cases involving the surveillance of citizens by the state.[20] Strict necessity should be understood as the fulfilment of two conditions: firstly, the necessity of applying a given measure in order to protect democratic institutions of the state (the narrower understanding invoked in previous ECtHR rulings), and secondly, the necessity of applying the measure in a particular case due to the need to obtain important data concerning the individuals subjected to surveillance. As a result, the Court emphasised that recognising an exception to the rule of non-interference of public authorities with the right to privacy as "*necessary in a democratic society*" (Article 8 (2) of the ECHR) should not only relate to the protection of the interests of society as a whole, but it must also be justified by the actual need to obtain information from specific individuals subjected to surveillance.

Furthermore, in *Szabo and Vissy v Hungary*, the Court noted that the time of the application of surveillance techniques must be limited and it is inadmissible to extend the consent for such measures without due judicial oversight. The Court also elaborated on its previous considerations on the executive's oversight, noting that consent for the use of surveillance techniques granted at the political level of the executive does not ensure safeguards against abuse of power.[21]

The analysis of the case-law developed by the Court to date indicates the growing importance of necessity and proportionality as conditions indispensable for determining the justifiability of the limitations of the right to privacy resulting from surveillance carried out by the state.

Since surveillance programmes based on the bulk collection of personal data do not meet these conditions by definition, it seemed obvious that they could not be considered as acceptable within the meaning of Article 8(2) of the ECHR. However, in none of the cases discussed did the Court explicitly deny the possibility of applying measures related to mass data interception. Instead, the Court carried out an analysis of domestic legislation, highlighting insufficient safeguards implemented to prevent arbitrary decisions of politicians or authorised bodies as well as to a lack of effective remedies available to citizens whose rights have been violated.

In addition to the above analysis of the existing case-law, it should be noted that the Court has not always found the analysed provisions to be incompatible with the Convention. It did not do so in *Kennedy v the UK* – however, as previously stated, in this case the Court ruled that UK law did not allow for bulk surveillance. In turn, in *Weber and Saravia v Germany*, the Court accepted the possibility of untargeted surveillance activities carried out by the intelligence services in which telephone communication of a particular type could be tapped. This case led to the formation of the concept of "strategic monitoring".[22]

---

[20] *Szabo and Vissy v Hungary*, para. 73.

[21] *Szabo and Vissy v Hungary*, para. 77.

[22] However, it should be noted that the legality of the electronic surveillance activities carried out by the German intelligence services is being questioned – *see, e.g.*, C. Schaller, *Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden*, German Law Journal 2018, vol. 19, pp. 941–980.

IV. The *Centrum för Rättvisa* case

Centrum för Rättvisa is a non-governmental organisation dedicated to the promotion and protection of human rights. In pursuance of the objectives defined in its charter, the organisation filed a complaint with the ECtHR against the Swedish domestic legislation allowing, in its opinion, for the conduct of secret surveillance programmes in violation of Article 8(2) of the ECHR. In its complaint, Centrum challenged the powers associated with conducting programmes which were untargeted and unrelated to fighting against crime. Therefore, the scope of the complaint encompassed strictly intelligence competences related to the areas of state security. Bearing in mind the previous considerations about the European Courts' competences, Centrum's complaint was aimed at assessing the legality of provisions which could not be subject to the CJEU's review. Therefore, the presented considerations primarily concern the area of strategic monitoring rather than measures applied by the police services.

The subject matter of the CfR application concerned, in particular, the powers granted to the National Defence Radio Establishment (Försvaretsradioanstalt, FRA). It is a specialised service designed for signals intelligence, operating within the structures of the Ministry of Defence. The mode of its operation is subject to a range of regulations, the most important of which are the Act of 30 March 2000 on Foreign Intelligence,[23] the Act of 10 July 2008 on Signals Intelligence[24] and the Regulation of the Minister of Defence of 20 November 2000 on Signals Intelligence.[25]

The scope of the application of the Act on Foreign Intelligence indicates that intelligence actions may be carried out in the territory of the country only if they are related to activities outside its borders. The direction of activities undertaken as part of foreign intelligence is defined by the government in general and detailed guidelines. Activities carried out under the Act may not pertain to criminal proceedings or actions related to the detection and prevention of crimes, to which the police services are authorised.

