ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3744
PRZEGLĄD PRAWA I ADMINISTRACJI CVII
WROCŁAW 2016
DOI: 10.19195/0137-1134.107.7

AGNIESZKA GRZELAK*
Kozminski University, Department of International and European Union Law

FUNDAMENTAL RIGHTS PROTECTION IN THE CONTEXT OF MASS SURVEILLANCE IN THE EUROPEAN UNION

DEFINITION OF MASS SURVEILLANCE

In the *Concise Oxford Dictionary* surveillance is defined as "close observation, especially of a suspected person". Obviously today many of the new surveillance technologies are applied not only to "a suspected person" (then it would be rather "targeted surveillance"). They are commonly applied to whole categories of people on the grounds that information is generally required for "national security" or "public security" purposes. Obviously, surveillance is also applied to contexts (geographical places and spaces, particular time periods, networks, systems and categories of person), not just to a particular person whose identity is known beforehand[1]. For Privacy International, mass surveillance is the subjection of a population or significant component of a group to indiscriminate monitoring[2]. Surveillance itself involves paying close and sustained attention to another person. But the question is what makes surveillance considered mass surveillance or large-scale surveillance[3].

According to various sources, mass surveillance means that an entire or a substantial fraction of a population is monitored. This differentiates mass surveillance from the so-called "targeted surveillance" — targeted against one or several persons involved in criminal investigations which is regulated in most countries by the criminal procedure codes. If surveillance of specific individuals is undertaken, it is on the grounds that the collection of data is deemed necessary to detect and

* Professor at Kozminski University, Department of International and European Union Law.

[1] Gary T. Marx, "What's New About the "New Surveillance"? Classifying for Change and Continuity, Surveillance & Society" 1(1), pp. 9–29, available at www.surveillance-and-society.org.

[2] https://www.privacyinternational.org/node/52 Cf. also http://definitions.uslegal.com/m/mass-surveillance/.

[3] To make it clear: I do not differentiate between large-scale surveillance and mass-surveillance for practical reasons related to the volume of the paper.

prevent violent actions in the making, not to gather information on lifestyles or political opinions. The European Parliament resolution of 2014 refers to "far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and nonsuspicion-based manner"[4]. This definition encompasses two essential aspects: first, a reference to a collection technique, and second, the distinction between targeted and untargeted collection[5].

According to the Study on National Programmes of Mass Surveillance, launched by the European Parliament, "the new resources for surveillance, the widespread use of smart phones and the development of cloud computing have blurred the line between 'targeted surveillance' — justified by the fight against crime — and data mining, which carries the risk of extending the scale and the purpose of surveillance"[6]. The mass surveillance programmes have been justified by the intention to protect the population from crimes, and were tailored to provide tools for the profiling of the categories of people likely to commit such crimes. However, once data are available to search and extraction, they may be put to other purposes. Therefore, what has to be questioned is the possible transformation of large-scale surveillance (mass surveillance) into what can be called "cyber-mass surveillance" that enables access without warrant to a much larger scale of data.

It is precisely the purpose and the scale of surveillance that differentiates democratic regimes from police states. In principle and rather in theory — intelligence services in democratic regimes do not, or at least should not, collect data in mass on large groups of the population in order to collect data which can be used in the future for an undefined goal[7]. In practice, however, especially as was revealed and proved by Edward Snowden, mass surveillance is often carried out by governments or governmental organisations or services, such as intelligence services or other security services and law-enforcement services, such as the police. So surveillance of certain population groups is not a new phenomenon in liberal regimes. Naturally, depending on each nation's laws and judicial systems, the legality of and the permission required to engage in mass surveillance vary. Since in a democracy the separation of power exists, any excess of powers should

[4] European Parliament (2014), Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), P7_TA (2014)0230, 12 March 2014.

[5] Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal Framework, European Union Agency for Fundamental Rights 2016.

[6] European Parliament, Directorate General for Internal Policies, National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law, Study 2013.

[7] A. Dulles, *The Craft of Intelligence*, New York 1963, p. 257.

be regularly denounced when the unlawful activities of intelligence services or law-enforcement services have been uncovered.

