Privacy in the digital era – Polish electronic surveillance law declared partially unconstitutional

Judgment of the Constitutional Tribunal of Poland of 30 July 2014, K 23/11

Jan Podkowik*

Introduction

On 30 July 2014, the Polish Constitutional Tribunal delivered a long-awaited judgment[1] in which it assessed the compatibility of particular provisions of domestic law on covert electronic surveillance with the Constitution of the Republic of Poland (henceforth: the Constitution)[2] and the Convention for the Protection of Human Rights and Fundamental Freedoms (henceforth: the Convention). The case was heard after seven joint motions were filed in 2011 and 2012 by the Human Rights Defender (Ombudsman) and the Attorney General.[3]

The case discussed is not only significant because the judgment was passed by the Tribunal, sitting as a full bench and after almost three years of deliberations, but because it challenged provisions that concern fundamental issues relating to the protection of privacy in the digital era. Moreover, the Tribunal assessed

*Ph.D. Assistant Professor at the Faculty of Law and Administration, Jagiellonian University in Cracow (post-doctorate researcher in the project: 'Implications of constitutional adjudication on private-parties legal relationships'); law clerk in the Office of the Constitutional Tribunal of the Republic of Poland. Previously employed in the office of the Human Rights Defender and as an assistant professor at the National Defense University in Warsaw.

[1] The operative part of the judgment is published in Dziennik Ustaw [*Official Journal*] 2014, item 1055. An official English version of the ruling does not exist.

[2] The Constitution of the Republic of Poland of 2 April 1997, Dziennik Ustaw [*Official Journal*] 1997, no. 78, item 483.

[3] It is worth mentioning that the Attorney General and divisional prosecutors play a crucial role in the ordering of an operational control and also have the power to grant or refuse consent for an operational control.

European Constitutional Law Review, 11: 577–595, 2015

doi:10.1017/S1574019615000322

the constitutionality of surveillance law pertaining to almost all law enforcement and intelligence services, including civil and military counter-intelligence agencies.

The Tribunal held that some of the contested provisions authorising agencies to access telecommunication metadata were unconstitutional, as they violated the right to the protection of privacy (Article 47 of the Constitution) and the secrecy of communication (Article 49 of the Constitution). Procedural guarantees in the regulations were insufficient and therefore led to disproportionate interference with the fundamental rights affected (Article 31, paragraph 3 of the Constitution). Additionally, the Tribunal pointed to a lack of external supervision over the access to metadata by the services as well as unclear rules regarding the destruction of unnecessary or inadmissible materials. It must be emphasised that in the case discussed, domestic laws requiring service providers of publicly-available electronic communications services to retain traffic and localisation data were not subject to constitutional adjudication.

The legislation allowing police and intelligence agencies to obtain information and evidence by wiretapping, visual monitoring, tracking a target by satellite navigation, etc., during so-called operational control were also declared partially unconstitutional. These provisions did not sufficiently protect professional secrecy, especially that of lawyers, journalists or doctors. For this reason, they were declared inconsistent with, *inter alia,* the right to defence (Article 42 paragraph 2 of the Constitution) and freedom of expression (Article 54 paragraph 1). The Tribunal also found it unconstitutional (due to the insufficient quality of the law, which was unclear in its definitions and did not give citizens an adequate indication as to the circumstances and conditions upon which public authorities were empowered to engage in surveillance) for a regulation authorising the Internal Security Agency to pertain to operational control in order to prevent or detect crimes against the economic wellbeing of the state.

The Tribunal recognised some deficiencies in the legislation on operational control in order to prevent and detect offences envisaged by binding international agreements. It also noted that the statutes did not specify the type of technical measures utilised to secretly obtain information and evidence during operational control. The Tribunal, however, did not declare them unconstitutional, but made a so-called interpretative judgment. This means that such provisions are consistent with the Constitution on the condition that they are understood and applied in the way indicated in the judgment.

In accordance with Article 190, paragraph 3 of the Constitution, the Tribunal decided that unconstitutional provisions would lose their binding force 18 months after the day on which the judgment was published in the Dziennik Ustaw [*Official Journal*]. The legislature must amend or repeal provisions on surveillance

over this period in accordance with the requirements indicated in the judgment. The motive behind such a decision is to ensure that the activities of law enforcement agencies are not paralysed, a condition which might undermine the security of the state and its citizens.

This decision is undoubtedly an interesting voice in the European judicial dialogue on the protection of privacy in the digital era.[4] The Tribunal generally took a position congruent to the other constitutional courts in Europe,[5] the Strasbourg Court[6] and the Luxembourg Court.[7] It can be said that so far all these authorities – despite some differences in their individual reasoning and approach towards surveillance – agree on the subject. Targeted surveillance is admissible in a democratic state, but numerous procedural safeguards must be put in place and adhered to.

The aim of this study is to present the most important arguments of the Polish Constitutional Tribunal's judgment. This case note is organised as follows: First, the normative background of the challenged provisions is examined. Additionally, the political context of the motions and the decision itself, as well as an outline of previous Polish Tribunal surveillance legislation case law. Finally, the main reasoning of the Tribunal in the judgment of 30 July 2014 is presented and compared with the constitutional case law of other European courts.