The scope of application of the Act on Signals Intelligence is specified in Article 1, which contains an exhaustive list of items that justify the use of electronic surveillance measures. All of them are directly related to international relations. For the avoidance of doubt, the legislature additionally elaborated on particular objectives and indicated the rules of their interpretation in the explanatory statement to the bill.[26] Moreover, the FRA may carry out signals surveillance activities "in order to monitor changes related to international communications, technological development and technologies connected with the protection of communications" (Article 1(3) of

[23] Lag (2000:130) om försvarsunderrättelseverksamhet, SFS 2014:687, http://cli.re/Lyq5NQ.

[24] Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet, SFS 2016:558, http://cli.re/LozYbe.

[25] Förordning (2008:923) om signalspaning i försvarsunderrättelseverksamhet, SFS 2009:972, http://cli.re/LqBJwm.

[26] Regeringens proposition: Förstärkt integritetsskydd vid signalspaning, 2008/09:201, 20.05.2009, http://cli.re/gA4wWm, pp. 108–109.

the Act). These actions are defined as '*auxiliary operations*', while actions related to Article 1(1) are referred to as '*defence intelligence operations*'. Mark Klamberg proves that the interception of the content of electronic communication is carried out by the FRA as part of defence intelligence operations, whereas metadata are gathered as part of auxiliary operations.[27] The FRA is the only agency authorised to undertake surveillance activities under the Act.

The Court noticed that the Act on Signals Surveillance contains an exhaustive list of purposes which justify the conduct of surveillance. At the same time, all of them meet the criterion defined in Article 8(2) of the ECHR. But more importantly, the purposes of surveillance laid down in the Act were specified in further documents presented during the legislative process.[28] In earlier cases, the lack of an exhaustive list of these purposes or the enactment of provisions which were too general and subject to broad interpretation were highlighted by the ECtHR as a proof of the incompatibility of the analysed laws with the Convention.[29]

As previously indicated, additional criteria taken into account by the Court when assessing the minimum legal safeguards for signals surveillance programmes include: (i) the time limit for the application of such measures, (ii) the presence of a detailed procedure specifying the rules of intercepting, processing and reporting data as well as (iii) precautions taken in the transfer of collected data to third parties. Each of the above safeguards is elaborated on in the statutory provisions governing the operation of the FRA.

The Act provides a detailed scope of the powers related to collecting data from electronic communications. First and foremost, it should be noted that, in accordance with Article 2a, it is prohibited to intercept domestic communications, namely such communications in which its parties are located in the territory of Sweden. The FRA is entitled to exercise its powers by tapping radio and wired communication. The interception of wired communication may pertain solely to international fibre-optic cables (Article 2) and must be effected with the use of search terms (Article 3). Hence, the Act does not allow for bulk data collection without the application of pre-selection. A number of experts stress that the use of pre-selection makes it impossible to deem a programme to be untargeted.[30] However, it must be noted that this

---

[27] M. Klamberg, *FRA and the European Convention on Human Rights – A Paradigm Shift in Swedish Electronic Surveillance Law* [in:] Dag Wiese Schartaum (ed.), *Overvĺking i en rettstat in the series Nordisk* Írbok *i rettsinformatikk*, Bergen 2010, p. 118.

[28] *Centrum för Rättvisa v Sweden*, para. 120.

[29] *Zakharov v Russia*, para. 302.

[30] It is a solution similar to the one used in the GCHQ's activities. The use of pre-selection (initial data filtering) was also indicated in the report of the British Parliamentary Committee on Intelligence and Security as proving that the GCHQ's activities cannot be referred to as non-targeted surveillance. *See*, *Privacy and Security: A modern and transparent legal framework*, Intelligence and Security Committee of Parliament 2015, p. 112. It is worth noting, however, that in the same report its authors indicate that the reason for applying initial filtering by the GCHQ is not only related to the fulfilment of legal requirements, but also to technical limitations and the lack of resources to process all data (ibid., p. 111). Preselection in the UK intelligence services' activities is achieved both by searching through the content of messages and filtering the content by data

opinion is controversial: the decision to use pre-selectors often results from technical conditions (the inability to collect all of the available data), and whether their use contributes to the actual limitation of intercepted information depends on the quality of the search criteria applied, not their mere application. Furthermore, the Swedish legislature stipulated that the application of search terms that point to a specific natural person is permissible only in cases of special importance (Article 3 of the Act).

