Filip Radoniewicz*

Strategic monitoring in the judicial decisions of the European Court of Human Rights

Abstract

The importance of the problem of surveillance carried out by state authorities, especially in recent years, in connection with the growing threat of terrorism is indisputable. State authorities sometimes take measures, which involve restricting human rights, especially the right to privacy, justifying them by the need to ensure security of both the state and its citizens. The objective of this article is to outline the standpoint of the European Court of Human Rights (under Article 8 of the European Convention on Human Rights) on the so-called strategic monitoring, i.e. mass interception of data transferred via telecommunications networks and their subsequent analysis with a view to acquiring specific information.

Key words: surveillance, wiretapping, right to privacy, metering, a chilling effect

* Filip Radoniewicz, Ph.D., Department of Cyber Security Law and New Technologies of the Institute of Law of the War Studies Academy in Warsaw, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

Introduction

The subject-matter of this article is the issue of strategic monitoring in the judicial decisions of the European Court of Human Rights. This term should be understood as activities, which do not consist of the surveillance of individuals in order to prevent crime, or surveillance exercised in connection with criminal proceedings, but which constitute a kind of „mass" interception of data transferred via telecommunications networks and their subsequent analysis, with a view to acquiring information to detect serious threats (such as terrorist attacks or particularly dangerous crimes) and, as a result, to prevent them. However, before properly discussing this issue, it seems advisable, as an introduction, to draw attention to some preliminary issues. It is necessary to at least give a brief overview of Article 8 of the European Convention on Human Rights, which protects the right to privacy, and of the most important judgements concerning „ordinary surveillance" (i.e. the surveillance of individuals by judicial authorities).

Article 8 of the European Convention on Human Rights

As noted above, Article 8 of the European Convention on Human Rights[1] is the provision protecting the right to privacy. It belongs among the so-called freedom provisions, the interpretation of which is governed by the following principles arising from the judicial decisions of the European Court of Human Rights (hereinafter „the Court"): 1) dynamic interpretation which results from treating the Convention as a „living instrument" taking into account social, economic and cultural transformations; 2) recognising that the Convention gives rise not only to certain „negative duties" of public authorities, but also to „positive duties" which involve taking measures by the state to enable the exercise of rights and freedoms which, in the case of the right to respect for private life, means the duty to effectively protect the privacy of an individual, even in relations with other individuals; 3) the so-called margin of appreciation, according to which the Convention sets certain standards, leaving the choice of how to implement them to the signatory states, the consequence being

1 Convention for the Protection of Human Rights and Fundamental Freedoms of the 4th of November 1950, Journal of Laws of 1993, no. 61, items 284–285 as amended, hereinafter „the ECHR" or „the Convention".

that the Court retains a „margin of appreciation" while deciding whether the provisions of the Convention are properly implemented. In other words, individual states enjoy a certain leeway in bringing these provisions into practice. The scope of that leeway depends on numerous factors (in some cases being quite broad while in others are virtually non-existent) and should be determined by reference to a specific case[2].

In accordance with Article 8 (1) of the Convention, everyone has the right to respect for his or her private and family life, home and correspondence. This is not an absolute right, as Article 8 also contains a restrictive clause. In accordance with Article 8 (2), there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In the judicial decisions of the European Court of Human Rights, the concept of correspondence refers to any form of direct communication between expressly identified persons, by means of writing and any form of information transmission using technical means, in particular phone calls and the exchange of information by electronic means of communication, e.g. e-mail or other network services[3]. Therefore, wiretapping understood in the broadest sense as any interception of information (data) during its provision (transfer, transmission) is considered a violation of Article 8 of the Convention[4].