[4] *See Report of the High Commissioner for Human Rights on the right to privacy in the digital age*, 30 June 2014; S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: an Element of Choice* (Springer Science & Business Media 2011); R.A. Grant and C.J. Bennett, *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press 1999).

[5] *See* judgment of the Bulgarian Supreme Administrative Court, No.13627, 11 December 2008; judgments of the Romanian Constitutional Court No. 1258, 8 October 2009 and 8 July 2014; judgment of the Federal Constitutional Court of Germany, 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08; judgment of the Czech Constitutional Court, 22 March 2011, Pl. ÚS 24/10; judgment of the Supreme Court of Cyprus, 1 February 2011, app. no.65/2009, 78/2009, 82/2009 & 15/2010-22/2010; judgment of Constitutional Court of Austria, 27 June 2014, G 47/2012; judgment of the Constitutional Court of the Republic of Slovenia, 3 July 2014, U-I-65/13-19.

[6] *See* e.g. ECtHR 6 September 1978, Case No. 5029/71, *Klass and Others* v *Germany*; ECtHR 2 August 1984, Case No. 8691/79, *Malone* v *The United Kingdom*; ECtHR 24 April 1990, Case No. 11801/85, *Kruslin* v *France*; ECtHR 25 September 2001, Case No. 44787/98, *P G and J H* v *The United Kingdom*; ECtHR 29 June 2006, Case No. 54934/00, *Weber and Saravia* v *Germany*; ECtHR 1 March 2007, Case No. 5935/02, *Heglas* v *Czech Republic*; ECtHR 28 June 2007, Case No. 62540/00, *Association for European Integration and Human Rights and Ekimdzhiev* v *Bulgaria*; ECtHR 10 February 2009, Case No. 25198/02, *Iordachi and Others* v *Moldova*; ECtHR 2 September 2010, Case No. 35623/05 *Uzun* v *Germany*; ECtHR 23 October 2012, Case No. 22373/04, *Hadzhiev* v *Bulgaria.*

[7] ECJ 8 April 2014, Case C-293/12, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.*

Normative background

The challenged provisions related to two forms of electronic surveillance conducted by law enforcement and intelligence services: operational control and access to retained metadata.

Operational control

Operational control is a form of so-called operational intelligence activity carried out by the Police, the Border Guard, the Treasury Intelligence Service, the Military Gendarmerie, the Military Counter-Intelligence Service, the Internal Security Agency and the Central Anti-Corruption Bureau.

The scope of the operational control is similar for all the bodies mentioned. Generally, such a form of surveillance is performed secretly and consists of reviewing the contents of correspondence, checking the contents of parcels and the use of technical measures which facilitate obtaining information and evidence in secret as well as the recording thereof, especially the contents of telephone conversations and other information submitted via telecom networks. The regulations allow wiretapping of persons and premises, including conversations conducted via landlines, wireless communications and websites, allowing the interception of text and multimedia messages or tracking the location of persons and objects using satellite navigation. The statutes do not, however, clarify which types of 'technical measures' may be used to obtain information. This means, therefore, that all the services are allowed to decide for themselves to what type of measure to use and what type of information on a person's private life can be secretly obtained during the operational control. Although a prosecutor and judicial consent (*ex ante*) is provided, the court has no legal power to assess the appropriateness of the measure chosen by the services in a specific case.

The operational control is allowed during preliminary investigations to prevent, detect and collect any evidence about serious – usually intentional – criminal offences. The statute defines these offences by their generic names (i.e. terrorism, espionage, manslaughter) or by referring to specific chapters of criminal acts or even to specific provisions. However, the operational control may also be carried out in order to prevent or detect some 'crimes prosecuted under international agreements'. The Attorney General claimed that such provisions are imprecise. Therefore, the legal scope of such surveillance is unknown and blurred.

On the other hand, the Internal Security Agency Act stipulates that the operational control may be pertinent in order to prevent, detect, investigate and prosecute offences against, *inter alia,* 'state security' and the 'economic well-being of the state'. In turn, the Military Counter-Intelligence Act authorises this agency to use operational control in order to identify, prevent or prosecute criminal

offences against the defence potential of Poland's Armed Forces, the Ministry of Defence and its organisational units and allied states as well as in the performance of its analytical tasks. The scope of operational control in these two Acts is quite broad and therefore – it was claimed – individuals are unable to recognise under what circumstances surveillance may be carried out and their privacy affected.

It should be noted that procedural guarantees of operational control may be considered to be relatively strong. As a general rule, it is required that a warrant issued by a district court is granted only upon written request from the appropriate chief of an agency, submitted after prior written consent from the Attorney General or a district prosecutor. Only in cases of the utmost urgency, where any delay could result in the loss of information or the obliteration or destruction of the evidence of a crime, may an operational control be ordered without a court warrant. In such cases, an *ex post* judicial review is provided. This must be carried out within five days. Another procedural safeguard is the so-called subsidiarity clause, whereby the information sourced from an operational control can only be secretly obtained when absolutely necessary and when less intrusive measures have proved ineffective or unsuitable.

As shown by statistics drawn up separately by the Attorney General and the Minister of Internal Affairs, approximately 4,000 operational controls are carried out in Poland annually.