The FRA's activities are undertaken upon consent granted by the Court for Foreign Intelligence (Försvarsunderrättelsedomstolen), which is one of the independent oversight authorities ensuring the legality of signals surveillance programmes. The Intelligence Court verifies the compliance of the application of surveillance measures with limitations arising from law and also ensures compliance with the principle of necessity, which states that surveillance activities may only be undertaken if the necessary information cannot be obtained in a less invasive way. Moreover, the Intelligence Court verifies compatibility with the rule of proportionality, namely whether the benefit brought by operational activities to the protected values (usually national security) significantly prevails over the restrictions of the fundamental rights of individuals subjected to surveillance. As a result, the Swedish legislature has adhered to the existing case-law of the ECtHR associated with the introduction of the 'strict necessity' principle, under which surveillance may be applied solely if it is indispensable in a given situation.

Granting consent for the conduct of these activities, the Intelligence Court passes an order in which it indicates the electronic communications means that can be monitored, the pre-selectors to be applied and the duration of tapping, which may not exceed six months (Article 5a of the Act).

In addition to determining the maximum duration of surveillance activities, the provisions of the Act state that if it is necessary to extend this period, the Intelligence Court must repeat full proceedings in order to re-assess the fulfilment of all formal conditions for the application of surveillance. Not only does this solution make intelligence activities dependent upon prior authorisation granted by the Intelligence Court, but it also reduces the risk of automatism in the form of repeated extension of the timeframe of these activities. In its case-law, the ECtHR has emphasised that overly excessive powers on the part of the judiciary may also increase the risk of the abuse of power.[31]

While the special court established in the Swedish legal system to oversee signals intelligence activities may resemble institutions that exist in other jurisdictions (for

quality (e.g. rejecting data sent via P2P protocols). However it limits the amount of data collected, the use of the latter type of filtering is not motivated by the attention to the privacy of monitored users, but mainly by limited technical resources held by the intelligence agency. In turn, in the case of Sweden, the legislature explicitly introduced a pre-selection requirement based on predefined terms. Regardless of the possibility of using data filtering according to other criteria, the FRA must target its surveillance activities using the search terms approved by the court.

[31] *Zakharov v Russia*, paras 257–267.

example, the IPT[32] in the United Kingdom or the FISC[33] in the United States), the actual scope of powers and the method of their exercise is substantially different. As opposed to the FISC, the Swedish Court may not grant blank consent applicable to an undefined group of individuals and for an indefinite term. The detailed requirements that must be met to grant authorisation for surveillance techniques, in particular, mandatory consideration of the principles of proportionality and necessity, positions the Swedish Court in the role of an authority limiting the application of the FRA's powers.

It should also be noted that the FRA does not have the power to maintain interfaces with communications networks itself. Pursuant to Article 19a of Chapter VI of the Act on Electronic Communications (Lagen om elektronisk kommunikation, LEK),[34] telecommunications system providers are obliged to grant access to international traffic exchange connections to the Inspectorate for Foreign Intelligence (Statens inspection för försvarsunderrättelseverksamheten, SIUN). The Inspectorate installs and manages tapping devices and gives the FRA access to the necessary infrastructure to the extent to which it follows from the order of the Court. The result is the limitation of the risk of abuse of power by ensuring that no authority has the autonomous capability to carry out large-scale signals surveillance (the SIUN oversees the access nodes, the FRA has the technical and analytical capacity). In addition, the SIUN exercises formal oversight over the activities of the FRA. It should also be noted that this measure differs from the ones used in most other countries, where the agency competent for signals intelligence installs devices that provide access to data on its own.

In the Swedish model, additional oversight functions are exercised by an advisory committee for privacy protection established within the FRA. Its members are appointed directly by the executive (Article 11 of the Act on Signals Intelligence). The tasks of the Committee include monitoring the use of the surveillance powers and reporting the identified inconsistencies to the management of the FRA and SIUN.

The Act on Signals Intelligence also contains a number of limitations related to the storage or further use of collected data. In the event of accidental interception of domestic communications, the data should be destroyed with no delay (Article 2a). In the event of the court authorisation being reversed, all the collected information for which there is no other basis for gathering must be deleted (Article 5b). In addition, irrespective of other limitations, the data collected must be destroyed with no delay if one of the following conditions is fulfilled: (i) the data are related to a particular natural person and there are no grounds for applying surveillance measures to them; (ii) the data are subject to legal protection under the provisions of the Constitution on a journalist's privilege; (iii) the data fall within the scope of an attorney-client privilege or (iv) the confessional privilege (Article 7).

---

[32] The Investigatory Powers Tribunal was established by Article 65 of the Regulation of Investigatory Powers Act, 2000 c. 23, http://cli.re/gVqQ2J.

[33] United States Foreign Intelligence Surveillance Court) was established by the Article 103 of the Foreign Intelligence Surveillance Act, 95 Stat. 1783, 50 U.S.C. §1803.