In Klass and Others v. Germany (a judgement of the 6th of September 1978, complaint No. 5029/71) it was first necessary to resolve the problem of the petitioners not being able to prove that they were wiretapped by state

2 Cf. L. Garlicki, *Artykuł 8 [Prawo do poszanowania życia prywatnego i rodzinnego]* [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*, t. 1, *Komentarz do art. 1–18*, red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010, s. 30–32, 482. See also: M. Krzyżanowska-Mierzewska, *Zasady interpretacji Konwencji* [w:] *Europejska Konwencja Praw Człowieka. Poradnik praktyczny*, red. Ł. Bojarski, M. Krzyżanowska-Mierzewska, Warszawa 2011, s. 85–89; M.A. Nowicki, *Wokół konwencji europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, Warszawa 2017, s. 295–296.

3 See, for instance, the decision of the 13th of May 1982 in X. and Y. v. Belgium, complaint No. 8962/80, points 4 and 5, a decision of the 29th of June 2006 in Weber and Saravia v. Germany, complaint No. 54934/00, point 77, and in particular those discussed in detail in the latter part of the decision in: Class and others v. Germany, point 41, Malone v. the United Kingdom, point 64, Copland v. the United Kingdom, points 41 and 42; Liberty and others v. the United Kingdom, point 56.

4 Cf. L. Garlicki, op. cit., s. 542–543.

authorities (after all, surveillance is covert). It was concluded that although Article 25 of the Convention (now Article 34) concerning individual complaints does not entitle individuals to bring a case against legal acts *in abstracto* simply because, in their subjective opinion, a given act is contrary to the Convention, an individual can, under certain conditions, claim to be the victim of violation (of his or her rights) by the mere existence of a legal regulation permitting such covert measures[5]. The Court found that even the potential ability to take measures against citizens to inspect their phone calls and correspondence, arising from the mere existence of regulations making such inspections possible, adversely affects the freedom of communication. In consequence, the mere existence of such regulations constitutes a form of interference with the right to privacy. At the same time, the existence of appropriate legal solutions enabling covert inspection of correspondence, mail and telecommunications by state authorities appears indispensable in a modern democratic society in order to ensure national security and to prevent breaches of order or crime. However, in order for such interference not to constitute a violation of Article 8 of the Convention, the premises stipulated in Paragraph 2 must be satisfied. First of all, the interference must arise from an act of law, be necessary in a democratic society and serve one or several purposes envisaged in that provision. The Court noted that modern democratic states and societies are threatened by various sophisticated forms of espionage and terrorism. Judicial authorities are, therefore, sometimes forced to carry out covert inspections on persons suspected of such activities. The state has a certain leeway in this respect, but it is not unlimited in its choice of measures, given in particular that this can pose a threat to the democratic system. For this reason, the legislator should provide for appropriate mechanisms to counter possible abuses. An assessment of whether these are sufficient is relative in itself, as it depends on the circumstances surrounding the case, including the type, scope and duration of surveillance, the type of authorities deciding to use it, and the appropriate supervision over its course[6].

Supervision over surveillance should take place at all of its stages, at the moment it is ordered, during its course and after its termination. Ideally, this

5 M.A. Nowicki, *Europejski Trybunał Praw Człowieka. Orzecznictwo*, t. 2, *Prawo do życia i inne prawa*, Kraków 2002, s. 815.

6 Cf. A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 18 listopada 1977 r., seria A 28. Sprawa Klass i inni przeciwko Niemcom*, „Prokuratura i Prawo"1995, nr 9, s. 129–134.

should be conducted by a court, because, as the Court found, wherever there is a risk of abuse that may harm a democratic society, it is advisable to entrust supervisory powers to an independent and autonomous body, and courts are one of these[7].

With regard to one of the most significant issues raised by the petitioners, the problem of subsequently notifying a person about the fact that he/she has been subjected to surveillance, the Court agreed with the arguments put forward by the German Constitutional Tribunal that the subsequent notification of a person subjected to a given measure could jeopardise the purpose for which the surveillance had been carried out and could contribute to the disclosure of the *modus operandi* of the secret service, and even the identity of its agents. Furthermore, according to the Court, if the interference with the right to respect for private life and correspondence, resulting from the contested provisions, is justified in the light of Article 8 (2) of the Convention, the mere fact that the individual subjected to surveillance was not informed of this measure being applied cannot be in conflict with that provision, since surveillance is effective as a result of its application (cf. he decision in Weber and Saravia v. Germany)[8].