LINK BETWEEN TERRORIST ATTACKS AND COMPETENCES OF INTELLIGENCE AND LAW ENFORCEMENT SERVICES IN THE AREA OF MASS SURVEILLANCE

Terror attacks worldwide always create a discussion about broad measures allowing intelligence and law enforcement services to use new methods and new competences in the hope of preventing further violence. Mass or large-scale surveillance has often been mentioned as necessary to fight crime, especially terrorism, and to protect national security. New competences interfere with several fundamental rights, so there is always a need to check whether this interference can be justified on the basis of norms provided by the international and constitutional standards in particular case of each state. One should remember that protecting the public from real threats to security and safeguarding fundamental rights involves delicate balancing, and has become a particularly complex challenge in recent years.

At the very pragmatic level, mass surveillance or large-scale surveillance creates a tendency to collect data extensively and retain them over a long period of time in order to establish trends that facilitate big-data correlations and hierarchies. Therefore, there is a fear that increasing mass surveillance could lead to the development of a surveillance state where civil liberties are infringed or political dissent is undermined by surveillance programs. The digital age has produced technological innovations facilitating large-scale communications data monitoring — which could easily be abused. Some even call for resignation from or at least serious limitation of, safeguarding human rights in such situations. Mass surveillance has equally often been criticized for violating privacy rights, limiting civil and political rights and freedoms, and being illegal under some constitutional systems.

Violations of fundamental rights in case of surveillance rights are not only a theoretical concern. This was clearly proved by Edward Snowden's revelations. Not only in the US, but also in Europe a series of programmes have been initiated, using all existing resources of the Internet. This involved also the development of integrated platforms, the breaking of software encryption keys and the development of new software that permits routine filtering, visualising and correlating unprecedented amounts of data and metadata[8]. Attempts of creating a list of surveillance programmes in Europe are not an easy task, because some of them are not public (like *Frenchelon* — whose existence the French government has never

[8] European Parliament, Directorate General for Internal Policies, National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law, Study 2013.

officially acknowledged[9]). Application of those programmes have been justified by the intention to protect the population from crimes. They were tailored to provide tools for the profiling of the categories of people likely to commit such crimes. However, it should be remembered that once data are available to search and extraction, they may be put to other purposes as well. Just to give an example of the Eurodac database, which was created for the purpose of asylum procedure[10], however, later on it was used also for crime combating purposes.

In order to illustrate this with examples of the surveillance programmes should be mentioned German *Nachriechtendienstliches Informationssystem*. This is a searchable database operated by the German security agency Bundesamt für Verfassungsschutz (BfV)[11]. Another example is Project 6 — a global surveillance project jointly operated by the German intelligence agencies Bundesnachrichtendienst (BND) and BfV in close cooperation with the U.S. Central Intelligence Agency CIA between 2005 and 2010. The project included a massive database containing personal information, such as photos, license plate numbers, Internet search histories and telephone metadata of presumed jihadists[12].

In the United Kingdom there are several programmes, such as for example *Impact Nominal Index,* which is a computer system that enables the UK police force to establish whether other relevant authorities hold information regarding a person of interest or *Interception Modernisation Programme*, which was an initiative to extend the UK government's capability to lawfully intercept and store communications data in a central database. However, the most relevant recently is *Dripa* (Data Retention and Investigatory Powers Act 2014), which allowed for the reten-

[9] FRENCHLON is a data collection and analysis network operated by the French Directorate-General for External Security. Its existence has never been officially acknowledged by the French authorities, although numerous journalists, have mentioned it based on military information, since the European Parliament investigated ECHELON and also its implications in counter-terrorism. See for example: http://www.zdnet.com/article/frenchelon-france-has-nothing-to-envy-in-echelon/.

[10] Cf. repealed Council regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, p. 1–10 and the new regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29.6.2013, pp. 1–30.

[11] http://www.bfdi.bund.de/DE/Datenschutz/Themen/Sicherheit_Polizei_Nachrichtendienste/RegisterDatenbankenArtikel/NachrichtendienstlichesInformationssystem-NADIS.html. See also M. Dahlke, *Demokratischer Staat und transnationaler Terrorismus: Drei Wege zur Unnachgiebigkeit in Westeuropa 1972–1975*, München 2011.