Data retention

The second form of surveillance law on which the Tribunal adjudicated is access to telecommunication metadata retained by providers of public communications networks or publicly available electronic communications services.[8] The metadata which must be retained pursuant to the Telecommunication Act of 2004[9] include: data necessary to trace and identify the source of a communication and its destination; data to identify the date, time, duration and type of communication; data that can identify users' communication equipment; data that can identify the location of mobile communication equipment; data which consists, *inter alia*, of the name and address of the subscriber or registered user, the originating telephone number, the number called and an IP address for internet services.

In Poland, telecommunication metadata are provided only to the courts and prosecutors upon their request during a criminal trial and preliminary inquiry (pursuant to Article 218 of the Code of Criminal Procedure[10]) and – at the

[8] *See* A. Adamski, *The telecommunication data retention in Poland: does the legal regulation pass the proportionality test?*, 1 *ICT Law Review* (2013), p. 4-11.

[9] The Telecommunications Act of 16 July 2004, Dziennik Ustaw [*Official Journal*] 2014, item 246.

[10] Criminal of Criminal Procedure of 6 June 1997, Dziennik Ustaw [*Official Journal*] 1997, no. 89, item 555.

pre-trial stage – to officers from the Police, the Border Guard, the Treasury Intelligence Service, the Military Gendarmerie, the Military Counter-Intelligence Service, the Internal Security Agency, the Central Anti-Corruption Bureau, and Customs Service. It should be emphasised that in the judgment of 30 July 2014, the Tribunal referred only to the latter problem of access to metadata by law enforcement and intelligence authorities.

Although the challenged provisions are the consequence of Directive 2006/24/EC,[11] it must be emphasised that access to telecommunication metadata during criminal proceedings was introduced as an innovative tool to combat terrorism and other illegal activities in Poland somewhat earlier, in 2000. The obligation to retain subscribers' traffic and localisation data, however, was expressly imposed on telecommunications entrepreneurs in 2003. In the beginning, the period of retention was 12 months. By 2005, it was extended to two years[12] (the maximum stipulated by Directive 2006/24/EC), then in 2012 it was again shortened to 12 months. It should be noted that according to 'Information for the European Commission on the provision of telecommunications data retained by telecommunications undertakings and operators in 2013' issued by the President of the Office of Electronic Communications, in approximately 49% of cases, retained data is requested within the first two months of its retention, while in 69% of cases, retained data is requested within the first four months of its retention. In this regard, a 12-month period of data retention could be reasonably considered as both too long and unjustified under the principle of proportionality.[13] In 2013, the telecommunication providers received approximately 1.75 million requests for data from authorised entities: courts, prosecutors and law enforcement or intelligence agencies. It should be noted that a declining trend in the number of requests was observed between 2012 and 2014.

The Directive was transposed into the Polish legal system in 2009 through changes in the Telecommunications Act, the Code of Criminal Procedure and a number of statutes concerning the organisation and competences of law enforcement and intelligence agencies. In fact, the Directive was adopted in a very extensive way. First of all, the period of retention was set at 24 months (the maximum allowed by the Directive). Second, contrary to the Directive,

[11] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54-63, declared invalid by the ECJ on 8 April 2014, C-293/12.

[12] There were political attempts in Poland to propose an even longer period of data retention than stipulated in the Directive (up to five years). This proposal, however, failed.

[13] For instance, the Federal Constitutional Court of Germany in its judgment of 2 March 2010 ruled that a six-month period of retention is enough and must be deemed as the maximum allowed under the principle of proportionality.

certain data was made available not solely for the purposes of the investigation, detection and prosecution of serious crimes as the Directive had expressly stated. Indeed, the legislature went further and entitled all the authorities to obtain data retained in case of any crime, even if trivial in nature. Treasury Intelligence officers may also obtain telecommunications data in order to detect and prosecute certain infringements of domestic and European customs law. Civil and military counter-intelligence agencies, as well as the Central Anti-Corruption Bureau, are entitled to obtain retained data in the course of their statutory tasks, even those regarded as analytical. Third, access to metadata is not dependent on a prior review carried out by a court or by an independent administrative body. In other words, there is no external, impartial supervision over access to metadata. Last but not least, the legislature did not stipulate the subsidiarity clause, which would have meant that telecommunications data could only be obtained in specific cases when strictly necessary and when other less intrusive measures proved ineffective or unsuitable.

Historical and political context

The problem of surveillance in Poland has a special dimension. After World War II – and until 1989 – the Communist Party was in power. Various forms of surveillance were employed against citizens, not only in order to combat serious criminal activities but also for the purpose of political repression. Security services did not serve well-understood interests for the common good and the state, but instead they served the people in power. Therefore, despite more than 25 years elapsing since the fall of the communist regime, a high level of distrust towards the government can be observed in Polish society and in particular towards the security services and their surveillance powers. For this reason, legislation granting surveillance powers to the authorities is generally viewed critically by the eyes of the public.