Another important judgement, which is worth mentioning at this point is the judgement passed in Malone v. the United Kingdom (dated the 2nd of August 1984, complaint No. 8691/79). The Court reiterated that the mere existence of the possibility of applying surveillance by the state constitutes an interference with the right to privacy. With a view to determining whether there had been a violation of Article 8 of the Convention, it thus proved necessary to assess if this interference, exercised by the state, with Malone's private life was justified, i.e. whether the premises stipulated in Article 8 (2) were satisfied. First, it was necessary to establish whether there were legal grounds for the surveillance. In its judgement in Silver and others v. the United Kingdom (dated the 25th of March 1983, complaints Nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75), the Court ruled that the idea of [being] „in accordance with the law" should be interpreted in line with the general principles formulated in The Sunday Times v. the United Kingdom (a judgement of the 26th of April 1979, complaint No. 6538/74), pursuant to the provision of Article 10 (2) of the Convention. Accordingly, the notion of the

7 M.A. Nowicki, *Europejski Trybunał…*, s. 816.

8 A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 18 listopada 1977 r., seria A 28. Sprawa Klass...*, s. 132–134.

„law" (the Polish translation of the Convention appears somehow misleading, it uses the term „act" while it would be more accurate to use „law") should be interpreted widely, in substantive and not only formal terms, as both codified and non-codified law. It would, therefore, include acts of a lower order than acts of law, acts of international and supranational law, as well as or above all common law[9]. The Court also stressed that regulations must meet the requirements of both „accessibility", the citizen must be able to obtain information on the legal provisions applicable under given circumstances, and „foresee-ability", the citizen must be able to foresee the consequences of given actions[10]. Transposing these considerations back to Article 8, a conclusion may be drawn that the provisions constituting the legal basis for undertaking surveillance measures by state authorities must be clearly and precisely formulated in such a way that citizens have no doubts under which circumstances the state would be entitled to interfere with their privacy. Obviously, this does not mean that individuals should be able to predict when the authorities may tap on them so that they could adjust their behaviour accordingly[11]. In Polish doctrine, this premise is reflected in the principle of definitiveness, under which a provision constituting the basis for interference must be formulated (or in case law established in judicature) so precisely that its addressee has no doubts as to the legal consequences of his/her behaviour under the circumstances specified therein[12].

The Court further stressed that the term „in accordance with the law" also imposes certain requirements as to the quality of that law. First of all, the regulations must comply with the principle of the rule of law referred to in the preamble to the Convention. This implies that there must be a means of legal protection in domestic law against random interference by state authorities, and the system of phone call inspections by law enforcement bodies should contain sufficient guarantees preventing any abuse[13].

9 Cf. L. Garlicki, op. cit., s. 485–486; M.A. Nowicki, *Europejski Trybunał…*, s. 828, 973; A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 2 sierpnia 1984 r., sygn. 4/1983/60/94. Sprawa Malone przeciwko Zjednoczonemu Królestwu*, cz. 2, „Prokuratura i Prawo" 1997, nr 5, s. 103.