[12] https://www.wsws.org/en/articles/2013/09/14/germ-s14.html or https://www.rt.com/news/germany-cooperate-cia-islamists-database-579/.

tion of data and the *Investigatory Powers Bill*, which replaces it[13]. The purpose of the legislation was to allow security services to continue to have access to phone and internet records of individuals following a previous repeal of these rights by the Court of Justice of the European Union in the *DRI* case. In December 2016 the Court of Justice decided that the national legislation which provides for general and indiscriminate retention of traffic and location data (such as DRIPA) should be regarded as contrary to EU law[14].

FUNDAMENTAL RIGHTS AFFECTED BY THE MASS SURVEILLANCE PROGRAMMES

Mass surveillance programmes and legislation may affect a variety of fundamental rights protected by European Union law and international law as well, such as the right to privacy and the right to data protection, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU, EU treaties and EU secondary law, but also for example in Article 8 of the European Convention on Human Rights (ECHR)[15]. This in no way means that other rights are not affected. The European Parliament resolution from 2015 adopted on the subject of mass surveillance highlighted — when referring to other affected fundamental rights — in particular freedom of expression, of the press, of thought, of conscience, of religion, of association, the presumption of innocence and the right to fair trial and non-discrimination[16]. Mass surveillance endangers a number of human rights, including the right to privacy, the right to free speech and expression, the right to equal treatment, the right to freedom of religion, and the right to a fair trial. Additionally the mass surveillance potentially damages the right to liberty and security

[13] This Act should include provisions about the interception of communications, equipment interference and the acquisition and retention of communications data and bulk personal datasets, as well as the treatment of material held as a result of such interception, interference or acquisition or retention and the powers of the Investigatory Powers Commissioner and other Judicial Commissioners.

[14] In July 2015 the High Court issued an order that sections 1 and 2 of the Act were unlawful, and to be disapplied, suspended until 31 March 2016, thereby giving the government a deadline to come up with alternative legislation which is compatible with EU law. As of 4 November 2015 an investigatory powers parliamentary bill was drafted providing new surveillance powers, requiring records to be kept by Internet Service Providers tracking use of the Internet from the UK, accessible by the police and security services without judicial oversight. See also judgement of the Court of Justice in case C-203/15 and C-698-15 Tele 2 of 21 December 2016, ECLI:EU:C:2016:970.

[15] Cf. for example J. York, *The harms of surveillance to privacy, expression and association,* Electronic Frontier Foundation, Global Information Society Watch 2014 — Communications surveillance in the digital age; https://www.giswatch.org/sites/default/files/the_harms_of_surveillance.pdf.

[16] European Parliament (2014), Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), P7_TA (2014)0230, 12 March 2014.

of persons, while endangering Internet security. Furthermore, it is a powerful tool that can be used to subvert democratic rule, especially if technology falls into the hands of an autocratic regime.

This means that introducing mass or large-scale surveillance programmes by state authorities can cause strong tensions between international obligations of the state — in case of the EU with the EU founding commitments, principles and legal obligations, as outlined in Article 2 of the Treaty on the European Union. This provision identifies a set of principles deemed to be common to all EU Member States which include, among others, respect of democracy, the rule of law and human rights. Those values cannot be interpreted without reference to the Council of Europe standards, as interpreted by the European Court of Human Rights.

The right to privacy is the right that is most directly undermined by mass surveillance. The indiscriminate collection of data, including personal data, allows the collector of the data access to all online activity, which includes not only what you knowingly put onto the Internet but also everywhere you go with a smart phone, limited only by the computing power. This access has led Amnesty International UK to equate mass surveillance with treating everyone as a criminal[17]. The European Court of Human Rights (ECtHR) ruled also that the Hungarian government had violated Article 8 of the European Convention on Human Rights (the right to privacy) due to its failure to include "sufficiently precise, effective and comprehensive" measures that would limit surveillance to only people it suspected of crimes[18].