Poland is among those European states that authorise a fairly wide range of authorities to carry out surveillance. As mentioned before, access to telecommunications data is, for example, provided to all courts and prosecutors in criminal proceedings as well as eight law enforcement and intelligence agencies. Over the last few years, the number of entities empowered to obtain retained data and granted operational control over data communication has increased (metadata has been available to Customs Service officers since 2009 in order to detect and combat illegal gambling and to the Central Anti-Corruption Bureau since 2006 in order to perform all its statutory duties, not only combating criminal activities, but also analysing financial statement of public officials). In addition, the legislature has extended the list of situations in which it is permissible to obtain information

about people during covert operations. Without any hesitation, it could be concluded that a variety of surveillance measures can be applied to combat at least half of all criminal or illegal offences envisaged in the Polish legal order.

The constitutionality of Polish surveillance law has been examined by the Tribunal a number of times in the past.[14] Many legal provisions concerning the competencies of law enforcement and intelligence services in that area had to be repealed or amended because they were inconsistent with the Constitution. Among others, in its 2006 decision S 2/06,[15] the Tribunal signalled the lack of a legal obligation to inform the concerned person about surveillance measures taken against him or her, even after operational control was concluded. In 2010, the Tribunal indicated in decision S 4/10[16] that the provision of the Internal Security Agency Act empowering this agency to carry out the operational control in order to recognise, prevent, detect and prosecute crimes against the 'economic well-being of the state' could be inconsistent with the Constitution and therefore should be amended. Both decisions have been ignored and no necessary procedural safeguards have been introduced so far.

Similarly, it seems that the state has not ensured the compliance of certain surveillance law provisions with the requirements imposed by the European Court of Human Rights in its well-established case law, despite the fact that Poland has been a member of the Council of Europe since 1991. In particular the legislation failed to identify the nature of the offences which could give rise to a surveillance order, to provide external supervision over the access to data retained, to explain the procedure to be followed in examining and storing data obtained, the precautions to be taken in communicating the data and the circumstances in which data could or should be destroyed.

It is difficult to explain exactly what caused the Human Rights Defender and the Attorney General's motions to challenge the surveillance law. Probably, the inaction of the legislature in executing previous judgments and decisions of the Constitutional Tribunal played a vital role. Then, some cases of illegal surveillance took place in Poland, including of politicians and journalists in particular.[17] This could have given rise to legitimate concerns that existing legal provisions did not provide sufficient safeguards against arbitrary measures and malpractice. Another factor influencing a negative approach to surveillance law was the difficulty in obtaining statistical data concerning a number of operational control measures in Poland and also an alarming number of metadata requests (circa 1.75 million annually) – one of the highest

[14] Judgments of the Constitutional Tribunal of: 20 April 2004, K 45/02; 20 June 2005, K 4/04; 12 December 2005, K 32/04; 23 June 2009, K 54/07.

[15] Decision of the Constitutional Tribunal of 25 January 2006, S 2/06.

[16] Decision of the Constitutional Tribunal of 15 November 2010, S 4/10.

[17] *See* the article Abuses in using surveillance methods against journalists – the need of legislative changes in Poland <humanrightshouse.org/Articles/15435.html> visited 19 October 2015.

among EU member states.[18] This situation raised legitimate concerns about the abuse of the law. Finally, it should be noted that the implementation of the Data Retention Directive 2006/24/EC met with staunch resistance from public watchdogs, especially the Helsinki Foundation for Human Rights and the Panoptykon Foundation. Their criticism was that the government's legislative process had been carried out in a hurry, without due consideration of critical voices, leading to the unconstitutionality of provisions on the data retention mechanism. Consequently, the Directive, as mentioned, was implemented in a very extensive way and – by chance – contained provisions which EU law did not require.

Main thesis of the judgment

Protection of privacy and secrecy of communication in the digital era

The judgment of 30 July 2014 is undoubtedly a milestone in the constitutional jurisprudence of Poland. The Tribunal commented more broadly on the protection of privacy and communication secrecy in the digital era and the legal scope of surveillance under present-day circumstances. It pointed out that technological development extends into the realm of an individual's capabilities as well as opening up new and unknown ways to exercise constitutionally protected freedoms and rights. It has made it possible in previously unprecedented ways to overcome logistical barriers of space and time in communication, in the way goods and services are acquired, and in meeting an individual's everyday needs.

The internet plays a special role now, and has ceased to be merely a means of communication. The internet is a multidimensional tool enabling creation, storage and transmission of different types of data. The Constitution of Poland does not directly relate to an individual's activities in virtual space. It does not stipulate access to the internet as a human right or provide specific guarantees of protection against infringements of freedoms and rights in this area.[19] According to the Tribunal, the constitutional protection of an individual's freedoms and rights in

[18] Press release on Information for the European Commission on the provision of telecommunications data retained by telecommunications undertakings and operators in 2013 <en.uke.gov.pl/information-on-annual-report-on-the-provision-of-telecommunications-data-13559> visited 19 October 2015. *See also* Evaluation report on the Data Retention Directive (Directive 2006/24/EC), European Commission, COM(2011) 225 final; Access of public authorities to data of internet service users. Seven issues and several hypothesis, Panoptykon Foundation available at <panoptykon.org/sites/panoptykon.org/files/transparency_report_pl.pdf> visited 19 October 2015.

[19] *See* among others: decision of the French Constitutional Council, 10 June 2009, No. 2009-580, in which the Council stated that internet access is a fundamental human right, protected by Art. 11 of the Declaration of the Rights of Man and the Citizen of 1789.

connection with their use of the internet is, however, similar to the protection afforded to traditional forms of communication or other activities.