[34] Lag (2003:389) om elektronisk kommunikation, SFS 2018:366, http://cli.re/LvbZMJ.

Furthermore, Swedish law introduces limitations on the transfer of collected information to foreign partners. As a rule, such cooperation is possible only in case it is connected with the FRA's execution of tasks falling within the field of defence and international security. The government may issue an individual consent for data transfer to foreign services in a specific case where it is necessary for the FRA to carry out its tasks. Nevertheless, it is important that such cooperation may not be unilateral and must, therefore, bring benefits to the Swedish state.[35]

Although the ECtHR has stressed the admissibility of *ex post* oversight over the application of surveillance activities in the existing case-law, it has also pointed out that preliminary judicial review provides more reliable protection against arbitrariness.[36] In this respect, its absence may be compensated for by *ex-post* oversight, with the proviso that it is not carried out in a fragmentary and random manner.

The Act on Signals Intelligence contains a number of safeguards to ensure effective legal remedies for individuals subjected to surveillance. First of all, if the pre-selectors used concerned a particular natural person, the FRA is obliged to notify this person of the measures used within one month of the termination of its operational activities. The Act sets forth a catalogue of situations that allow for the limitation of this obligation, such as the need to preserve state secret or an exclusive connection of these activities with the area of international relations.

The law provides for the possibility of filing a complaint against the FRA's activities with the Inspectorate, which, after necessary verifications, provides information whether a given person was subjected to unlawful surveillance techniques. This means that the Inspectorate does not indicate whether a particular individual actually was under surveillance and what data were obtained, but only if they were subjected to unlawful surveillance. In other cases, the applicants receive a response in an identical form indicating that they were not subjected to surveillance or surveillance was conducted in accordance with the law ("neither confirm nor deny").[37] The Inspectorate's decisions are final, which means that the individual has no right to appeal. According to the available data, the SUIN carried out 4 inspections in individual cases in 2012, in 2013 – 62, in 2015 – 22, and in 2016 – 14.[38]

In addition, in accordance with the Act on Processing Personal Data in Connection with Surveillance Activities,[39] each person may request once a year that the FRA notify them whether the agency has been interested in their personal data (Article 1 of Chapter II of the Act). In its response, the FRA is obliged to indicate the fact of data processing, the source of obtaining the data, and the category of the recipients

[35] Article 6 of Regulation on Signals Intelligence (*supra* note 25).

[36] See, *Zakharow v Russia*, para. 249; *Szabó and Vissy v Hungary*, para. 77.

[37] Surveillance by intelligence services…, p. 120.

[38] The data for the years 2012–2013 cited after: *Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet*, Försvarsutskottets 2015, http://cli.re/gqNvYa, p. 6; the data for the years 2015–2016 cited after: *Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet*, Försvarsutskottets 2018, http://cli.re/GAazRj, p. 6.

[39] Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, SFS 2018:52, http://cli.re/LRwjD1.

of the information. Nonetheless, this right is subject to limitation in the event that the requested information is classified (Article 3 of Chapter II). In a report on the activities of the FRA presented by a special parliamentary committee tasked with oversight over signals intelligence (Signalspaningskommittén), it was pointed out that this right is largely unenforceable due to the widespread use of secrecy clauses by the agency.[40]

Oversight over the FRA is also exercised by a number of other independent authorities, such as the Ombudsman (Justititeombudsmannen), Personal Data Protection Office (Datainspektionen, DPA) and the parliamentary Committee for Defence (Försvarsutskottets). The competences of some of these bodies are limited and do not allow them to attend to individual cases. Therefore, the report on secret surveillance programmes in the Member States and their compatibility with EU law published in 2017 by the EU Agency for Fundamental Rights indicated only the SUIN and DPA as non-judicial authorities protecting the rights of individuals.[41]

The establishment of the SIUN as an oversight authority and making the possibility of conducting signals surveillance dependent on the cooperation of the SIUN and the FRA provided another safeguard and control mechanism. The Court emphasised the importance of the complaint procedure carried out by the Inspectorate, which allows for the protection of the rights of individuals subjected to surveillance. At the same time, however, the Court pointed out the areas to be further improved, e.g. the possibility of lodging appeals against the Inspectorate's decisions.[42] Irrespective of the above, interested parties may submit individual complaints to the DPA, which is also competent to assess their validity. In conclusion, the ECtHR highlighted that Swedish law provides for a number of judicial and administrative procedures which allow for the protection of individuals' rights against illegitimate surveillance.[43]

Summarising the detailed considerations, the ECtHR declared that the Swedish legislation governing the operation of the FRA is compatible with the provisions of the Convention.

