Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego, vol. XVI, A.D. MMXVIII

ARTYKUŁ

Marcin Rojszczak*

UK ELECTRONIC SURVEILLANCE PROGRAMMES IN THE CONTEXT OF PROTECTION OF EU CITIZENS' RIGHTS AFTER BREXIT

I. Introduction[1]

On 29 March 2017, Prime Minister Theresa May notified the Council of Europe of the United Kingdom's intention to leave the European Union (*Brexit*). In accordance with the procedure specified in Article 50(2) of the Treaty on the European Union (TEU),[2] not later than on 29 March 2019, the provisions of the treaties will cease to be binding on the UK. Until that time, it is a possible to arrange the terms of the withdrawal and conclude a withdrawal agreement which would govern future relations between the parties. Currently, the need for such an agreement and its essential elements are being intensely negotiated. Taking into consideration mutual relations between the UK and the Member States, including their strong economic relationship, it should be expected that the negotiations will be primarily centred on reaching an agreement as to the terms of access to the single market. Aside from the economic talks, the EU underscores the need to regulate the rights of individuals, especially in the fields of freedom of movement, civil rights and electoral rights. In discussion of this issue, special emphasis is placed on the legal status of EU citizens staying in the UK and the British residing in the Member States of the Union.

A matter which is directly associated with both the scope of fundamental rights and mutual relations between the UK and the EU, including the access to the internal market, is the effect of the legislation on data protection applicable in the Union to the legal situation after the Brexit. For other legislatures, the EU model of data protection is considered to be the most advanced and exemplary as regards reinforcing

* Ph.D. in Law; Institute of Legal-Administrative Studies, University of Warsaw. E-mail: marcin.rojszczak@gmail.com

[1] All internet links verified as of 1 September 2018.

[2] The Treaty on the European Union (OJ C 202, 2016, p. 13).

the right to privacy in cyberspace.[3] Legislative works carried out since 2010 resulted in the adoption and entry into force of Regulation 2016/679[4] (General Data Protection Regulation), as well as Directives 2016/680[5] and 2016/681.[6] A draft of further legislation, which is a new regulation related to the protection of privacy in the electronic communications sector and intended to replace Directive 2002/58 in the near future, is being discussed among the Member States and institutions of the EU.[7]

In light of the European data protection laws, the United Kingdom's withdrawal from the EU means that this state will cease to be a member of the internal market and will commence to be treated as a third country, to which it will only be possible to transfer data under certain conditions. This raises the particularly interesting issue of the specifics of UK secret electronic surveillance programmes.

The term "mass surveillance" is used to describe activities in which large sets of data are collected, the source of which is wiretapping of different types of communication channels. As a rule, mass surveillance is indiscriminate (all those who use a given transmission medium are subjected to control) and of a bulk nature (all the information possible to be captured is collected). In practice, mass surveillance consists in registering all or a substantial part of communications transferred via specific means of communications with a view to its further analysis. In most cases, it is a measure taken by public authorities, especially in the field of intelligence and fighting the most serious crimes. Individual surveillance is applied within criminal proceedings under external oversight (a public prosecutor, court). However, mass surveillance is deprived of such legal protection against abuse of power, because it is related to the activity of intelligence agencies. At the same time, such surveillance efforts might result in monitoring the activity of a significant part of society. Therefore, mass surveillance is of fundamental importance in regard to individual's enjoyment of basic liberties and freedoms, such as respect for privacy.

---

[3] *See* P. Schwartz, *The EU-U.S. Privacy Collision: A Turn To Institutions And Procedures*, Harvard Law Review 2013, vol. 126, pp. 1973–1974; also, G. Buttarelli, *The EU GDPR as a clarion call for a new global digital gold standard*, International Data Privacy Law 2016, no 2, pp. 77–78.

[4] 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), OJ L 119, p. 1.

[5] Directive (EU) 2016/680 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, 2016, p. 89).

[6] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 2016, p. 132).

[7] 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, 2002, p. 37.

For many years the British intelligence services have been suspected of carrying out complex mass surveillance programmes which have affected not only the communications of their own citizens but primarily electronic communications transmitted via transatlantic fibre-optic cables passing through the UK territory. According to information revealed by the US National Security Agency (NSA), the intelligence services of the United Kingdom, in particular the Government Communications Headquarters (GCHQ), which is responsible for electronic surveillance, are closely cooperating with their counterparts from other countries belonging to the so-called Five Eyes Agreement. The cooperation involves capturing, collecting and processing electronic communications.

The legal status of UK electronic surveillance programmes has been discussed for years by the representatives of various branches of science and organizations protecting human rights. The legality of UK surveillance laws has been revised by parliamentary bodies[8], national courts[9] as well as the CJEU[10] and the ECtHR.[11]

The withdrawal of the United Kingdom from the European Union will give rise to new legal circumstances. Many of the rulings passed so far will lose their relevance. Moreover, the loss of the status of a member state and, consequently, no direct applicability of the treaties will create a new situation that will enable effective regulation and restriction of the legally contested activity of the UK intelligence services as well as provide enhanced protection of the rights of EU citizens who use modern means of electronic communications.

This article discusses the issue of legal consequences which the Brexit will have for the assessment of the legality of mass surveillance programmes carried out by the United Kingdom. For this purpose, the current legal framework for the activities of UK intelligence services will be first presented. This will be followed by an analysis of possible effects which the UK's withdrawal from the Union may have on the issues in question, from the perspective of both British and EU law, taking into account the European human rights system.