The obligation on the state to respect and protect privacy and the general prohibition of interference with this private sphere is defined in Article 47 of the Constitution, according to which everyone shall have the right to legal protection of private and family life, of dignity and good standing as well as to make decisions about his personal life. Those guarantees are supplemented by Article 49 (freedom and secrecy of communication) and Article 51 of the Constitution (informational autonomy). All the aforementioned values have their roots in inherent and inalienable human dignity (Article 30 of the Constitution), which is the source of all constitutional freedoms and rights. The relationship between privacy and human dignity is of a specific nature. The protection of dignity requires the respect of the purely personal human sphere, where the person is not forced to 'be with others' or 'share with others' their experiences or intimate details. Therefore, privacy is the constitutionally protected freedom of individuals who are able to act within that freedom as long as a relevant statute does not delimitate its scope. Only an unambiguous statutory regulation may impose restrictions within the purview of undertaking certain actions that fall within the boundaries of a specific freedom.

Referring to Strasbourg and other constitutional courts' case law, especially that of the Federal Constitutional Court of Germany's jurisprudence, the Tribunal pointed out that the right to the protection of privacy (Article 47) and secrecy of communication (Article 49) should embrace, *inter alia*, transmission of information and the activity of individuals in any form, regardless of the physical medium (e.g. personal and telephone conversations, written correspondence, fax, text and multimedia messages, email). Constitutional protection covers not only the content of messages transmitted via the internet or other telecommunication networks, but also all the circumstances of the communication process which include personal data such as dialled phone numbers, the time and frequency of calls, the geographic location of participants of the conversation, IP numbers or web browsing history, etc. Consequently, there is no personal sphere for human beings, even connected with new technologies, where constitutional protection would be blocked or reduced.

The protection of privacy and secrecy of communication extends to the whole process of collection, storage and processing (including analysis and comparison) of information on individuals. Examples of separate interference with the constitutionally-protected status of individuals that would require separate constitutional justification are as follows: the obtaining of information during operational control; imposing legal obligations on private entities to retain metadata; access to the data by public authorities; the subsequent verification or transfer of such metadata to other bodies.

One of the main findings in the judgment was the following: in the Tribunal's opinion, in a democratic state ruled by law, each person has the right to anonymity while exercising their constitutional freedoms. There is no obligation to disclose their identity and the details of their life to the state nor other individuals. Any interference with this rule requires a constitutional justification and must be proportionate.

With globalisation in progress, the state is obliged to protect the privacy of its citizens against different invasions stemming from different sources. The obligation of the state is to protect each citizen's privacy from the monitoring of various spheres of their life by foreign entities, particularly intelligence agencies. Breach of the right to privacy stipulated by Article 47 of the Constitution occurs not only by the direct action of the Polish authorities, it also occurs in the absence of sufficient protection against interference caused by foreign agencies' surveillance of Polish citizens.

The Constitutional Tribunal emphasised that, regardless of specific formal and material requirements that must be in accordance with the law authorising surveillance by public authorities, it is not acceptable in a democratic state ruled by law to record all aspects of an individual's private life, especially in a way which enables it to reconstruct all forms of their activity in life. This would be deemed as a violation of the essence of the right to privacy and informational autonomy, as is strictly prohibited by Article 31(3) of the Constitution.

Privacy and security of the state – balancing conflicting values

Although new technologies facilitate individual lives, they can also be used to commit crimes and to violate the legal order. Technological development has brought about new ways of committing traditional crimes. Thus, new technologies have become an additional, sophisticated tool that can make criminal activity easier. Technological development has also led to new, previously non-existent types of offences that can be committed only by technological means (e.g. cybercrime). According to the Tribunal, this justifies providing law enforcement and intelligence agencies with adequate powers so that they will be able to prevent or detect different types of criminal offences. A democratic state ruled by law may not, in fact, ignore the growing importance of new technologies and the scale of their use in violating the law. Public authorities should have legal and actual remedies to detect committed offences and activities against state security. They should also be able to pre-empt the actions of persons infringing the legal order.

The power of law enforcement and intelligence services to secretly obtain the contents of a communication (or even metadata connected with it) interferes with the right to privacy, secrecy of communication and informational autonomy. As the Tribunal reiterated, the mere existence of legislation authorising surveillance

by such authorities must be considered an intrusion into the constitutionally protected status of human beings.

The legal possibility of surveillance affects the use of constitutional freedoms and rights. Awareness of being subject to continuous supervision can discourage people from exercising their constitutional freedoms and rights. It can raise fears of the unauthorised collection and use of information by public authorities, not only in order to ensure the state and citizens' security, but also for other purposes. These concerns are particularly strong in Polish society, which over the decades of the Communist regime fell under surveillance by the security services.

Constitutional standard of surveillance law

In its judgment of 30 July 2014, the Tribunal not only reiterated previous case law concerning constitutional standards of surveillance. Bearing in mind that the legislature had not yet carried out the recommendations stemming from well-established constitutional adjudication, and taking into account the application of existing legal provisions in practice, the Tribunal recalled all requirements which must be met by the legislature.