V. Compliance of bulk surveillance with the ECHR after the CfR case

The fact that the Court deemed the activities of the FRA to be compatible with the Convention necessitates the assessment of whether the standard developed in the Court's prior jurisprudence is still relevant. According to some researchers, "the Swedish case manifests a serious deviation from the previous case-law".[44] Does this

[40] *Uppföljning av signalspaningslagen*, Signalspaningskommittén 2011, SOU 2011:13, http://cli.re/g92vzj, p. 18

[41] Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume II: field perspectives and legal update, European Union Agency for Fundamental Rights 2017, http://cli.re/gxwvJL, p. 112.

[42] *Centrum för Rättvisa v Sweden*, para. 173.

[43] *Centrum för Rättvisa v Sweden*, para. 178.

[44] D. Bychawska-Siniarska, *Masowa inwigilacja do pogodzenia z prawem do prywatności* [*Mass surveillance to reconcile with the right to privacy*], 19.06.2018, http://cli.re/G58Ze5.

really mean that the ECtHR pointed to the possibility of reconciling the operation of mass surveillance programmes with the provisions of the Convention?

A detailed analysis of the CfR ruling does not provide evidence that the Court has departed from the standard previously developed in its case-law. Indeed, the Court pointed out that states have a large margin of discretion with regard to the application of measures designed to ensure public security, especially in the field of protection against the most serious crimes. These measures include signals surveillance programmes based on bulk data interception.[45] However, this thesis is not new and was also referred to by the Court in its previous rulings.[46] At the same time, the protection of the rule of law and democracy requires the implementation of a number of safeguards against abuse of power, including the application of the principles of proportionality, data minimisation and strict necessity. In addition, the basis for the use of surveillance measures must be accurate and arise from statutory provisions, whereas oversight over the observance of these provisions has to be effective and efficient.

Therefore, while states may have the power to conduct mass surveillance as a rule, the way of exercising this power, in order to be compatible with the Convention, must not lead to large-scale data collection. As a result, referring to the terminological issues discussed above, it should be noted that although the FRA's powers allow for the conduct of very extensive surveillance activities, both the number and quality of safeguards incorporated into the process of managing and controlling the Agency lead to the fact that, actually, the activities of the FRA are more similar to targeted surveillance programmes.

Another interesting question which arises from the analysis of the CfR ruling is the lack of full consistency between the ECtHR and CJEU's approaches to the admissibility of the application of the general data retention obligation. The CJEU found that the enactment of this measure in domestic legislation leads to disproportionate interference with fundamental rights and, therefore, it is irreconcilable with the Charter of Fundamental Rights. As a result, on 8 March 2017, the Administrative Court of Appeal in Stockholm (Kammarrätteni Stockholm) ruled that the domestic provisions imposing the general data retention obligation were incompatible with EU law. Currently, there are works carried out in order to assess the rules on data retention and to determine the need for introducing ones which would be compatible with EU law. It is proposed that the drafted provisions enter into force on 1 January 2019.[47]

At the same time, the method of intercepting information by the FRA, which relies on the tapping of fibre-optic cables, may be used to attain a similar scale of collected data. As pointed out by the CJEU in the case of *Schrems*, where the Court was analysing the possibility of transferring personal data from the EU to the United States, "legislation is not limited to what is strictly necessary where it authorises, on

[45] *Centrum för Rättvisa v Sweden*, para. 179.

[46] *Weber and Saravia v Germany*, para. 106.

[47] See the final report discussing the current status and recommended legislative actions in the area of data retention: Rättssäkerhetsgarantier och hemliga tvĺngsmede: Slutbetänkande av Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvĺngsmedel, SOU 2018:61, http://cli.re/6YVZ3K.

a generalised basis, storage of all the personal data of all the individuals whose data has been transferred from the European Union without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail"[48] – and hence this legislation cannot be compatible with EU law. A similar assessment was presented in the CJEU's earlier rulings[49] and the case-law of the ECtHR. For instance, in the case *M.K. v France,* the ECtHR found that "the domestic law should notably ensure that such data [collected personal data] are relevant and not excessive in relation to the purposes for which they are stored, and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored".[50]

However, analysing the case of CfR, the Court came to the conclusion that enabling the FRA to intercept data for a period of 12 months does not lead to a violation of the right to privacy because stored information is "unprocessed".[51] In this regard, the Court found that the storage of this information is necessary to enable its manual analysis, and only this analysis may identify which information is actually needed, and which should be removed with no delay. This approach is an important novelty since it brings the ECtHR's standpoint closer to the one presented by US courts,[52] at the same time moving it away from the case-law of the CJEU. According to a view which is prevalent in the United States, a breach of privacy as a result of surveillance activities may not occur at the stage of data interception and it may not take place earlier than at the stage of data analysis (processing).[53] This viewpoint is neither shared by the ECtHR[54] nor by most representatives of European legal studies.[55] Its adoption

[48] The judgment of the CJEU of 6.10.2015 in the case of *Schrems*, C-362/14, para. 93.