---

[8] The activities of UK intelligence services, including GCHQ, are subject to oversight by the Intelligence and Security Committee of Parliament. The Committee publishes annual summaries as well as special reports on selected topics. The problems of mass surveillance programmes were discussed, among others, in a statement on the cooperation of GCHQ with the NSA published in July 2013 (http://cli.re/L2Aq2o) and in a report on the access of authorised agencies to communications data published on 5 February 2013 (http://cli.re/gYVkqa).

[9] *See* for example the judgment of the High Court of Justice of 17 July 2015, [2015] EWHC 2092 – compliance of the UK surveillance regulations with EU law.

[10] *See* for example judgment of the CJEU of 21 December 2016 r. in case *Tele2 and Watson*, C-203/15 and C-698/15 – the rules of access to electronic communications data by competent national authorities.

[11] *See* for example judgment of ECtHR of 18 May 2010 in the case *Kennedy v. United Kingdom*, 26839/05 – the rules of conducting secret surveillance programmes by public authorities.

II. The Five Eyes Agreement and current UK's electronic surveillance programmes in the context of EU law

To understand the specifics of British electronic surveillance programmes, it is necessary to determine whether and to what extent the activities of the GCHQ may lead to a violation of EU residents' privacy and what the scale of this interference is. In order to answer this question, it is necessary to discuss the legal basis of transferring electronic surveillance data to third countries and to juxtapose this basis with the foundations of EU law.

Upon the end of the Second World War, the United Kingdom and the United States agreed on the terms of intelligence cooperation in respect of communication intelligence programmes. The first agreement was concluded in 1946[12] and initiated the intelligence cooperation of both countries which has been continued to date. In the 1950s, further states acceded to the agreement, i.e. Australia, New Zealand and Canada.[13]This agreement and the ones concluded subsequently by the same parties are often referred to as the 'Five Eyes Agreement' (FVEY). The established intelligence cooperation enabled the creation of a global system of intercepting radio and telephone communications, and then internet surveillance. A widely discussed project carried out within the FVEY was a system of electronic interception named Echelon.[14]

Each of the parties involved created an intelligence service responsible for communication intelligence (COMINT)[15] activities and it was obliged to provide the other partners with access to intelligence information from foreign communication intelligence and with the possibility of exchanging the information[16]. Although the Five Eyes Agreement was created over sixty years ago, in the initial period of the Cold War it undoubtedly served to increase the effectiveness of the defence of the Western States through quick exchange of essential intelligence information. The rules of cooperation established at that time have continued to apply with almost no changes until today. Actually, surveillance techniques are being adapted, and with the

[12] British-US Communication Intelligence Agreement, 5 March 1946, http://cli.re/gnxJ7k.

[13] Although there were more countries in the FVEY partnership, only Canada, Australia and New Zealand were recognized as „participating countries of the Community" – see Article 7 of Annex J of the UK-US Communications Intelligence Agreement, 10 May 1955, http://cli.re/6kZedX.

[14] L. Sloan, *ECHELON and The Legal Restraints on Signals Intelligence: A Need for Reevaluation*, Duke Law Journal 2001, vol. 50, p. 1467–1510.

[15] In the case of the United States, it was the NSA, the United Kingdom – GCHQ, Australia – ASD (Australian Signals Directorate), Canada – CSE (Communications Security Establishment), and New Zealand – GCSB (Government Communications Security Bureau).

[16] Despite the broad definition of the term „foreign communication" used in the agreement of 5 March 1946, there is no doubt that the scope of the agreement covered only information on foreign governments, individuals and persons acting on their behalf (see the definition on page 3 of the agreement referred to in footnote 14). Both in the agreement of 5 March 1946 and in subsequent agreements (which were disclosed), the term „foreign communication" has not been defined in a way that allows acceptance that any electronic communication – regardless of its nature – can be transferred to foreign services as part of the FVEY partnership.

development of the Internet and information society services, they allow for the collection of increasingly extensive data sets and their immediate cross-border transfer to foreign partners.

According to information revealed in recent years, it is possible to estimate the extent of activities carried out by the GCHQ. One of the main communication intelligence programmes is Tempora, which involves the interception of communications transmitted through approximately 200 transatlantic fibre-optic cables.[17] Owing to its geographical location, a large part of international telecommunications traffic (including Internet traffic) between Europe and North America is transmitted via connections passing through the UK territory. This enables the GCHQ to capture huge quantities of data, including voice calls, users' data and files, email messages and instant messengers. Due to the extent of the data available and existing technical limitations, the GCHQ must use pre-selectors which allow for the limitation of the communications captured. This mode of activity is mistakenly raised as evidence that the Tempora is actually not a mass surveillance programme[18]. The scale of collected data is enormous, as also demonstrated by the fact that approx. 300 technicians have been assigned by the GCHQ for preliminary analysis and sorting of information.[19]

Data obtained by wiretapping fibre-optic communications are not the only source of information for British secret surveillance programmes. The GCHQ closely cooperates with the NSA, including other programmes such as Muscular, in which both agencies intercept internet communications coming from Google and Yahoo data centres located in the United Kingdom. In turn, under the Optic Nerve programme carried out jointly by both intelligence agencies, images and relevant personal data received from Yahoo webcam users have been registered on a massive scale. According to documents disclosed by E. Snowden, during only six months of 2008, photographs from more than 1.8 million Yahoo users' accounts were obtained in this manner.[20] Surprisingly, according to the GCHQ, about 7% of the pictures were of an intimate nature, part of which were clearly erotic.[21] The Optic Nerve programme was of an indiscriminate nature, which means that all user's photographs were obtained regardless of whether a person was suspected of any criminal activity or not.

Data obtained by the GCHQ are shared with other agencies as part of the Five Eyes Agreement. A detailed scope of cooperation is not known, and it may only be analysed on the basis of publicly available documents and information disclosed by whistle-blowers such as E. Snowden. As far as the Tempora is concerned, the monitoring is actually aimed at traffic transmitted outside the EU which might there-

---

[17] *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, 21 July 2013, https://goo.gl/FCsrUd.