Such requirements are as follows:

- collection, storage and processing of data relating to individuals, and especially in the sphere of their privacy, are permissible only on the basis of a clear and precise provision by statute;
- it is necessary to specify by statute which authorities are empowered to collect and process data on individuals;
- surveillance is allowed only in the detection, prevention or prosecution of serious offences, whereby the statute should specify the type (nature) of such offences;
- the statute must specify the categories of individuals who can be under covert operations;
- it is highly desirable to determine by statute the nature of surveillance measures which enable information to be secretly obtained;
- surveillance should be a subsidiary measure of acquiring information that is admissible only when relevant information or evidence cannot be obtained in a less intrusive manner;
- the statute should specify the maximum period of surveillance as is necessary in a democratic society under the rule of law;
- surveillance is admissible only upon an order issued by a court or other independent administrative authority;
- the statute must have precise rules and define a set of principles concerning the use of collected materials in criminal proceedings, as well as the conditions of destruction of unnecessary data;

- the law must ensure an appropriate level of security against unauthorised access to retained data;
- transparency of statistical information relating to the quantity and type of used surveillance is welcome;
- it is not ruled out that differentiation may be introduced with regard to the intensity of the protection of privacy, informational autonomy and communication secrecy, depending on whether data on given persons are obtained by civil and military intelligence and counter-intelligence services or whether they are gathered by law enforcement agencies (police forces);
- differentiation with regard to the level of protection of privacy, informational autonomy and communication secrecy may also be introduced, depending on whether the obtaining of information in secret concerns citizens or persons who are not Polish citizens.

Shortcomings of the judgment

The judgment of 30 July 2014 forms a significant part of the European approach towards privacy and personal data protection. In this case, the Polish Tribunal has joined a successful dialogue with the Strasbourg and Luxembourg courts and the other European constitutional bodies. None of them undermined admissibility of surveillance as an effective tool for combating serious offences, although they do demand that strong procedural safeguards should be laid down. It seems to be an important observation in the judgment, that if the scale of surveillance and interference with privacy becomes larger and inevitable, the procedural framework of surveillance must become more effective. The judgment of the Polish Tribunal, other constitutional courts and supranational bodies give a clear signal to governments that all attempts to regulate mass surveillance may face resistance from constitutional adjudication. Nevertheless, it is not acceptable in a democratic state ruled by law to maintain the security of its citizens at any cost, including the loss of their privacy.

In my opinion, however, the Tribunal's decision seems to be inconsistent with some of the requirements developed in the case law of the European Court of Human Rights and the European Court of Justice.

First of all, it found the legal provisions authorising law enforcement agencies to carry out an operational control in order to prevent or detect crimes 'prosecuted under binding international agreements' to be compatible with the Constitution and the Convention.[20] Although the Tribunal recognised some doubts that had arisen in the context of its linguistic construction, it found that an alternative

[20] It is stipulated in the Police Act, Border Guard Act, Treasury-Intelligence Act and Military Gendarmerie Act.

https://doi.org/10.1017/S1574019615000322 Published online by Cambridge University Press

interpretation in accordance with the Constitution and the Convention was also possible and must be applied. Therefore, the contested provisions – construed as concerning offences specified in the Polish penal law that were prosecuted on the basis of ratified international agreements – are consistent with Article 2, Article 47 and Article 49 in conjunction with Article 31 paragraph 3 of the Constitution as well as Article 8 of the Convention. Moreover, the Tribunal stated that one of the provisions of the Internal Security Agency Act, insofar as it comprised the wording 'and other offences that are against national security', is consistent with Article 2, Article 47 and Article 49 in conjunction with Article 31(3) of the Constitution as well as Article 8 of the Convention. According to the Tribunal, the law in question is sufficiently clear. Minimal procedural safeguards are also met.

In my opinion, such statutory provisions are inconsistent with the Constitution and the Convention and the Tribunal's approach is thereby contrary to established constitutional and Strasbourg case law. The European Court of Human Rights has consistently demanded that 'in accordance with the law' within the meaning of Article 8(2) of the Convention, requires that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned who must, moreover, be able to foresee its consequences for him. That said, it must also be compatible with the rule of law. Consequently the nature of the offences which may give rise to an interception order should be set out precisely within the law. In *Weber and Saravia* v *Germany*[21] the Court ruled the complaint inadmissible, partially because in German law the nature of the offences was precisely described. The same approach can be found in *Iordachi and Others* v *Moldova.*[22] Moldovan surveillance law was found inconsistent with Article 8 of the European Convention on Human Rights because 'the nature of offences' which may give rise to the issue of an interception warrant was not clearly defined in the impugned legislation. In particular, the Court noted that more than half of the offences provided for in the Criminal Code fell within the category of offences eligible for interception warrants, so there was no opportunity to determine to what extent the state was authorised to interfere in privacy and the secrecy of correspondence.