[49] The judgment of the CJEU of 8.04.2014 in the case of *Digital RightsIreland*, C-293/12 and C-594/12, para. 62.

[50] The judgment of the ECtHR of 18.04.2013 in the case of *M.K. v France*, application no. 19522/09, para. 35.

[51] *Centrum för Rättvisa v Sweden*, para. 146.

[52] *See, e.g.*, the judgment of the US Supreme Court of 26.02.2013 in the case of *Amnesty v Clapper*, 568 U.S. 398 (2013). *Contra,* the reflections of Judge A. Davis related to the use of automatic scanning of private information by a public authority without legal safeguards, in particular without issuing a court order cited in *In Federal Appeals Court for Wikimedia v NSA: Here's How It Went*, ACLU 16.12.2016, http://cli.re/LqBPWg.

[53] *See, e.g.*, R. Posner, *Privacy, Surveillance, and Law*, University of Chicago Law Review 2008, vol. 75, pp. 253–254.

[54] *See* the judgment of the ECtHR of 16.02.2000, 27798/95, in which the Court decided that in order to determine the occurrence of an interference, it is enough that the public authority had access to data concerning the private life of an individual – it is irrelevant whether the data were further processed or used (see para 70).

[55] According to EU law, the very existence of national provisions establishing secret surveillance programmes is sufficient to establish interference. *See*, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, European Union Agency for Fundamental Rights 2017, p. 35.

could actually lead to any extension of the data interception period if only security services demonstrated that the data have not been subject to prior processing. This concept contradicts the thesis that interference with privacy occurs irrespective of whether someone monitors an individual's behaviour and it is enough that monitoring may take place.[56] Uncritical acceptance of the ECtHR's opinion could lead, in the extreme case, to the creation of a preventive system of registering all online activities of the whole population for the purposes of possible future criminal proceedings. The implementation of this idea would make the model of democracy known to us similar to a dystopia in which the way of expressing thoughts and views reflects the needs and expectations of those in power.

Obviously, the CfR ruling cannot be interpreted as making it possible to determine *a priori* that unlimited surveillance programmes are compatible with the Convention. At the same time, however, its wording suggests that if relevant legal safeguards are adopted, including compliance with the principles of strict necessity and proportionality, it is possible to reconcile the application of such a measure with the obligations arising from the protection of fundamental rights.

VI. Conclusions

The juxtaposition of the Swedish regulations with those applicable in other European countries demonstrates significant differences in the quality of the enacted legislation. Sweden has frequently amended its laws governing the operation of the FRA, adjusting them to recommendations issued by international institutions and the judgments of the European Courts. As a result, despite existing room for improvement, this country has introduced much more mature legal measures in the field of secret surveillance powers than those applicable in plenty of other legal systems, including other EU Member States.

The judgment in the case of CfR has been the first judgment in the last eight years in which the ECtHR did not challenge the conditions for conducting secret signals surveillance programmes while analysing domestic legislation.[57] As a result, this judgment should be considered a landmark decision for numerous reasons.

First, the Court declared the compatibility with the Convention of a secret signals surveillance programme carried out by state authorities, thus pointing to the Swedish

[56] In fact, this is a definition of the so-called *'chilling effect'* – a well-recognised and described phenomenon that is also related to the impact of public secret surveillance programmes on the privacy and freedom of expression of citizens. *See, e.g.*, J. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, Berkeley Technology Law Journal 2016, vol. 31; J. Penney, *Internet surveillance, regulation, and chilling effects online: a comparative case study*, Internet Policy Review 2017, vol. 6, http://cli.re/GQm9o1.

[57] The previous case of this type was *Kennedy v the United Kingdom* heard in 2010, where the Court analysed exclusively the provisions on the activity of police and security services. The provisions regulating the operation of the GCHQ (the UK equivalent of the FRA) were not subjected to review then and, therefore, the safeguards for untargeted surveillance programmes were not analysed.

legislation as a positive example for other legislatures. The analysis of the legal measures adopted in Sweden allows for assessing other legal systems and determining whether they contain equally effective safeguards.