[18] *Privacy and Security: A modern and transparent legal framework*, The Intelligence and Security Committee of Parliament 2015, http://cli.re/LKaJXd, p. 28.

[19] *GCHQ taps fibre-optic*….

[20] *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*, The Guardian, 28 February 2014, http://cli.re/Lmrj8p.

[21] *OPTIC NERVE – Yahoo Webcam display and target discovery*, GCHQ, December 2018, http://cli.re/LX8adR, p. 3.

fore also be intercepted by other states through whose territory the transfer passes. However, in the case of the Muscle programme, data which have not left the area of the UK are transmitted to a third country. This leads to a situation in which one of the Member States, operating within the common market of information processing, subjects the electronic communications of a significant part of EU citizens to surveillance, and then transfers the data thus obtained outside the EU, to intelligence services of a third country.

The protection of personal data constitutes one of the fundamental rights guaranteed directly by the treaties (Article 16 of the TFEU[22]) and the provisions of the Charter of Fundamental Rights of the EU (CFR).[23] Previous considerations lead to the conclusion that the EU's model of privacy protection is one of the most developed in the world which means that the scale and massive nature of the British government's activities may be perceived as a clear example of violating European standards in the field of data protection. There are two major reasons why the abovementioned situation is possible in the current legal circumstances, where the UK is still a member state. One reason concerns mutual relations between the treaties and international agreements entered into by the Member States. The other refers to the scope of the application of EU law, in particular the national security exception.

The Five Eyes Agreement (formally an intergovernmental agreement[24]) was concluded before the entry into force of the Treaties of Rome and the establishment of the European Economic Community,[25] and obviously before the date of the UK's accession to the EEC.[26] This results in the applicability of Article 351 of the TFEU, pursuant to which the provisions of the treaties shall not affect the rights and obligations arising from agreements concluded before the date of accession. The discussed Article does not stipulate any time limit for the adaptation of the provisions arising from such agreements to the obligations under the treaties. It merely states that the Member States concerned "shall take all appropriate steps to eliminate the incompatibilities established." The contracting parties did not specify *a priori* any precedence of the relations within the EU over international agreements concluded by the Member States prior to the date of accession.

It should be borne in mind that the Five Eyes Agreement may be interpreted as a formal basis for the transfer of information by security services (including intel-

[22] The Treaty on the Functioning of the European Union, consolidated version – OJ C 202, 2016, p. 47.

[23] The Charter of Fundamental Rights of the European Union (OJ C 202, 2016, p. 389).

[24] As already indicated, the term Five Eyes is used to describe an intelligence community operating on the basis of a series of agreements that are characterized by different levels of formalization. The first agreement of 5 March 1956, was signed by STANCIB (State-Army-Naval Communication Intelligence Board) and LSIB (London Signal Intelligence Board) – intelligence bodies acting on behalf of US and UK authorities.

[25] The Treaty of 25 March 1957 establishing the European Economic Community (CELEX: 11957E/TXT).

[26] Which took place on 1 January 1973 on the basis of Article 2 of the Treaty of 22 January 1972 on the accession of Denmark, Ireland, Norway and the United Kingdom to the European Communities (CELEX 11972B/TXT).

ligence services), but not of its collection. Therefore, even if the exception provided for in Article 351 of the TFEU were deemed to apply to the transfer of data to foreign partners in performance of an agreement preceding accession, the sole activity of bulk interception and analysis of electronic communications could not be legitimised in this manner.

Until recently, in domestic legislation, the legal basis of the collection and processing of surveillance data by public authorities, including the GCHQ, was the Regulation of Investigatory Powers Act of 2000 (RIPA) and the Data Retention and Investigatory Powers Act of 2014 (DRIPA)[27]. As a result of its judicial review, the provisions of the DRIPA were declared incompatible with EU law on 17 July 2015.[28] At the same time, a national court ruled that the contested provisions lose force as of 31 March 2016, thus providing time for the legislature to comply with the wording of the judgment.[29] In effect, the provisions of DRIPA were replaced by the Investigatory Powers Act (IPA)[30] of 29 November 2016, which entered into force on 30 December 2016.

In the judgment *Tele2 and Watson* of 21 December 2016, the CJEU ruled that the provisions of DRIPA which did not limit the access of public authorities to electronic communications metadata solely to cases involving the detection of serious crimes were incompatible with EU law.[31] Moreover, the Court indicated that the absence of the obligation to store those data within the Union may not be reconciled with the requirements of Directive 2002/58 and the Charter of Fundamental Rights.[32] Although initially the UK government stressed that the solutions adopted in the IPA were compatible with EU law, later it presented a draft of amendments to the Act, pointing out that "some aspects of our current regime for the retention of and access to communications data do not satisfy the requirements of the CJEU's judgment."[33]

The case-law of the Investigatory Powers Tribunal (IPT) should also be highlighted in the analysis of the UK's domestic law. This is a specialised court competent to hear cases related to complaints against the application of secret surveillance techniques. Considering a complaint filed by Privacy International, the IPT resolved that the activities of the GCHQ within the Tempora programme did not lead to a violation of domestic law and obligations arising from the ECHR.[34] However, when

---

[27] The Regulation of Investigatory Powers Act, 2000 c. 23, http://cli.re/gVqQ2J; the Data Retention and Investigatory Powers Act, 2014 c. 27, http://cli.re/gYn1vA.

[28] The judgment of the High Court of Justice of 17 July 2015, [2015] EWHC 2092, http://cli.re/gKWkdZ.

[29] The order of the High Court of Justice of 17 July 2015, CO/3665/2014 and CO/3667/2014, http://cli.re/G5B9VL, para 3.