Since — in general — protection of national or internal security can justify interference in the fundamental rights (see for example Article 8 para 2 of the ECHR or Article 52 para 2 of the Charter of Fundamental Rights of the EU), some governments and other institutions claim that surveillance is necessary in order to protect national security. The notion of "national security" as framed and understood by them does not correspond to the democratic understanding of national security as foreseen in the constitutional systems, where a key element of constitutionality remains in the effective judicial control and supervision of the executive or governmental actions.

The European Court of Human Rights has over the years developed standards, based on Article 8 of the ECHR, including its procedural aspects, and on Article 13 of the ECHR — the right to effective remedy. Its case law has reviewed various forms of surveillance. ECtHR standards have triggered legislative reforms at a national level, narrowed the scope of the term "national security" and required that the threat to national security has some reasonable basis in facts and clarified procedural rules, such as legal standing in the area of surveillance, the extent to

[17] https://www.amnesty.org.uk/issues/Mass-surveillance.

[18] Cf. case *Szabo and Vissy v Hungary*, appl. 37138/14. http://www.theregister.co.uk/2016/01/20/human_rights_court_rules_mass_surveillance_illegal/. Cf. case *Szabo and Vissy v Hungary*, appl. 37138/14.

which an individual can have an expectation of privacy, and the minimum safeguards that should be in place during surveillance[19]. Moreover, the European Court of Human Rights has many times cited the 1981 Council of Europe data protection convention (Convention No. 108[20]) principles when examining personal data processing within the scope of the ECtHR and the concept of private life.

So there is significant jurisprudence of the ECtHR on what constitutes unjustified interference in the context of secret surveillance and information gathering. Recently, this jurisprudence was collected and confirmed in a case decided by the Grand Chamber of the European Court of Human Rights — *Zakharov v Russia*[21]. Although this case analyses the Russian legal system, it has much broader scope of application, because it will be applied also in cases of other states (including EU Member States) that introduce such systems and was also recently mentioned by the Court of Justice in case C-203/15 Tele 2.

Mr. Zakharov is a publisher and a chairman of an NGO which runs campaigns for media freedom and journalists' rights. He decided to challenge the Russian system for permitting surveillance in the interests of crime prevention and national security. According to his position, the privacy of his communications and his right to privacy in general was infringed, because Russia — on the basis of Order No. 70 — required the network operators to install equipment which permitted the Federal Security Service to intercept all telephone communications and for that it was not necessary to have prior judicial authorisation. What is important — the applicant was not sure whether his phone calls were in fact tapped or not, but he just challenged the theoretical possibility. According to his understanding, the Russian law introduced the system of mass surveillance, because it facilitated blanket interception of mobile communications. His attempts to challenge this at the national level and to ensure that access to communications was restricted to authorised personnel were unsuccessful in Russia, therefore the matter was brought before the European Court of Human Rights. Mr. Zakharov argued that the laws relating to monitoring and interception of communication infringed his right to private life under Article 8 of the ECHR, as well as — since some parts of these laws are not accessible and there are no effective remedies — also infringing Article 13 of the ECHR.

The European Court of Human Rights, when deciding the case, first had to deal with the problem of admissibility of the case, which is very interesting. The applicant claimed that there had been an interference with his rights as a result of the mere existence of legislation permitting covert interception of mobile telephone communications as well as risk of being subjected to interception measures, rather than as a result of any specific interception measures applied to him. The Court

[19] Cf. cases *Klass v Germany*, *Copland v UK*, *Weber and Saravia v Germany*, *Z. v Finland* etc.

[20] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981.

[21] Appl. 47143/06, *Zakharov v Russia*.

noted that the contested legislation institutes a system of secret surveillance under which any person using mobile telephone services of Russian providers can have his or her mobile telephone communications intercepted, without ever being notified of the surveillance. To that extent, the legislation in question directly affected all users of these mobile telephone services. Therefore, the applicant was entitled to claim to be the victim of a violation of the Convention, even though he was unable to allege that he has been subject to a concrete measure of surveillance in support of his application. For the same reasons, the mere existence of the contested legislation amounts in itself to an interference with the exercise of his rights under Article 8 of the ECHR.

