RELEVANT PRINCIPLES IN THE ECHR AND CJEU JURISPRUDENCE REGARDING NATIONAL SECURITY

Maj. Sorina Ana MANEA, PhD Candidate *

The European system ensuring the protection of human rights is nowadays one of the most advanced in the world. However, there are also areas of activity where clarification and improvement are constant demands. Counter-terrorism measures considered or adopted in Europe, in particular those that increase mass surveillance, the collection and storage of electronic information or the protection of personal data are such areas. Some of these measures give more intrusive powers to the intelligence services to channel decisions in the direction of the executive branch, without the necessary judicial guarantees being established in a state governed by the rule of law.

Keywords: community law; ECHR; CJUE; national security.

Electronic surveillance by national law enforcement authorities is inherently linked to the right to privacy and the protection of personal data. Such rights are enshrined in EU law, which requires compliance with the principles of necessity, proportionality and subsidiarity. Legal issues arising from electronic surveillance, which may affect the rights of individuals, are not subject to review by the Court of Justice of the EU (CJEU), which has jurisdiction to rule on cases brought against States or institutions for failure to fulfill their obligations under EU law, in which case the state that has not fulfilled its obligations is obliged to take measures to put an immediate end to the violation of the legal norms. Injured persons, after exhaustion of national remedies, can apply to the European Court of Human Rights (ECHR) for a final decision. Therefore, the decisions of the two international courts form the jurisprudence that can lead to a change in the internal procedures according to which the competent state authorities operate to protect the national security.

After September 2001, mass electronic surveillance experienced an unprecedented evolution in response to the aggressiveness with which the terrorist phenomenon began to manifest. Precisely because of the urgency with which they had to act to meet the obligation to protect their citizens throughout the European Union, the work of intelligence services was supported by national governments by measures that allowed for greater easiness in assessing how information gathering takes place mostly in regard with the technical and technological means employed.

The intelligence activity to identify, prevent and counter threats to national security, in particular that carried out through large-scale surveillance, may interfere with fundamental rights and freedoms, in particular the right to privacy and data protection which may lead to disruption of the rule of law and the respect of the fundamental rights and freedoms of citizens.

Following the revelations of NSA analyst Edward Snowden[1] and those of the press regarding the mass electronic surveillance by US intelligence services more or less with the agreement of several EU Member States[2], the European Parliament adopted a resolution on the US NSA Surveillance Program, supervisory bodies in different Member States (EU) and their impact on the fundamental rights of EU citizens.

In this context, the CJEU and the ECHR have developed a set of legality tests transposed into principles that are compatible with the rule of law.

Thus, in the Digital Rights Ireland Ltd Case[3], the CJEU annulled the EU Directive[4] which required states to ask telecommunications providers to keep metadata for a period of six months (minimum) and two years (maximum) and to make it available to criminal investigation and investigation bodies in case of investigation of serious crimes. The directive left it up to states to establish safeguards to regulate access to metadata and prevent abuse of power.

***"Carol I" National Defence University**
e-mail: *sorinaman2@yahoo.com*

However, the case has not led to a standardization of investigative practice in criminal or national security matters in the EU Member States, who prefer to consider liability, at least in the field of security, to be exclusively national.

In October 2015, in the Schrems case[5], the CJEU invalidated the EU-US agreement called The Umbrella Agreement[6], which replaced the Safe Harbor Agreement[7] and allowed private companies to transfer personal data to EU citizens in the US, ruling that, in light of the Snowden disclosures, it was reasonable and pertinent to argue that the law and practice in force in the US did not ensure adequate protection of personal data, finding that monitoring the content of emails, phone calls and text messages, as well as extracting large amounts of metadata about the location of the mobile phone, internet browsing, e-mails, e-mail address books, etc., was not protected against illegitimate surveillance. The CJEU found that EU countries were not free to transfer data to third countries, unless those third countries provided for data protection standards equivalent to those applicable in the EU.

In December 2016, in the case of Tele2 Sverige AB[8] concerning Directive 2002/58[9] laying down the rules applicable to the processing of traffic and location data generated by the use of electronic communications services, as well as the anonymization or deletion of such data, except in criminal and national security, the CJEU found that the guarantees of safeguarding and access that must exist are under Community law. In this respect, the CJEU ruled that access to metadata must be conditional on the prior approval of a court.

The CJEU noted that discriminatory storage of traffic and location data, in order to combat serious crime under national law, can be accepted as a precautionary measure when „In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data have been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 54 and the case-law cited)"[10]. Also, „in regard to the material condition to be met by national legislation which allows, in the fight against crime, the preventive storage of transfer data and location data, in order to ensure that it is limited to what is strictly necessary, it must be shown that, although these conditions may vary depending on the measures taken to prevent, investigate, detect and prosecute serious crime, data retention must always meet objective criteria that establish a relationship between the data to be kept and the purpose pursued. In particular, such conditions must prove, in practice, capable of effectively delimiting the extent of the measure and, consequently, of the relevant public."[11].

In October 2020, the Grand Chamber of the CJEU gave two rulings[12] on data retention, national security and fundamental rights prohibiting EU Member States from enacting legislation designed to undermine the scope of its confidentiality obligations in the field of traffic and location data unless it respects the general principles of Community law, in particular the principle of proportionality, and the fundamental rights enshrined in the EU Charter of Fundamental Rights.