Taking into account established Strasbourg case law,[23] the opinion of the majority of the Tribunal seems to settle on the edge of European human rights

[21] ECHR 29 June 2006, Case No. 54934/00, *Weber and Saravia* v *Germany.*

[22] ECHR 10 February 2009, Case No. 25198/02, *Iordachi and Others* v *Moldova.*

[23] The European Court of Human Rights in the case of *Kennedy* v *The United Kingdom* explained, however, that the term 'national security' is sufficiently clear and frequently employed in national and international legislation, including Art. 8(2) of the Convention. This approach is also applied to surveillance legislation. Therefore, the ECtHR said in the case under consideration – contrary to its

adjudication.[24] Let me explain the point. To apply operational control in order to prevent or detect crimes 'prosecuted under binding international agreements' or 'against state security' – within the meaning of the challenged provisions – the authorities have to determine which of all the offences criminalised in the Polish legal system are of such a nature. There is not, however, any official list of offences which are considered to be 'against state security' or 'prosecuted under international agreements' and it is impossible to reconstruct them easily. Such a catalogue has not been developed in the case law or legal science. Moreover, the Tribunal was not able to establish it at the hearing, although it had formally inquired with the Minister of Justice and Minister of Foreign Affairs beforehand and again during the hearing to clarify doubts that had arisen. As a result, neither the statute nor international agreement and their judicial interpretation determined the real scope of the contested provisions and their interference with individual privacy, and so it all depends on interpretations made by law enforcement and intelligence agencies. Consequently, too much discretion was left to the executive power. The Tribunal ought to have held the contested provisions to be unconstitutional.

Secondly, the Tribunal approved the constitutionality of provisions that do not specify the nature of technical measures in operational control in the form of a so-called interpretative sentence. In other words, these provisions are constitutional provided that they are construed in a way that the authority ordering operational control indicates is a technical measure specified by law in a given case. The Tribunal emphasised that specifying the nature of technical measures in the statute is highly recommended. However, in the case in point, where the legislation did not stipulate the nature of technical measures of surveillance, it said that a change in judicial practice is sufficient in order to meet the constitutional standard. According to the Tribunal, in each case a specific technical measure for obtaining information and evidence must be indicated. The nature of such measures ought to be stipulated by law, even by secondary or internal legislation. Undoubtedly, this requirement on the one hand is to guarantee individuals' protection against arbitrary measures. On the other hand, it leads to a situation in which the Parliament – as a representative body of the Nation (*vide* Article 4 of the Constitution) – has no real power to assess the admissibility of the scope and

judgment in *Iordachi* v *Moldova* and the vast majority of judgments – that the requirement of 'foreseeability' of the law does not go so far as to compel states to enact legal provisions, listing in detail all conduct that may prompt a decision concerning individuals (ECtHR 18 May 2010, Case No. 26839/05, *Kennedy* v *The United Kingdom*, para 159).

[24] These arguments were also raised in dissenting opinions to the judgment submitted by Justice Marek Zubik and Justice Wojciech Hermeliński, who contested the Tribunal's reasoning on the provisions of the Internal Security Agency Act allowing for operational control in order to combat unspecified crimes against state security.

methods of intrusion in an individual's privacy. After the judgment, measures of covert surveillance remain outside of democratic and parliamentary control.[25]

Thirdly, the Tribunal found the provisions concerning access to telecommunication data by law enforcement and intelligence services to be unconstitutional due to an absence of independent supervision over such access. In order to meet constitutional requirements, *ex post* supervision consisting of examining the validity of data accessibility in specific cases is judged sufficient. The Tribunal thus prioritised such values as national security and the efficiency of public authority activities at the expense of the procedural guarantees of fundamental rights. The Tribunal observed that introducing prior consent regarding the acquisition of data might paralyse operational activities and hinder criminal prosecutions. Prior consent may be provided for particular situations, i.e. cases involving the protection of professional secrecy. In this regard, the position of the Tribunal departs from the established and dominant case law of the European Court of Human Rights and the views expressed by the European Court of Justice. It is emphasised in Strasbourg case law that prior consent is crucial for preventing the abuse of law and the surveillance of citizens for illegal purposes.[26] To some extent, prior consent constitutes an institutional guarantee for both the public interest and the interest of the person under surveillance. It must be emphasised that Directive 2006/24/EC was found invalid by the European Court of Justice in the *Digital Rights Ireland* judgment due to the fact that

> the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.[27]

[25] The judgment in this regard seems surprising for one more reason: at the hearing representatives of law enforcement and intelligence services pointed out that the legal definition of technical measures by their generic names do not influence their effectiveness in combating crimes.

[26] ECtHR judgments regarding the issue refer mostly to the tapping and interception of telephone calls, not raising the issue of metadata directly. *See* amongst others: ECtHR in *Klass and others* v *Germany,* paras. 55-56, ECtHR 14 April 1990, Case No. 11801/85, *Kruslin v France*, para. 34; 29 June 2006, Case No. 54934/00, *Weber and Saravia* v *Germany*, paras. 115-117; 28 June 2007, Case No. 62540/00, *Association for European Integration and Human Rights and Ekimdzhiev* v *Bulgaria*, paras. 79-84; 25 June 2013, Case No. 18540/04, *Valentino Acatrinei* v *Romania*, paras. 57-59 and the cited previous judgments concerning Romanian cases; 15 January 2015, Case No. 68955/11, *Dragojević* v *Croatia*, § 92-95. In the case of *Uzun* v *Germany* the ECtHR accepted a subsequent court review (ex post revive) of surveillance consisting of monitoring the movement of vehicles via satellite navigation devices. *See* ECtHR 2 September 2010, Case No. 35623/05, § 71-72.