10 Ibidem, s. 103.

11 M.A. Nowicki, *Europejski Trybunał...*, s. 835.

12 L. Garlicki, op. cit., s. 486–487.

13 A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 2 sierpnia 1984 r., sygn. 4/1983/60/94. Sprawa Malone przeciwko Zjednoczonemu Królestwu*, cz. 1, „Prokuratura i Prawo" 1997, nr 4, s. 136–137; idem, *Wyrok Europejskiego Trybunału Praw*

In addition, in the reference judgement, the Court dealt with the issue of the legal qualification of the so-called metering, of which Malone accused the authorities in his complaint. „Metering" consists of recording the calls made using a given telephone (the numbers selected, together with the date of making the telephone calls and their duration). This is a standard activity carried out by telecommunications service providers. It is not „metering" itself that constitutes interference with the right to privacy but the provision of information obtained in this manner, e.g. in the form of billing records, to the police without the subscriber's consent. This is due to the fact that, according to the Court, billing records constitute an integral part of a telephone conversation[14].

In Halford v. the United Kingdom (a judgement of the 25th of June 1997, complaint No. 20605/92), the Court sought to determine whether phone calls made from the workplace should enjoy as much protection as private ones.

The Court had already stated in an earlier judgement, in Niemietz v. Germany (a judgement of the 16th of December 1992, complaint No. 13710/88 that the right to respect for private life includes the right to establish and maintain contacts with other people. Therefore, the concept of „private life" (within the meaning of Article 8(1) of the Convention) also includes activities of a professional nature, as most people come into contact with the outside world in this field, too. Furthermore, it is not always possible to separate an individual's activities pursued within the professional sphere from those belonging to the private one[15].

In Kruslin v. France (a judgement of the 24th of April 1990, complaint No. 11801/85) and Huvig v. France (a judgement of the 24th of April 1990, complaint No. 11105/85), the Court determined the minimum standards, which the national statutory regulations on surveillance should meet in order to prevent abuses by state authorities. In this respect, it appears indispensable to: 1) define the categories of persons in respect of to whom wiretapping measures may be applied; 2) indicate offences the prosecution (or prevention) of which may justify the decision to use wiretapping; 3) determine the maximum duration

Człowieka w Strasburgu z dnia 2 sierpnia 1984 r., sygn. 4/1983/60/94. Sprawa Malone..., cz. 2, s. 103–104. Cf. M.A.Nowicki, *Europejski Trybunał...*, s. 828–829.

14 See A. Rzepliński, *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 2 sierpnia 1984 r., sygn. 4/1983/60/94. Sprawa Malone...*, cz. 2, s. 109–111.

15 Cf. A. Redelbach, *Prawa naturalne – prawa człowieka – wymiar sprawiedliwości: Polacy wobec Europejskiej Konwencji Praw Człowieka*, Toruń 2000, s. 242–243; M.A. Nowicki, *Europejski Trybunał...*, s. 852–853.

of wiretapping measures; 4) establish the relevant procedures for drawing up reports containing intercepted calls; 5) provide for precautions to be taken in connection with the transmission of the obtained materials in order to enable other entities (in particular, the court and defence lawyers) to become acquainted with them; 6) define the circumstances resulting in the destruction of collected materials (in particular, the acquittal of the accused)[16].

In the already mentioned judgement passed in Copland v. United Kingdom, the Court stressed that communication by both telephone and e-mail or the Internet, made from the workplace, is *per se* private and, being considered a form of correspondence, enjoys the protection arising from Article 8. In turn, billing records and comparable data compilations regarding communication by the Internet constitute integral parts of such communication, and their collection and storage (even with no purpose of their use at a later date) without the knowledge of the person concerned constitute interference with private life[17].

Strategic monitoring

The Court first addressed the issue of strategic monitoring in Liberty and other organisations v. the United Kingdom (a judgement of the 1st of July 2008, complaint No. 58243/00). As indicated above, these are activities involving „mass" interception of data transmitted over telecommunications networks and their subsequent analysis, in order to obtain information enabling the detection of serious threats (such as terrorist attacks or particularly dangerous crimes). Their purpose is to identify threats (of terrorist acts or serious crime) as early as possible and to prevent them. In the case under discussion, three civil liberties organisations: Liberty, British Irish Rights Watch and The Irish Council for Civil Rights, filed a complaint alleging that between 1990 and 1997 they had been subjected to surveillance by the ETF (Electronic Test Facility), a special unit of the British Ministry of Defence.