[30] The Investigatory Powers Act, 2016, c. 25, http://cli.re/6BRv8A.

[31] *Tele2 and Watson* case, para 120.

[32] *Tele2 and Watson case*, para 122.

[33] *Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data*, The Home Office 2017, http://cli.re/6DykyM, p. 2.

[34] Investigatory Powers Tribunal rules GCHQ mass surveillance programme TEMPORA is legal in principle, Privacy International, 18 December 2014, http://cli.re/65rB2B.

considering another case regarding the legality of investigative powers arising from the IPA on 30 October 2017, the Tribunal decided to refer a request to the CJEU for its preliminary ruling. The first question that was posed is a fundamental one: "does a requirement (...) to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies (SIAs) of a Member State fall within the scope of Union law?"[35]

The CJEU's answer to this legal issue will be crucial to determine the limits of the European Union's competencies in the area of mass surveillance programmes, and thus to ensure the effective protection of the rights arising from the Charter of Fundamental Rights.

In accordance with the principle of conferral, the scope of the application of EU law encompasses exclusively the powers expressly set out in the EU treaties. Because initially the Union (formerly the EEC) was perceived as an organization established for the purpose of strengthening economic cooperation, issues related to the protection of public security, defence, state security and cooperation of law enforcement agencies were excluded from the scope of the application of EU law. With the entry of the Lisbon reform into force and the abolition of the division into three pillars of integration, the tasks related to territorial integrity, maintaining public order and protecting national security were defined as the tasks constituting the main functions of the state.

Moreover, pursuant to Article 4(2) of the TEU, "national security remains the sole responsibility of each Member State." This exception applies to all EU law, including all secondary legislation, such as the provisions enacted in the area of the protection of privacy (e.g. Regulation 2016/679 or Directive 2016/680). Although the term "national security" has not been precisely defined neither in EU law or the case-law of the CJEU (which stresses the necessity of using such terms in a restrictive manner[36]), in the present legal circumstances the prevailing standpoint is that the operation of authorised bodies in the field of intelligence information collection is not governed by EU law.[37] The electronic surveillance programmes carried out by the GCHQ should also be deemed as such. Examining the questions referred by IPT for

---

[35] The application for a preliminary ruling from the Investigatory Powers Tribunal made on 31 October 2017 in the case *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, C-623/17, p. 1.

[36] *Cf.* the judgment of the CJEU of 6 November 2003 in the case *Lindqvist*, C-101/01, para 44. The issue of ambiguity related to the understanding of the term "national security" also became the reason for the reference for a preliminary ruling made by the Irish court (The High Court) in the course of case 2016/4809/P ([2017] IEHC 545, http://cli.re/6n32nd, paras 339–340). The first question posed in the application request of 9 May 2018 (C-311/18) seems to be particularly relevant: "*does EU law (including the CFR) apply to the transfer of the data notwithstanding the provisions of Article 4(2) of TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive 95/46/EC3 ("the Directive") in relation to public security, defence and State security?"*

[37] *See generally*, the working document of the WP29 on surveillance of electronic communications for intelligence and national security purposes, WP 228, p. 22. Also: *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, European Parliament Directorate General for Internal Policies 2003, https://goo.gl/d6WSSE, p. 28.

a preliminary judgment in case C-623/17, the CJEU may provide a different interpretation; however, it is unknown whether the Court's ruling will be passed before March 2019 and what impact it will have on UK legislation after Brexit.

The result of the United Kingdom leaving the EU framework will be the loss of its status as a member state and therefore, the exceptions arising from Article 351 of the TFEU and Article 4 of the TEU will no longer apply to the activities of this state. This creates a completely new situation for re-defining the principles of cooperation between the UK and the EU, including the area of creating a secure space for data processing–taking into account the dangers involved in extensive surveillance programmes carried out by the British authorities and affecting EU citizens.

III. The free movement of data from the EU territory in the light of Brexit

The EU and third countries cooperate in the area of the trans-border flow of data and the establishment of a secure space for their processing on three main levels: (i) facilitating economic cooperation, (ii) cooperation in the field of criminal law and (iii) the prevention of tax evasion and the financing of terrorism. As regards the first level, the main applicable instruments are Resolution 2016/679 and Directive 2002/58, which are the primary sources of the standards of privacy protection in cyberspace. The principles of the cooperation of justice system authorities are governed by Directive 2016/680. Finally, the issues of the prevention of tax evasion and combating the most serious of crimes are elaborated on in the provisions of Directive 2016/1164.[38] Aside from the enactment of secondary legislation, the Union may exercise its competences through the conclusion of international agreements. For instance, there are agreements concluded between the United States and the European Union on the exchange of data in the field of the detection and prevention of crime,[39] the exchange of PNR data[40] and the transfer of financial data as part of fighting terrorism.[41]

The regulations which form the basis of transferring commercial data to third countries are the most significant for the present analysis. Based on these laws, companies offer services that rely on the transfer of data for processing outside the EU. Examples include all the major social networks, file storage, storage of photographs, email or instant messengers. All of these services could not be properly provided

[38] Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market (OJ L 193, 2016, p. 1).

[39] The Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (OJ L 25, 2016, p. 1).

[40] The Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (OJ L 215, 2012, p. 5).

[41] The Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (OJ L 195, 2010, s. 5).

without cross-border data transfer to data processing centres located outside the EU, mostly in the United States. Currently, the basis of such transfer is Regulation 2016/679, which was preceded by the provisions of Directive 95/46, applicable for over twenty years.