When analysing the challenged law, the ECtHR found it very important that the challenged measure must be based in domestic law and the Court noted that: "… domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures". The ECtHR referred to a long body of jurisprudence relating to surveillance, which recognises the specific nature of the threats that surveillance is used to address. While the precision required of national law regulating surveillance (both targeted and large-scale) might be lower than the normal standard, the risks of abuse and arbitrariness are clear, so the exercise of any discretion must be laid down by law both as to its scope and the manner of its exercise. The Court noted that prior judicial authorisation was an important safeguard. It gave examples of other minimum safeguards and produced a list of what should be regulated in the national law:

— the nature of offences which may give rise to an interception order,

— a definition of the categories of people liable to have their telephones tapped,

— a limit on the duration of telephone tapping,

— safeguards and procedures for use, storage and examination of resulting data,

— safeguards relating to the communication of data to third parties,

— circumstances in which data/recordings must be erased/destroyed.

The Court then considered the principles for assessing whether the intrusion was "necessary in a democratic society", highlighting the tension between the needs to protect society and the consequences for this society of the measures taken to protect it.

Since the European Court of Human Rights just collected its previous findings it could be understood as emphasising in its judgment by repeated reference to its earlier extensive case law on surveillance that there is nothing to be added. However, the situation seems to be completely different: the Grand Chamber reaffirmed and highlighted points made in the previous judgments about the dangers of surveillance and the risk of abuse. This, together with the timing of the judgment, is also significant, because *Zakharov* was handed down as the drafts of acts in various

EU Member States (UK — Investigatory Powers Bill, Poland — the amendment to the Police Act etc.) were published. If the rules from *Zakharov* were applied by the ECtHR to mass surveillance currently operated in other European states, many systems might be hard to justify.

At the EU law level, the rights to privacy and data protection are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU. The right to data protection is also laid down in Article 16 of the Treaty on the Functioning of the EU and in Article 39 of the Treaty on the European Union. In addition, secondary legislation adopted earlier than the Charter protects this right. Relevant legal instruments include Regulation 2016/679[22] (which replaces Data Protection Directive 95/46/WE) and Directive 2016/680[23], e-Privacy directive 2002/58/WE[24] and some other secondary law acts. These instruments ensure, among others, that in their respective scope of application, the processing of personal data is carried out legally and only to the extent necessary for the fulfilment of the legitimate aim pursued. These rights extend to all persons, whether they are EU citizens or third-country nationals. According to Article 52(1) of the Charter, any limitation to this right must be necessary and proportionate, genuinely meet the objectives of general interest recognised by the Union, be provided by law and respect the essence of such rights.

The applicability of these instruments in the field of security is, however, subject to specific legal and policy framework in the area and particularly to the national security exemption. Article 4(2) of the TEU provides that "national security remains the sole responsibility of each EU Member State". This exemption is reiterated in Article 2 para 2 of the new General Data Protection Regulation, which states that this Regulation does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law[25]. Since, according to Article 72 of the Treaty on the Functioning of the European Union which states that the maintenance of law and order and the safeguarding of internal

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, pp. 1–88.

[23] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–131.

[24] 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, 31.07.2002, pp. 37–47 (as amended).

[25] Cf. also Article 2 para 3 of Directive 2016/680.

security is the responsibility of the Member States, the limits of application of both acts should be decided.

The limits of national security exemption are subject to debate, including in relation to the activities of intelligence services. There is no uniform understanding of national security across the EU. The concept is not further defined in EU legislation or in the Court of Justice of the European Union (CJEU) case law, although the CJEU has stated that exceptions to fundamental rights must be interpreted narrowly and justified[26]. The CJEU has also stated that the mere fact that a decision concerns state security does not render EU law inapplicable[27].

The lack of clarity on the precise scope of the national security exemption must be analysed together with a not clearly drawn line between the areas of law enforcement and national security in the Member States. Terrorism and counter-terrorism actions are good examples, since terrorism is generally considered a threat to both national security and law and order. As a result, the division of competences among intelligence and law enforcement authorities throughout the EU Member States varies a lot. There are also differences in the schemes of information exchange which make it particularly impracticable and ineffective, weakening the mutual trust which is also one of the basic theoretical rules of cooperation between responsible services in the European Union.