Secondly, Sweden is an example of a state that has been amending its legislation for many years, thus strengthening the safeguards against the arbitrariness of and lack of oversight over the application of surveillance. In a 2013 report prepared for the European Parliament, Sweden was mentioned as a state suspected of mass surveillance programmes along with the United Kingdom and France.[58] In the CJEU's judgment of 2016 in the case *Tele2 Sverige AB*[59], Swedish legislation was subject to analysis and the Court ruled on the inadmissibility of the application of national provisions which set forth the general data retention obligation. The statutes analysed by the ECtHR in the CfR case had been amended and supplemented a number of times, also after the submission of the original complaint in 2008. Analysis of the Swedish legal measures can be helpful not only to determine the standard for evaluating statutory measures used in other countries, but also to follow the evolution of the Swedish legislation and understand the significance of particular procedural safeguards for the final decision of the Court.

Thirdly, the ruling in CfR may be invoked as an argument indicating that the development of surveillance programmes makes it necessary to introduce to the previously described division into untargeted and targeted surveillance a new, third type: '*pre-targeted surveillance'*. It would be characterised by the application of technical measures typical of untargeted surveillance (tapping fibre optic cables, processing large data sets) assisted with the use of safeguards related to targeted surveillance (mandatory use of pre-selectors, numerous legal and organisational safeguards). It seems that the identification of a new type of surveillance would not only help to understand the Court's current case-law correctly, but also to qualify programmes conducted by individual states according to their interference with fundamental rights.

In the source literature, the activities of the FRA, both in terms of technical capacity and the scale of programmes conducted, are often compared to the most advanced signals intelligence programmes carried out by the GCHQ and NSA. Nonetheless, while comparing the provisions on the functioning of the NSA to those governing the FRA, a significant difference is visible in the number and specificity of the legal safeguards established (*checks and balances*).

Therefore, it seems that the activities of the United States' NSA and UK's GCHQ should be qualified as untargeted surveillance, German and Swedish programmes – as pre-targeted surveillance, and the measures traditionally associated with criminal procedure – as targeted surveillance. The US and Swedish legislation are on opposite sides of balancing the importance of the protection of fundamental rights and national security. The UK legislation should be placed in the middle of this scale. This conclusion is corroborated by a recent ruling of the ECtHR, in which UK surveillance pro-

[58] National programmes for mass surveillance…, p. 7.

[59] The judgment of the CJEU in cases C-203/15 and C-698/15 (*Tele2 and SSHD*), 21.12.2016, ECLI:EU:C:2016:970.

visions were deemed to be partially incompatible with Article 8 of the Convention.[60] The case of the UK is especially interesting, not only because of the very extensive signals surveillance programmes carried out by the GCHQ and its close cooperation with the United States' NSA, but also due to similarities between the Swedish and British legislation in the field of bulk surveillance.

From the point of view of other countries in the region, the judgment in the case of CfR should be a clear incentive to the modernisation of their domestic surveillance legislation. The above thesis is particularly valid in light of the cases still processed by the Court in which French[61] and Polish[62] regulations are being examined. The analysis of the Swedish legal system, which has been successfully tested for compatibility with the ECHR standards, may substantially aid and facilitate the enhancement of the existing legal mechanisms with a view to striking a better balance between national security and the protection of fundamental rights.

However, the CfR ruling does not resolve all doubts related to the permissible scope and scale of surveillance activities carried out by state authorities. Notably, one of the reasons for the current public interest in mass surveillance was the disclosure of information about the secret cooperation between US intelligence services and their European partners. This issue, namely the permissible scope of intelligence cooperation in mass spying on the states' own citizens, has not been subjected to sufficient legal analysis in terms of the ECHR so far.[63]

The actual significance of the ECtHR's case-law, including the ruling in CfR, for the improvement of the EU model of privacy protection may be limited, taking into account the exclusion of the national security from the scope of EU law. The embodiment of the ideas of building a knowledge-based society and establishing the single digital market also requires unification of minimum safeguards applied by states in the field of signals surveillance. It is obvious that the single digital market created by states tapping one another's communications on a massive scale will not meet the expectations held by the EU institutions as well as the Member States themselves. Developing a positive standard of compatibility assessment, the ruling in CfR facilitates the pursuit of a supranational agreement on the limitation of mass surveillance activities. A greater problem seems to be the fact that currently none of the states suspected of carrying out extensive mass surveillance programmes appear to be interested in building such a consensus.