While EU legislation provides a few modes leading to the possibility of cross-border data transfer to third countries, the so-called decisions on the adequacy of the level of protection are of the greatest practical significance. The decisions are issued by the EC and they confirm that the legislation and international obligations of a third country are sufficient to ensure that personal data transferred from the EU will be processed in a manner ensuring an appropriate level of protection, not lower than that arising from EU law. Decisions on adequacy are the basis of data transfers to a given third country, without the necessity of implementing additional protection mechanisms.

The General Data Protection Regulation has significantly extended the rules of issuing such decisions and monitoring whether the decisions are up to date. Compared to the provisions of Directive 95/46, an obligatory mechanism of regular reviews has been introduced. The reviews may not be carried out less frequently than once in four years and their function is the verification of whether the basis of a decision is still up to date. Moreover, the criteria of evaluating the legislation of a third country have been enhanced, clearly indicating that for the recognition of the equivalence of protection it is necessary to determine that relevant legislation ensures respect for human rights and fundamental freedoms also "concerning public security, defence, national security and criminal law and the access of public authorities to personal data."[42] Therefore, in the analysis of the legal system of a third country, the Commission is obliged to consider the method of protecting fundamental rights, including the right to privacy, against illegitimate interference by the authorities responsible for ensuring public security.

Failure to comply with this obligation led the CJEU to declare the invalidity of an adequacy decision issued by the EC with regard to the United States, which was also connected with the termination of the transatlantic data exchange programme *„Safe Harbor*."[43] In its ruling, the Court found it unacceptable to allow for a situation where legislation of a third country (the USA in this case) stipulates absolute precedence of national security requirements over the principles arising from a decision on adequacy.[44]

---

[42] *See* Article 45(2a) of the Resolution 2016/679.

[43] See generally, M. Rojszczak, *Skuteczność ochrony praw podmiotów danych wynikających z prawa Unii Europejskiej w świetle umowy Tarcza Prywatności oraz prawodawstwa federalnego USA, Transformacje Prawa Prywatnego* 2018, no 1, p. 111–133; Also: A. Börding, *Safe Harbor: The Decision of the European Court of Justice* [in:] T. Hoeren T., B. Kolany-Raiser B. (eds), *Big Data in Context,* Springer 2018; D. Svantesson, *Cross-Border Data Transfers after the CJEU's Safe Harbour Decision: A Tale of Gordian Knots*, Alternative Law Journal, vol 41, pp. 39–42; Philipp E. Fischer, *Getting Privacy to a new Safe Harbour. Comment on the CJEU Judgment of 6 October 2015, Schrems v Data Protection Commissioner*, JIPITEC 2015, vol 6, pp. 229–233.

[44] The judgment of the CJEU of 6 October 2015 in the case *Schrems v. DPC*, C-362/14, para 86.

This means that the laws of a third country that allow for unlimited interference with the sphere of EU citizens' privacy are irreconcilable with the norms of EU law.

Consequently, there are no grounds for the recognition of adequacy (equivalence) of the legal system assessed and the legislation of the Union. However, related to the EU-USA relations and the analysis of the US legal system, these arguments may clearly be applicable to the assessment of the UK regulations forming the basis of the GCHQ's mass surveillance programmes. Therefore, it seems likely that the extensive British electronic surveillance programmes may in the long term become an obstacle to the establishment of the rules of secure data exchange between the EU and UK based on the mechanism of decisions on the adequacy of protection. This scenario seems even more likely because the CJEU, in its judgment in *Tele2 and Watson*,[45] ruled that the existing UK legislation imposing the general data retention obligation on communications service providers may not be reconciled with EU law since it entails a disproportionate violation of the right to privacy of a large part of society. V. Mitsilegas, one of the experts surveyed as part of the analysis ordered by the UK Parliament on the effects of Brexit on the data protection sector, said that "as long as domestic law allows for mass surveillance programmes, we will have a compatibility problem with EU law."

An alternative to the abovementioned scenario is basing the data exchange mechanism not on a decision on adequacy issued under Article 45 of Regulation 2016/679, but on individual arrangements arising from a withdrawal agreement concluded pursuant to Article 50(2) of the TEU. A withdrawal agreement is negotiated on the basis of the European Council's guidelines and concluded on behalf of the Union. Thus, the European Union is party to it, not particular Member States. Consequently, although the agreement contains individual arrangements in respect of the withdrawal of the state's future relations with the Union, it may not set forth solutions incompliant with the treaties. Yet, it is possible to establish deviations from the application of secondary law in a withdrawal agreement (e.g. in respect of the issuance or validity of decisions on adequacy concerning the UK).

Additionally, there are no obstacles for the agreement itself to replace a decision on adequacy, thus being the formal basis of the transfer of data. However, it is unacceptable for this agreement to introduce solutions contrary to the provisions of superior laws, which in the legislation of the EU are both the treaties and the Charter of Fundamental Rights. Namely, while a withdrawal agreement is a more flexible legal tool to regulate future relations of the parties, including the exchange of data, in practice, strong emphasis on the right to privacy in the primary legislation means that the validity of the arrangements made in this agreement will be verified against the same standards as decisions on adequacy. Notably, the Court declared the Commission's decision invalid in the case *Schrems* not on the basis of Directive 95/46, but pursuant to the underlying norms of the Charter of Fundamental Rights, whose force in the EU legal system is equal to the treaties.

[45] *Brexit: the EU data protection package*, The European Union Committee of the House of Lords 2017, http://cli.re/6DMrJn, para 139.

Regardless of the method of regulating future mutual relations, the withdrawal of the United Kingdom from the European Union shifts the debate on the legality of British surveillance programmes from analysing possible violations of EU law by a member state to assessing if the British legal system guarantees a suitable degree of protection of personal data transferred to the UK. Furthermore, in this case, the EU institutions will not be limited by the scope of the application of EU law and, therefore, they will be able to address their expectations to foreign partners regarding the implementation of effective legal safeguards embodying the principle of proportionality of electronic surveillance programmes.