[27] ECJ 8 April 2014, Case C-293/12, *supra,* § 62.

Furthermore, it is an Achilles' heel of the judgment from the Polish Constitutional Tribunal that the Tribunal examined only the narrow issue of the absence of independent control over obtaining metadata, which in addition was interpreted differently from the obligations in respect of the judgments of the European Court of Human Rights and the European Court of Justice. Moreover, the remaining allegations of the applicants were not examined on the merits, to wit: the acquisition of metadata in order to prosecute every crime or fiscal crime, including trivial ones, and analytical and planning tasks (concerning the Internal Security Agency, the Counter-Intelligence Service and the Central Anti-Corruption Bureau). Such broadly implemented statutory objectives breached the EU Directive (in the light of which retained data was to be made accessible to the competent national authorities solely to prosecute *serious* crimes – emphasis added) and led to disproportional interference with the right to privacy and secrecy of communication. Another of the applicant's allegations was not examined by the Tribunal, namely the alleged lack of a subsidiarity clause. As was mentioned, such guarantees are not provided for by Polish law. Unfortunately, the Tribunal remained silent on this issue.

Concluding remarks

The new legal situation following the judgments of the European Court of Justice and the Constitutional Tribunal presents a great challenge to the Polish lawmaker.

Firstly, in the event that the legal situation is not adjusted to requirements which derive from the Tribunal's judgment, the contested provisions will stop being in force as of 7 February 2016. As a result, from that date forward, there would be no legal basis for, *inter alia*, gathering telecommunication metadata by the law enforcement and intelligence services, the exercise of operational control for crimes against the well-being of the state – the identification and prosecution of which is the task of the Internal Security Agency. In that regard, it is necessary to undertake legislative action, otherwise there is a risk of hindering efficiency in combating serious crime and threats to public security.

Secondly, the standard of surveillance determined by the Constitutional Tribunal must be considered a minimum, not a maximum. However, the legislature is not prevented from providing stronger guarantees as requested by the European Court of Human Rights or the European Court of Justice. In accordance with Article 9 of the Constitution, the Republic of Poland shall respect international law binding upon it. Therefore, public authorities are bound to take into consideration all requirements, i.e. also those stemming from international agreements (as interpreted by international judicial authorities exercising the competence of a binding interpretation of the treaties). In my opinion, this means

that electronic surveillance is allowed only in order to prevent or prosecute serious crimes, as laid down by the law in the most precise manner. The legislature should also determine the technical measures of classified acquisition of information and of telecommunication metadata; it should not only provide independent prior control as a rule, but also limit the instances of admissibility of submitted data and introduce a subsidiarity clause.

Thirdly, although the judgment of the European Court of Justice in the *Digital Rights Ireland* case found Directive 2006/24/EC to be invalid on account of its infringement of the right to privacy and family life (Article 7 of the Charter of Fundamental Rights of the European Union) and the right to the protection of personal data (Article 8 of the Charter), the judgment has no immediate effect on the domestic provisions implementing the directive. The only consequence of the European Court of Justice's judgment is that member states ceased to be obliged to uphold the provisions regulating the retention of data. However, the domestic provisions concerning the issue have not been rescinded by the Polish legislature. As a result, providers of publicly available telecommunication services continue to be statutorily obliged to retain metadata for 12 months and transfer it to competent authorities on demand (Article 180a of the Telecommunications Act).

Fourthly, despite the fact that Directive 2006/24/EC was invalidated by the European Court of Justice, the retention of metadata by operators and providers seems to fall within the scope of European Union law, and as such is subject to the guarantees of the Charter of Fundamental Rights (Article 51 of the Charter).[28] This means that the requirements of the *Digital Rights Ireland* judgment are binding on the Polish legislature. Therefore, it must be noted that the data retention directive harmonised the exceptions from protection of personal data provided in Directive 2002/58/EC (the so-called e-Privacy Directive)[29] and influenced the functioning of the single market. In the light of Directive 2002/58/EC, if member states decide to uphold the provisions regarding the retention of telecommunication data, these provisions – as exceptions from the principles of data protection and data security expressed in Directive 2002/58 – must fulfil all requirements laid down by Article 15 of this Directive. In that regard, the established solution must be a necessary, appropriate and proportional measure within the framework of a democratic society to ensure national security, defence, public security, and the prevention, investigation, detection and prosecution of

[28] ECJ 7 May 2013, Case C-617/10, *Åklagaren* v *Hans Åkerberg Fransson*, § 19; ECJ 6 March 2014, Case C-206/13, *Cruciano Siragusa* v *Regione Sicilia – Soprintendenza Beni Culturali e Ambientali di Palermo*, § 21-25.

[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37

criminal offences or of unauthorised use of the electronic communication system. Consequently, it would be fair to assume that the provisions regulating the retention of telecommunications data fall within the application of European Union law (in accordance with Article 51 of the Charter of Fundamental Rights) and as such the requirements laid down in the Charter of Fundamental Rights of the European Union also apply. In that regard, the Polish lawmaker should take into consideration the judgment of the European Court of Justice in the *Digital Rights Ireland* case and the guarantees stemming from the Charter of the Fundamental Rights of the European Union when amending statutory provisions regulating the retention and access to metadata.