In its judgement passed in this case, the Court stressed that there was no basis for applying different rules regarding the accessibility and transparency

16 Ibidem, s. 862.

17 Cf. A. Lach, *Glosa do orzeczenia ETPCz w sprawie Copland przeciwko Zjednoczonemu Królestwu – 62617/00*, „Monitor Prawa Pracy" 2007, nr 7, Legalis/el; M.A. Nowicki, *Europejski Trybunał Praw Człowieka. Wybór orzeczeń 2007*, Warszawa 2008, s. 127–129.

of legal regulations in relation to the interception of individual communication and more general surveillance programmes (i.e. strategic monitoring, for example). In consequence, the situation was analysed in compliance with general principles, and the Court concluded that the British regulations did not provide sufficient protection against abuses by the state authorities as they failed to define the rules of surveillance in detail. More specifically, the procedure for selecting which of the intercepted data should be subject to analysis, and for determining their storage, further access and destruction, was of a covert nature, and thus the regulation failed to satisfy the requirement of „accessibility". For this reason, the interference with the right to privacy could not be considered lawful in the light of Article 8 (2) of the Convention.

In its judgement of the 4th of December 2015 in Zakharov v. Russia (complaint No. 47143/06), which concerned a system of secret surveillance of mobile phone calls used in Russia, the Court defined in further detail the conditions that must occur for the petitioner to be considered a victim of the breach of Article 8 without the need for him/her to prove that he/she had indeed been subjected to surveillance, due to the mere existence of a provision allowing covert surveillance measures. First, it needs to be shown that the petitioner either belongs to a group of persons to whom the rules allowing surveillance by the state authorities are intended to apply by definition, or the contested regulation offers such a possibility to all persons using telecommunications services, by creating a system intercepting all forms of communications by technical means, i.e. phone calls, e-mails, etc. (strategic monitoring). Secondly, it must be determined whether the national legal system contains a mechanism of preventing abuses, enabling the person being subjected to surveillance to institute a procedure to verify the legality of the surveillance measure imposed on him or her. However, if this mechanism is found to exist, the degree of its effectiveness must be assessed, as it is this level that determines the degree of inspection applied by the Court. As stressed in Kennedy v. the United Kingdom (a judgement of the 18th of May 2010, complaint No. 26839/05), in the absence of a system for verifying the legality of such measures, the petitioner does not have to prove that he/she was subjected to surveillance. However, if the law provides for ways to control the legality of its application, the petitioner must prove that, because of his/her personal situation, he/she is vulnerable to the state's actions entailing such measures.

In Szabó and Vissy v. Hungary (a judgement of the 12th of January 2016, complaint No. 37138/14), the Court investigated the provisions of the act, under which a special unit for combating terrorism was established and

was granted very broad powers. These included, *inter alia*, the right to apply surveillance measures, which could be carried out on the basis of an approval obtained from the court (if they were meant to be applied in the course of specific proceedings) or from the Minister of Justice (if they were intended to prevent terrorist acts or threats to national security).

In the judgement in question, the Court reiterated that, in view of the growing threat of terrorism, the governments of the Member States are resorting to the latest technological advances, including technologies enabling the mass monitoring of citizens' communications, in order to search for information, which may enable taking measures against terrorism, in the communication intercepted in this manner. That advancement in surveillance techniques should be accompanied by the increasing effectiveness of legal measures to counter the potential abuse on the part of law enforcement bodies. Furthermore, the Court once again stated that in cases involving surveillance, due to the scale of potential infringements with the right to privacy, the idea of „necessity in a democratic society" must be interpreted strictly, by investigating its two aspects in a general sense, that is to say, assessing whether the interference is necessary for the protection of democratic institutions, and in a specific sense, determining whether it is necessary in a given case[18].