IV. The possibility of assessing UK surveillance programmes by the ECtHR in the light of the Brexit

All Member States of the EU are parties to the ECHR[46]. The status of the Convention and judgments issued by its judicial body has been reinforced by Article 6 (1) of the TEU, stipulating that the fundamental rights guaranteed in the ECHR are part of EU law as general principles of law. In turn, pursuant to Article 52 (3) of the Charter of Fundamental Rights, the meaning and scope of the rights guaranteed by the ECHR will be the same. This provision applies, in particular, to the right to privacy, which in both instruments was formulated in an equivalent manner (*see* Article 8(1) of the ECHR and Article 7 of the CFR).

At the same time, the ECHR does not contain an exception related to national security (counterpart to Article 4(2) of the TEU). Hence, the competence of the ECtHR is not limited, and it may investigate complaints associated with the conduct of secret surveillance programmes by the states being parties to the Convention. The Court has undertaken the assessment of the legality of public authorities' actions resulting in the collection of excessive data on individuals a few times. As a result, it has developed its own test used to assess whether the analysed measures of interference with individuals' privacy are compatible with law and necessary in a democratic society.[47] This test was used *inter alia* to determine violations of obligations arising from the Convention by the authorities of Russia and Hungary[48]. In both cases the provisions analysed, which formed the basis of electronic surveillance programmes, were found to violate the principle of proportionality and the rule of law. Although the Court has not ruled directly on the legality of mass surveillance programmes so far, the

[46] The Convention of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms, https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[47] M. Rojszczak, *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC* (Legal basis for mass surveillance of citizens based on wholesale and non-targeted interception of data in the EU, including the jurisprudence of the CJEU and the ECtHR), Studia Prawa Publicznego 2017, nr 2, s. 179–180.

[48] *See also* the judgments of ECtHR: of 4 December 2015 r. in the case *Zakharov v. Russia*, 7143/06; and of 12 January 2016 in the case *Szabo and Vissyv. Hungary*, 37138/14.

observance of the rule of "*strict necessity*",[49] whose importance is highlighted in the Court's case-law, may not be reconciled with the conduct of extensive electronic surveillance programmes which involve bulk interception of electronic communications of an indefinite group of individuals and potentially society as a whole.

The withdrawal of the United Kingdom from the European Union will not result in the limitation of the application of the rights and guarantees arising from the ECHR. The UK will remain a party to the Convention, which entails the necessity of respecting the judgments passed by the Strasbourg Court. In the past, the Court reviewed UK legislation in terms of its compatibility with Article 8(2) of the ECHR. In the case *Kennedy v. the UK*, one of the Court's arguments proving lack of violation of the Convention was that the UK legislation did not allow surveillance activities based on bulk and unlimited data interception.[50] The above thesis may lead, *a contrario,* to the conclusion that laws enabling public authorities to perform such activities would be deemed to be in violation of the Convention.

Nonetheless, the Brexit may facilitate the assessment of the compatibility of UK surveillance programs with the ECHR. For many years it has been pointed out that there might be a potential competence dispute between the ECtHR and CJEU as to the precedence of the case-law of either court. This particularly refers to a situation where a member state, applying EU law, is complained against for a breach of its obligations under the ECHR. Until now, the ECtHR has upheld its case-law that states being parties to the Convention may transfer part of their competences to an international organization.[51] If this organisation ensures the protection of fundamental rights equivalent to the Convention level, law enacted by it may not lead to a violation of the obligations arising from the Convention. The adoption of such jurisprudence might lead to ambiguity in assessing the lawfulness of domestic mass surveillance programmes. Although, as indicated before, the implementation of programmes of this type is outside the scope of the application of EU law and they also have impact on the area falling within the competence of the Union. As a result, the CJEU is unable to directly challenge the compatibility of states' national security activities with the treaties, but it is capable of assessing their effect on the sectors covered by EU law.[52] In turn, the ECtHR is not restricted to assess the proportionality of all public authorities' activities, including the field of national security. At the same time, such assessment may indirectly affect the application of EU law. This fragile equilibrium between the two European courts is widely discussed.[53]

---

[49] M. Rojszczak, *Prawne podstawy…*, p. 181.

[50] The judgment of the ECtHR of 18 May 2010 in the case *Kennedy v. United Kingdom*, 26839/05, para 160.

[51] The judgment of the ECtHR of 30 June 2005 in the case *Bosphorus*, 45036/98.

[52] As an example, in the *Tele2 and Watson* ruling, which is related to the general obligation to retain data (so-called data retention), the Court recognized domestic law's obligation for commercial entities to intercept all electronic communications as violating the principle of proportionality and, as a result, incompatible with the CFR.

[53] *Cf.* L. Garlicki, *Europejski Trybunał Praw Człowieka a prawo UE*, Europejski Przegląd Sądowy 2014 (European Court of Human Rights and EU law, European Judicial Review 2014),

The withdrawal of the United Kingdom from the EU will lead to a situation in which the risk of incompatible case-law of the ECHR and CJEU may not arise. The CJEU will have the right to analyse the whole legal system of the UK when examining the validity of the issuance of an adequacy decision. On the other hand, the ECtHR will be able to verify whether the activities of the UK's authorities (including security and intelligence services) do not lead to a violation of the right to privacy as guaranteed by the Convention.