As the EU Agency for Fundamental Rights correctly pointed out in its report, "this unclear delineation of 'national security' also has consequences for the applicability of EU law, which depends both on the interpretation of the national security exemption's scope and on the specific characteristics of the various surveillance programmes carried out by specific services"[28]. Anyway it is clear that — although the existence of mass surveillance programmes may be fully unknown — some of them surely contain elements that can justify the full applicability of EU law. For instance, when EU companies transfer data to intelligence services, they are considered under the General Data Protection Regulation (or Directive 95/46/WE) as data controllers who collect and process data for their own commercial purposes. Any subsequent data processing activities, such as transfer of personal data to intelligence services for the purpose of the protection of national security, will therefore fall within the scope of EU law[29]. Any limitations of the rights to privacy and personal data protection should be examined according to Article 52(1) of the Charter. Such limitations are to be treated as exceptions to the protection of personal data, and thus subject to narrow interpretation and requiring proper

[26] Cf. case C-387/05 *European Commission v Italian Republic*, ECLI:EU:C:2009:781.

[27] Cf. C-300/11 *ZZ v Secretary of State*, ECLI:EU:C:2013:363.

[28] Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' Legal Framework, European Union Agency for Fundamental Rights 2016, p. 11.

[29] Cf. C-362/14 *Schrems*, ECLI:EU:C:2015:650.

justification. The essence of the right to privacy and protection of personal data shall at any rate be respected.

Moreover, in the case *ZZ v Secretary of the State of Home Department*[30] the CJEU confirmed that the provision of effective judicial review is a central component even within the scope of Member States' measures adopted on the basis of "State security". The CJEU was of the opinion that "although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable".

Therefore, the national security exception cannot be seen as entirely excluding the applicability of EU law.

As it has already been mentioned, in case of EU legislation, as well as in case of EU Member States adopting national laws when applying EU law, provisions of the EU Charter of Fundamental Rights should also be considered. The EU Charter has been recognised as having the same legal value as the Treaties since the entry into force of the Lisbon Treaty. The EU Charter comes along a set of EU general principles some of which have their origins in national constitutional traditions and others have been further developed by the CJEU jurisprudence. And although the CJEU pointed out in the *Fransson* case that "outside the scope of EU law" national authorities and courts remain free to apply national standards of protection of fundamental rights, provided that the level of protection offered by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European law are not compromised[31]. The CJEU in this way held that the EU Charter is becoming a constitutive component of "the national constitutional traditions" of EU Member States.

But there are also cases in which the Court of Justice referred to mass surveillance directly and applied the Charter, finding the necessary link which allows for control of conformity of national law with the standards from the Charter. In the *Digital Rights Ireland* case[32], the CJEU has given a judgement in the challenge taken by Irish NGO to the EU's regime of data retention (at that time regulated by Directive 2006/24/EC[33]) and mass surveillance. The Court has found that data retention "entails particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data" and that it "entails an

[30] Cf. C-300/11 *Z.Z. v Secretary of the State Home Department*, ECLI:EU:C:2013:363.

[31] Cf. judgment of the Court (Grand Chamber), 26 February 2013, *Åklagaren v Hans Åkerberg Fransson*, ECLI:EU:C:2013:105.

[32] Cf. judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others,* ECLI:EU:C:2014:238.

[33] 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 and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54–63.

interference with the fundamental rights of practically the entire European population". The Court stated that the interference caused by Directive 2006/24/EC with the fundamental rights laid down in Articles 7 and 8 of the Charter is wide-ranging, and it must be considered to be particularly serious. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance. It should also be noted that recently the CJEU decided in another case — Tele 2[34] — where the national court asked whether the *Digital Rights Ireland* ruling applies to national data retention schemes. Applicants in case C-698/15 argued that Dripa (the Data Retention and Investigatory Powers Act 2014) permits the police and security services to spy on citizens without sufficient privacy safeguards. They maintained that the legislation was incompatible with Article 8 of the ECHR and Articles 7 and 8 of the Charter. They also complained that the use of communications data was not limited to cases involving serious crime, that individual notices of data retention were kept secret, and that no provision was made for those under obligation of professional confidentiality, in particular lawyers and journalists. Nor, they argued, were there adequate safeguards against communications data leaving the EU. The CJEU agreed with those arguments.