In the most recent of the judgements discussed in this article, i.e. the one passed on the 13th of September 2018 in Big Brother Watch and others v. the United Kingdom (complaints Nos. 58170/13, 62322/14 and 24960/15), the Court, having examined the complaints, divided the problems they raised into three main issues: „mass" interception of communication, the exchange of data collected in this manner between the authorities of different states, and the acquisition of data from telecommunications service providers. Regarding the first issue, the Court again highlighted that the existence of strategic monitoring systems did not automatically constitute a violation of the Convention, their use being currently indispensable for the effective protection of national security. Regulations enabling the use of surveillance systems, however, must meet a number of standards, which also guarantee the protection of society from abuses on the part of the state authorities. Most of all, reliable and independent supervision must be exercised over the functioning of the system used for acquiring mass data regarding communication between individuals.

18 Cf. B. Grabowska-Moroz, A. Petryka, *Służby specjalne, policyjne i skarbowe a prawa człowieka – standardy konstytucyjne i międzynarodowe oraz kierunki niezbędnych zmian legislacyjnych*, Warszawa 2016, s. 32.

While the Court did not find that the British services abuse their powers, it pointed out some weaknesses of the applicable regulations, including in particular the lack of supervision over the data interception system, especially in terms of the selection of entities subjected to surveillance, and the criteria for filtering and selecting communication to be analysed, or the lack of any regulation concerning the interception of communications data.

Regarding the issue of the interception of data from communications service providers, the Court noted that this was only possible when combating „serious crime" was at stake, subject to prior review of the decision to do so by an independent authority (preferably the court). The British regulations binding at that time did not fulfil this requirement, as they allowed access to data for a general purpose of „combating crime" and did not provide for the review of the decision authorising it (except where it involved obtaining data relating to journalist's informants). In consequence, the Court found that Article 8 had been violated because the interference did not meet the criterion of lawfulness.

In analysing the last issue, the Court stated that the exchange of intercepted data between the authorities of different states did not violate the Convention, as the petitioners did not specify which authorities were to transfer the information obtained through surveillance between one another.

In its judgement, the Court also found that Article 10 of the Convention (freedom of expression) had been violated due to the lack of criteria for selecting entities subjected to secret inspection and protection of confidentiality of the intercepted information, which might have a chilling effect on the freedom of press given the fear of the communications exchanged by journalists and their informants being put under surveillance.

Summary

It is worth stressing that the Court, when dealing with cases involving the right to respect for private life, must touch upon two issues. First, the fact that technological progress has made interpersonal communication easier, on the one hand, and more susceptible to interference from the state authorities, on the other. Second, the growing threats to security of both the state and society, resulting from organised crime and terrorism. As a result, balancing the interests of society related to ensuring security, on the one hand, and the interests of individual people related to protecting their right to privacy, on the other, has

become a much more complex issue. The use of mass surveillance involving strategic monitoring is a form of preventing threats. The Court, however, in its judgements has assumed that there are no grounds for treating surveillance of individual people as different from the so-called strategic monitoring, or „mass surveillance", in the light of Article 8. This implies that it is permissible as long as the provisions enabling it do not violate Article 8 of the Convention, and thus meet numerous conditions arising from Paragraph 2 of the Article, the interference must be in accordance with the law (the term is understood broadly and is meant to include both codified law and case law, and the practice of its application), precise, accessible and foreseeable, as well as compliant with the rule of law. The law may provide for a possibility to exercise public surveillance only if necessary in a democratic society and only for the purposes indicated in Article 8 (2). At the same time, domestic law must contain clear principles of using surveillance involving technical means. In particular, it is imperative to: 1) define the categories of persons in respect of whom surveillance may be exercised; 2) indicate offences the prosecution (or prevention) of which may justify the decision to use it; 3) determine its maximum duration; 4) establish the relevant procedures for drawing up reports containing intercepted data; 5) provide for precautions to be taken in connection with the transmission of the intercepted data in order to allow other entities to become acquainted with them; 6) define the circumstances under which these data are to be destroyed; 7) the regulations should envisage that the person subjected to covert surveillance measures will be informed of this fact unless this jeopardises the purpose of the surveillance or entails the risk of, for example, revealing the informants' identity or the methods used by the authorities for interception.