Currently, the Court is hearing cases initiated by non-governmental organizations' applications in which they seek to undermine the legality of bulk and indiscriminate electronic surveillance programmes conducted by UK authorities.[54] In the case *Big Brother Watch and others v. the UK*[55] the complainants request that *inter alia* the domestic provisions on which the Tempora programme is based be declared incompatible with Article 8 of the ECHR. A similar complaint has been lodged by ten organizations active in the field of privacy protection, thus initiating the case *Amnesty International and others v. the UK*.[56] The latter case was, however, brought before the Court after exhausting national remedies before the IPT.[57] In turn, in the case *Bureau of Investigative Journalism and Alice Ross v. the UK*,[58] the complainants point out that, as a result of the interception of electronic communications by the GCHQ on a mass scale, the right to freedom of expression is being violated (Article 10 of the ECHR).[59] On 7 November 2017 a public hearing took place for all three cases. Although these complaints will be considered in accordance with the law applicable prior to the UK's withdrawal from the EU, the Court's interpretation will be important for the determination of the UK's future relations with the Union in the area of cross-border flow of personal data.

V. Conclusions

The United Kingdom's withdrawal from the structures of the European Union is a process which entails significant consequences for most sectors of economy,

---

no 1, s. 20–2; T. Lock, *The ECJ and the ECtHR: The Future Relationship between the Two European Courts*, The Law and Practice of International Courts and Tribunals 2009, vol. 8, pp 375–398; Sybe A. de Vries, *EU and ECHR: Conflict of Harmony?*, Utrecht Law Review 2013, vol. 9, pp. 78–79.

[54] *UK intelligence agencies face surveillance claims in European court*, The Guardian, 7 November 2017, http://cli.re/Lwa47b.

[55] The application to the ECtHR of 4 September 2013 , *Big Brother Watch and Others v. United Kingdom*, 58170/13.

[56] The application to the ECtHR of 20 May 2015, *10 Human Rights Organisations v. United Kingdom*, 24960/15.

[57] *Amnesty International takes UK to European Court over mass surveillance*, Amnesty International, 10 April 2015, http://cli.re/6JnkDy.

[58] The application to the ECtHR of 11 September 2014, The Bureau of Investigative Journalism and Alice Ross v. United Kingdom, 62322/14.

[59] *A summary of the Bureau's application to the European Court of Human Rights*, The Bureau of Investigative Journalism, 14 September 2014, http://cli.re/Le22JD.

including the digital market and the data processing sector. Until recently, the United Kingdom has postulated the so-called *clean break*, which consists in maintaining the current *status quo* after the Brexit. This, however, is increasingly considered to be unrealistic. The provisions of the General Data Protection Regulation lead to the reinforcement of privacy protection, also concerning extraterritorial application of EU law to processing activities carried out in third countries. The United Kingdom actively participated in the legislative work on the reform of EU data protection laws. Along with its withdrawal from the Union, these provisions will be applied to the UK as a third country, not a member state.

A practical ramification of the change to privacy protection resulting from the Brexit will be new tools allowing the European partners to exert influence on the UK with a view to limiting or changing its mass surveillance programmes. The UK government will no longer be able to take advantage of the exception provided for in Article 4(2) of the TEU and the EU institutions (including the CJEU) will be able to assess the entire UK legal system in order to verify whether it contains privacy protection measures equivalent to those applicable in the EU. Recognising the importance of this issue for building future relations, the Information Commissioner considered it likely that "the UK's surveillance and data retention regime would be a risk for a positive adequacy finding."[60]

At the same time, organizations protecting human rights which operate in the UK perceive Brexit as a threat of further expansion of security services' powers to conduct activities which violate the right to privacy.[61] The withdrawal from the EU may reduce the influence of the recent judgments passed by the CJEU in respect of disproportionate general data retention on UK legislation. At the same time, proceedings coming before the ECtHR are considered as a lengthy and ineffective measure to change domestic laws.[62]

The UK's current standpoint in the negotiations aims to base its future relations with the Union on the mechanisms arising from the General Data Protection Regulation, in particular a decision on adequacy.[63] Concerns are being raised whether it will be possible to issue such a decision in full scope or it will be limited, e.g. to the free flow and processing of data for commercial purposes (with the exception of police cooperation and cooperation in criminal cases).[64] The British government stresses that the UK, even during its membership in the European Union, carried out works

[60] *Brexit: the EU data protection package…*, para 138.

[61] *Into The Unknown: Government Surveillance After Brexit*, Privacy International, 1 December 2017, http://cli.re/LKMaY3.

[62] An example of this is the draft of a new bill presented in Hungary in August 2017, which led to the ineffective implementation of the provisions of the Court's judgment in the case *Szabo v. Hungary*. See: *Standpoint on the draft bill on secret information gathering for national security purposes*, Eötvös Károly Institute, http://cli.re/Lvd1eq. *See also* current status of execution of judgement in the ECtHR database: http://cli.re/g1XBA5.

[63] The exchange and protection of personal data: a future partnership paper, HM Government 2017, http://cli.re/Gp9Eyo, para 4.

[64] *Brexit: the EU data protection package…*, paras 140–141.

in order to adapt to the General Data Protection Regulation and is fully prepared to protect data transferred from the EU in the same manner as the one stipulated by EU law. Nonetheless, this viewpoint omits the issue of surveillance programmes, which are excluded from EU law and, therefore, are not subject to any regulation or limitation by EU institutions. Even assuming that at the moment of the UK's withdrawal its legislation will be fully compatible with the General Data Protection Regulation, the enactment of new EU regulations,[65] in the adoption of which the UK will no longer participate, may change this situation.

From the point of view of the other Member States, the withdrawal of the UK from the European Union may contribute to increased effectiveness of the European data protection model. Actually, the problem of extensive UK surveillance programmes has remained insoluble at the level of EU law. This practice has not been changed by the case law of the ECtHR, in which the lack of proportionality of such activities has been highlighted. The UK's withdrawal from the EU and basing their future relations on an adequacy decision will make it possible to solve this problem. Additionally, it could be expected that if UK legislation happens to be declared irreconcilable with EU law, this will constitute another incentive for the reform of surveillance laws in the Member States as well.