---

[60] In fact, one of the observations that led the Court to declare that the UK surveillance laws violate Article 8 of the Convention was the lack of oversight over the pre-selection process (*supra* note 31). The judgment of the ECtHR of 13.09.2018 in the case of *Big Brother and others v the United Kingdom*, applications no. 58170/13, 62322/14 and 24960/15, paras. 387–388.

[61] Application to the ECtHR no. 49526/15, case *Association confraternelle de la presse judiciaire v France*.

[62] Application to the ECtHR no. 25237/18, case *Bychawska-Siniarska v Poland.*

[63] The Court partly referred to this issue while analysing UK legislation in the case of *Big Brother Watch and others v the UK*; however, due to a specific legal situation (functioning in the so-called Five Eyes Agreement regime), this ruling does not dispel all doubts. In particular, it did not refer to the most significant problem, namely the transmission of data collected by the UK intelligence services to a third country.

SUMMARY

In recent years, public attention has been increasingly drawn to the problem of the constantly expanding surveillance powers of public authorities. Although these powers are intended to protect public security, there is a lot of evidence indicating their suitability for achieving non-legal purposes, such as social control. Unlimited control in the hands of government is a way to create an undemocratic state.

In the judgment of *Centrum för Rättvisa v. Sweden* (CfR), issued on 19 June 2018, the ECtHR again examined national surveillance laws, considering that the Swedish legislation introducing electronic surveillance mechanisms contained sufficient legal safeguards and, as a result, did not lead to a violation of the Convention. For the first time in almost 10 years, the ECtHR had found no violation of standards arising from the European Convention when examining national surveillance regulations.

The judgment in the CfR case leads to the need to reassess whether and to what extent the use of mass surveillance can be reconciled with the provisions of the Convention. However, the purpose of the article is not only to discuss the judgment in detail, but also to indicate practical consequences for assessing the compliance of national surveillance regulations with the Convention. In addition, it will be considered whether the interpretation of convention provisions in the CfR case indicates a departure of the Court from its previous case-law, or whether this case-law may evolve in a direction that takes into account arguments of the supporters of strengthening the state's powers in the field of national security.

STRESZCZENIE

WYROK ETPC W SPRAWIE *CENTRUM FÖR RÄTTVISA V. SWEDEN* JAKO WZORZEC KONTROLI KRAJOWYCH PRZEPISÓW W ZAKRESIE INWIGILACJI ELEKTRONICZNEJ

W ostatnich latach uwagę opinii publicznej coraz częściej zwraca problem stale rozbudowanych uprawnień inwigilacyjnych organów władzy publicznej. Chociaż uprawnienia te mają służyć ochronie bezpieczeństwa ogólnego, to w praktyce nie brakuje dowodów wskazujących na ich przydatność do realizacji celów pozaprawnych, takich jak kontrola społeczna. Nieograniczona kontrola w rękach władzy to droga to stworzenia systemu niedemokratycznego.

W wydanym 19 czerwca 2018 r. wyroku w sprawie *Centrum för Rättvisa (CfR) v. Szwecja*, ETPC ponownie zajął się analizą krajowych przepisów inwigilacyjnych, uznając, że szwedzkie prawodawstwo wprowadzające mechanizmy inwigilacji elektronicznej zawiera wystarczające zabezpieczenia prawne i w efekcie nie prowadzi do naruszenia postanowień Konwencji. Po raz pierwszy od niemal 10 lat ETPC, badając krajowe przepisy inwigilacyjne, nie stwierdził naruszenia norm wynikających z Europejskiej Konwencji.

Wyrok w sprawie CfR prowadzi do konieczności ponownej oceny, czy i w jakim zakresie stosowanie masowej inwigilacji można pogodzić z postanowieniami Konwencji. Celem artykułu jest jednak nie tylko szczegółowe omówienie wyroku, ale również wskazanie praktycznych konsekwencji dla oceny zgodności krajowych przepisów inwigilacyjnych z Konwencją. Ponadto rozważano, czy wykładnia przepisów konwencyjnych dokonana w sprawie CfR świadczy o odejściu Trybunału od wcześniejszego orzecznictwa, czy też może świadczyć o jego ewolucji w kierunku uwzględniającym argumenty zwolenników wzmocnienia uprawnień państwa w dziedzinie bezpieczeństwa narodowego.

Słowa kluczowe: inwigilacja elektroniczna, masowa inwigilacja, prawo do prywatności, retencja danych

Key words: electronic surveillance, mass surveillance, right to privacy, data retention