Finally, even when EU law does not apply, other international instruments do, notably the ECHR and Convention 108 and its 2001 Additional Protocol. It should be noticed that the CJEU refers to the Member States' international obligations under the ECHR when a subject matter falls outside the scope of EU law[35].

Regarding other fundamental rights that can be significantly harmed by mass surveillance, one cannot forget about freedom of speech and freedom of expression. When people are aware of mass surveillance they are more likely to self-censor their comments online. Particularly hard hit by the suppression of opinions are minority opinions. Stoycheff's study found, "the majority of those primed with surveillance information were less likely to speak out about their more nonconformist ideas, including those assessed as less likely to self-censor based on their psychological profile"[36]. The Oxford study also found that "people were afraid to read articles about those topics because of fear that doing so would bring them under a cloud of suspicion". The study further showed that "users were less likely to search using search terms that they believed might get them in trouble with the U.S. government" and that these "results suggest that there is a chilling effect on search behavior from government surveillance on the internet".

---

[34] Cases C-203/15 and C-698/15 Tele 2, ECLI:EU:C:2016:970.

[35] Cf. case C-127/08 *Metock*, ECLI:EU:C:2008:449.

[36] E. Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", *Journalism & Mass Communication Quarterly* 2016, no. 1, pp. 1–16.

It is clear that the violation of privacy through surveillance has the direct effect of causing suppression of freedom of speech and the freedom of expression. Suppression of these key rights often causes disproportional effects on minorities, including religious and ethnic/racial minorities. We have seen this in history, as activists and disfavoerd minorities have been targeted. Metadata and mass surveillance purports to be indiscriminate in the information they picks up, but the way the data are used carries a high risk that minorities and minority opinions are the most likely to suffer from the use of mass surveillance. These instances show that mass surveillance infringes on the right to equal treatment.

The right to fair trial is also jeopardized by mass surveillance due to the high probability that in the blanket gathering of data a number of privileged emails and communications between a lawyer and client would be collected. These communications often contain advocacy strategies and weaknesses in facts or legal arguments that may not be known to one party, and if known to the adversarial party could severely disadvantage the other, especially if the State is a party.

Mass surveillance also allows for the collection of GPS data that reveals a person's common locations in significant detail. The right to security of person is undermined when the government is collecting tracking data on a person. If this information and data is disclosed to a person intending to abuse it and the security of an individual is significantly reduced.

Through the suppression of rights and causing self-censorship we see the fundamental democratic governance deteriorating.

POLISH LEGISLATION — THE "SURVEILLANCE LAW"

In Poland the parliament has passed the Act which in fact introduces provisions allowing for large-scale surveillance. It is the Act on the amendment of the Act on the Police and several other acts, adopted on 15th January 2016. The Act admitted the police and other services (Border Guard, Fiscal Control, Military Police, Internal Security Agency, Central Anticorruption Bureau and others) the right to obtain telecommunication, postal or Internet data (which however cannot constitute the content). This right has been granted for the prevention of or detection of crimes or for the purpose of saving human life or health, or the support of search or rescue operations. It does not have to be connected to any particular proceeding or investigation. The measures envisaged in the law expand access to telecommunication and other digital data and allow for greater surveillance by the police and other agencies.

Key problems include the use of intrusive surveillance measures on the basis of vague conditions and unspecified catalogue of crimes, as well as the use of surveillance tools that capture online data, that collect and analyse personal data of an Internet user, without the obligation to submit an application before each

instance of data collection. The law does not contain a requirement of obtaining prior approval from a judge or other independent authority for collecting telecommunication and online data. Moreover, it is practically impossible for people to find out whether they are being unlawfully spied on, or to expose abuse of surveillance powers, since the law does not contain an obligation to notify targeted persons following the conclusion of surveillance.