At the same time, EU residents will receive an effective tool to protect their rights, namely the possibility of filing a complaint with the CJEU regarding a future EU-UK adequacy decision.[66] So far, the case-law of the Court has led to the reinforcement of guarantees arising from the Charter of Fundamental Rights. This may be exemplified not only by the abovementioned cases of *Schrems* or *Tele2 and Watson*, but also the judgment in *DRI* (the invalidity of the data retention directive)[67] or the recent opinion 1/15 about the compatibility with EU law of the planned agreement with Canada on the exchange of PNR data.[68] In each of these cases, the Court stressed the necessity of considering the provisions of the Charter of Fundamental Rights with laws which are being enacted or are planned to be enacted by the European Union, particularly in the field of privacy protection. In the long run, a declaration of the invalidity of the legal basis of transferring data outside the EU will open up the

[65] An example of this could be the new regulation on the protection of privacy in the electronic communications sector, which is going to replace Directive 2002/58 and which is currently being discussed among the Member States and the EU institutions – see CELEX 52017PC0010, legislative procedure 2017/03

[66] *Cf.* a complaint filed by the Digital Rights Ireland regarding the incompliance with the EU law of the EC Decision 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-US Privacy Shield; this decision replaced Decision 2000/520, which was declared invalid in an earlier case (C-362/14, footnote 44). The complaint was based on the procedure provided for in Article 263 of the TFEU, which means that the proceedings were not initiated by a national court. In the decision of 22 November 2017 (T-670/16), the CJEU dismissed the complaint, raising its inadmissibility due to the lack of standing. Another case in which the validity of Decision 2016/1250 is being contested is T-738/16.

[67] The judgment of CJEU of 8 April 2014 in the case *Digital Rights Ireland*, C-293/12.

[68] The opinion of CJEU of 26 July 2017, 1/15, ECLI:EU:C:2017:592.

possibility to seek compensation from entrepreneurs.[69] Actually, it may turn out that moving data processing centres from the United Kingdom to the Member States of the EU will be seen as mitigating the risk involved in the e-service providers' activity.

In consequence, the UK government's approach to solving the issue of surveillance programmes and ensuring their compatibility with EU law has also a noticeable economic dimension. The arguments raised so far, referring to the violation of fundamental rights and international law, have been insufficient to change the practice of UK intelligence services. Arguments of an economic nature might prove to be more effective. Undoubtedly, this subject will be elaborated on in further negotiations related to the process of the United Kingdom's withdrawal from the European Union.

STRESZCZENIE

BRYTYJSKIE PROGRAMY INWIGILACJI ELEKTRONICZNEJ A OCHRONA PRAW OBYWATELI UE PO BREXICIE

Stosowanie rozbudowanych środków inwigilacji elektronicznej jest coraz częściej wskazywane jako jedno z głównych zagrożeń dla ochrony prywatności w cyberprzestrzeni, a w konsekwencji – dla budowy społeczeństwa opartego na informacji i wiedzy. Zagadnienie to jest często wiązane z poszukiwaniem równowagi pomiędzy ochroną praw jednostek (prawo do prywatności) a bezpieczeństwem publicznym (ochrona przed najpoważniejszymi przestępstwami) i kojarzone z działaniami realizowanymi przez amerykańskie służby wywiadowcze. Rozbudowane programy inwigilacyjne są jednak również prowadzone przez niektóre państwa członkowskie UE. Działania te budzą uzasadnione wątpliwości co do ich zgodności z prawem Unii, a także z obowiązkami wynikającymi z EKPC. Szczególne znaczenie mają programy inwigilacji elektronicznej prowadzone przez brytyjskie służby wywiadowcze (zwłaszcza GCHQ). Działania te nie tylko opierają się na hurtowym gromadzeniu danych elektronicznych, ale także na ich przekazywaniu do służb specjalnych państw trzecich.

Problem szeroko zakrojonych działań inwigilacyjnych prowadzonych przez władze brytyjskie pozostał nierozwiązany na poziomie prawa UE. Również orzecznictwo ETPC, w którym wskazano na brak proporcjonalności tego typu programów, nie przyczyniło się do zmiany brytyjskiej praktyki. Wyjście Wielkiej Brytanii z Unii Europejskiej i oparcie przyszłych stosunków na wydawanej przez KE decyzji o adekwatności zabezpieczeń otwiera nowe pole dla rozwiązania tego problemu.

[69] *See* a class action initiated by M. Schrems after the ruling in case C-362/14 (see footnote 44), in which the plaintiffs demand, among others, payment of compensation in the amount of 4.000 Euros from Facebook Ireland Ltd. in connection with an alleged disclosure of personal information to the US intelligence services in violation of EU law. The case is still pending. The court in Austria referred to the CJEU regarding the admissibility of the claims by Mr Schrems pursuant to Regulation 44/2011. The Court replied to the request in the judgment of 25 January 2018, C-498/16.

W artykule omówiono możliwy wpływ Brexitu na ramy prawne brytyjskich programów inwigilacji elektronicznej oraz przedstawiono nowe środki wpływu, które będą dostępne dla europejskich partnerów w celu ograniczenia masowych działań inwigilacyjnych prowadzonych przez władze brytyjskie.

Słowa kluczowe: masowa inwigilacja, brexit, bezpieczeństwo narodowe, ochrona prywatności, dane osobowe, FVEY, GCHQ, Tempora

Key words: mass surveillance, bulk surveillance, Brexit, national security, privacy, data protection, FVEY, GCHQ, Tempora