These regulations must be compliant with the rule of law, and there must be a means of legal protection in domestic law against random interference by state authorities. There must be adequate guarantees to prevent any abuse; there must be a means of protection against arbitrary actions by the authorities. In particular, a system for supervising the use of surveillance measures, preferably carried out by the court, must be envisaged. Supervision over surveillance should take place at all its stages, at the moment it is ordered, during its course and after its termination. There may be a possibility not to inform the person subjected to surveillance of the fact that this measure has been applied if it is in the interest of the justice system.

Bibliography

Garlicki L., *Artykuł 8 [Prawo do poszanowania życia prywatnego i rodzinnego]* [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*, t. 1, *Komentarz do art. 1–18*, red. L. Garlicki, P. Hofmański, A. Wróbel, Warszawa 2010.

Grabowska-Moroz B., Petryka A., *Służby specjalne, policyjne i skarbowe a prawa człowieka – standardy konstytucyjne i międzynarodowe oraz kierunki niezbędnych zmian legislacyjnych*, Warszawa 2016.

Krzyżanowska-Mierzewska M., *Zasady interpretacji konwencji* [w:] *Europejska Konwencja Praw Człowieka. Poradnik praktyczny*, red. Ł. Bojarski, M. Krzyżanowska Mierzewska, Warszawa 2011.

Lach A., *Glosa do orzeczenia ETPCz w sprawie Copland przeciwko Zjednoczonemu Królestwu – 62617/00*, „Monitor Prawa Pracy" 2007, nr 7, Legalis/el.

Nowicki M.A., *Europejski Trybunał Praw Człowieka. Orzecznictwo*, t. 2, *Prawo do życia i inne prawa*, Kraków 2002.

Nowicki M.A., *Europejski Trybunał Praw Człowieka. Wybór orzeczeń 2007*, Warszawa 2008.

Nowicki M.A., *Wokół konwencji europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, Warszawa 2017.

Redelbach A., *Prawa naturalne – prawa człowieka – wymiar sprawiedliwości: Polacy wobec Europejskiej Konwencji Praw Człowieka*, Toruń 2000.

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 18 listopada 1977 r., seria A 28. Sprawa Klass i inni przeciwko Niemcom*, „Prokuratura i Prawo"1995, nr 9.

Rzepliński A., *Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 2 sierpnia 1984 r., sygn. 4/1983/60/94. Sprawa Malone przeciwko Zjednoczonemu Królestwu*, cz. 1–2, „Prokuratura i Prawo" 1997, nr 4–5.

Monitoring strategiczny w orzecznictwie Europejskiego Trybunału Praw Człowieka

Streszczenie

Doniosłość problematyki inwigilacji prowadzonej przez organy państwa – w szczególności w ostatnim czasie, w związku z narastającym zagrożeniem terroryzmem – nie podlega dyskusji. Władze państwowe, powołując się na konieczność zapewnienia bezpieczeństwa państwa i obywateli, nieraz podejmują działania wiążące się z ograniczaniem praw człowieka, w tym przede wszystkim prawa do prywatności. Niniejszy artykuł ma na celu prezentację stanowiska Europejskiego Trybunału Praw Człowieka (na gruncie art. 8 Europejskiej Konwencji Praw Człowieka) w kwestii tzw. monitoringu strategicznego, tj. masowym przechwytywaniu przesyłanych sieciami telekomunikacyjnymi danych, a następnie ich analizy w celu uzyskania konkretnych informacji.

Słowa kluczowe: inwigilacja, podsłuch, prawo do prywatności, metering, efekt mrożący