It should be noted that the law was controlled by the Venice Commission, which on 10th June 2016 adopted its recommendations and stated that procedural safeguards and material conditions set in the Police Act for carrying out secret surveillance in some respects are still insufficient to prevent excessive use and unjustified interference with individual privacy. The opinion — requested by the Council of Europe's Parliamentary Assembly — focused on two provisions of the Act: Article 19 regulates "classical" surveillance measures, such as wire-tapping. Article 20c describes the collection of "metadata", which refers to all data connected to tele- and Internet-based communication, from websites visited to localization of cell phone use. The Venice Commission considered that some types of metadata are so sensitive that obtaining such data should require judicial authorisation, by analogy with "classical" surveillance. For accessing other, less sensitive, types of metadata judicial warrant may not be necessary, but the law should put in place a system of effective subsequent oversight of specific metadata monitoring operations by an independent body. The existing system of "generalized reporting" to a court every six months is inefficient. The Venice Commission recommended some amendments to the law, from which the most important seems to be the establishing of an effective mechanism of oversight of specific operations by an independent body[37].

CONCLUSION

Even if intelligence or security activities are said to remain within the scope of Member States' exclusive competences in the EU legal system, this does not necessarily means that Member States' surveillance programmes are entirely outside the remits of the EU's intervention. Both the European Convention on Human Rights and the EU Charter of Fundamental Rights could play a significant role here, especially given the fact that, from a legal point of view, EU surveillance programmes are incompatible with minimum democratic rule-of-law standards and compromise the security and fundamental human rights of citizens and residents in the EU.

Intelligence services have adopted several strategies to avoid the accusation of privileging security over liberty, but the mass surveillance programmes (general

[37] For other recommendations see the full text of the Opinion, available at http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e.

or even more — targeted) do not stand outside the realm of EU intervention but can be analysed from the EU law perspective via i) an understanding of national security in a democratic rule of law framework where fundamental human rights and judicial oversight constitute key norms, ii) the risks posed to the internal security of the Union as a whole as well as the privacy of EU citizens as data owners and iii) the potential clash with the obligations arising from the Charter of Fundamental Rights.

Most European services involved in the fight against terrorism and organised crime have used the large-scale collection of metadata as a way to "connect the dots" between the activities of suspects in criminal investigations. They have used surveillance in order to reconstitute networks of possible suspects associated with their main target, drawing both on real-time and stored data. In this case, even if large-scale collection is taking place, it may be considered as 'targeted surveillance'. Based on warrants and on clear purposes that can be overseen at a later date, it can be justified. But no one should forget that various programmes involving practices of large-scale surveillance have to be carefully examined from the fundamental rights perspective. The implications are far-reaching and go beyond the traditional dilemma between the rights of citizens to data protection and the right of the state to depart from the rule of law in the name of national security. They raise questions about the fundamental character of our political regimes and the nature of sovereignty.

OCHRONA PRAW PODSTAWOWYCH W KONTEKŚCIE MASOWEJ INWIGILACJI W UNII EUROPEJSKIEJ

Streszczenie

Artykuł dotyczy kwestii problematyki „masowej inwigilacji" i potencjalnego naruszenia praw podstawowych przez programy wprowadzające tę praktykę. W artykule wyjaśnia się wstępnie samo pojęcie, a także odróżnia je od inwigilacji skierowanej wobec konkretnej osoby w związku z prowadzonym postępowaniem. Celem artykułu jest zarysowanie problemu relacji między obowiązkiem państw związanym z kwestią zapewnienia bezpieczeństwa narodowego a koniecznością ochrony praw podstawowych. Podkreśla się, że powoływanie się na względy ochrony bezpieczeństwa narodowego nie w każdym przypadku mogą uzasadniać ingerencję w prawa jednostki, a także że nie oznacza to możliwości niestosowania zasad wynikających z prawa Unii Europejskiej czy dorobku prawnego Rady Europy. Podstawowym prawem, o którym mowa w artykule, jest prawo do prywatności, ale wskazane są również inne prawa, mogące być potencjalnie naruszane przez programy masowej inwigilacji.