In the related cases C-511/18 and C-512/18, the situation regarding the legality of national legislation requiring communications service providers to transmit to users traffic data and location data to a public authority or to keep such data was brought to justice, given in a general or non-discriminatory manner. National courts referred cases to the CJEU to clarify whether: the activities of national security services – as opposed to criminal bodies – fall within the scope of EU law and whether the non-discriminatory retention of data for national security is compatible with EU law.

The CJEU decided that automated analysis and real-time collection of traffic data, location data or real-time collection of device location data is permitted if: automatic analysis is limited to cases where a Member State faces a serious threat, authentic and present or predictable for national security, and real-time collection is limited to persons validly suspected of being involved in

terrorist activities. In both cases, the seriousness of the threat and the danger posed by the suspect must be subject to prior verification by a court or an independent administrative body whose decision is binding.

Finally, the CJEU analyzed the situation where it is possible to temporarily maintain the effects of a national provision that infringes EU law in order to avoid legal uncertainty and to use data previously collected and stored. On this issue, the CJEU considered that the Directive, read in the light of the Charter, does not allow a national court to temporarily apply a provision of national law that would otherwise be incompatible with EU law. In particular, the CJEU has prohibited national courts from applying a national provision requiring providers to keep traffic and location data in a generalized and non-discriminatory manner, even if the purpose of the contested provision is to protect national security and prevent serious crime.

The CJEU ruling has an important role to play in regulating national security and intelligence activities in EU Member States. In this regard, Advocate General Campos Sanchez-Bordona, in his Opinion delivered in January 2020[13] on the above-mentioned cases, argued that there was a distinction between intelligence work carried out to protect national security and legislation adopted to protect national security. obligations that affect their Community rights. This relative novelty is reflected in the EU legal framework, where national security, despite European integration, has explicitly remained the responsibility of the Member States.

The ECHR also plays an active role in ensuring respect for fundamental human rights and freedoms against the arbitrary use of state power. In this regard, the ECHR has ruled on the interception of communications of any kind that when a State takes surveillance measures it is possible that the persons concerned may be treated in a manner contrary to Article 8 of the Convention without them being aware of it, and, therefore, without being able to obtain an appeal at national level or before the institutions of the Convention. The Court has therefore accepted that a person may, under certain conditions, claim to be the victim of an infringement caused by the mere existence of secret measures or legislation permitting secret measures, without having to claim that such measures were applied to him. The relevant conditions must be established in each case in accordance with the provisions of the Convention or the allegedly violated rights, the secrecy of the contested measures and the link between the person who considers himself injured in his rights and those measures. The Court also noted that the possibility of secret surveillance of certain citizens is permitted under the Convention only to the extent strictly necessary for the protection of democratic institutions. „Noting, however, that democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction, the Court considered that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications was, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime"[14].

Therefore, this judgment, reflecting the conventional provisions, establishes the principles of the legality test on the implementation of temporary restrictive measures of fundamental rights and freedoms, namely the right to privacy, freedom of expression, access to justice and the right to a fair trial, as well as their correlative rights.

The Court ruled that the storage of data relating to the privacy of a person by a public authority constitutes an interference with the right to privacy, regardless of the subsequent use of the information or whether or not the information collected has harmed the data subject[15]. Including public information collected and stored systematically by the authorities falls within the scope of privacy, especially if the information concerns a person's distant past and some of this information has been declared false and is likely to harm the concerned person's reputation[16].

According to the case law of the Court, the requirement that any interference be in accordance with the law is met where the contested measure must have a basis in national law and the law in question must be accessible to the person concerned and have foreseeable consequences[17]. In the case of Rotaru v. Romania[18], the Court examined the Romanian legislation on secret surveillance

measures related to national security and concluded that the legislation on the collection and storage of information did not provide the necessary guarantees. The court reiterated this finding in its decisions regarding the cases of Dumitru Popescu against Romania, no. 2, 2007 and the Association „21 December 1989" and others against Romania, 2011.

The State's interest to protect its national security must be proportionate to the seriousness of the interference with the person being monitored in respect of his or her privacy. Thus, in the case of Kennedy v. The United Kingdom, the Court held that the power to institute oversight of citizens was tolerated only in accordance with the provisions of the Convention in so far as it was strictly necessary for the protection of democratic institutions, in other words that there were adequate and effective safeguards against abuse.

Conclusions

The activity of the CJEU and the ECHR formulates the democratic framework for carrying out the intelligence activity at legislative level, also as a result of the constitutionality control, but especially of Romania's membership in the EU, at executive and judicial level. If in 1990 the intelligence activity carried out for the achievement of national security was shrouded in secrecy and inaccessibility, today and certainly in the future it will have as coordinates the observance of human rights and the jurisprudence of the community courts.

The importance of the two sources of regulation of some of the working methods of the intelligence services is enhanced especially if the rules and tests established by jurisprudence were to be taken as the performance standards of the mentioned activity. For example, in order to prevent terrorism, States may take measures that, for example, interfere with the right to privacy, freedom of expression or association, or the right to free choice. However, the rule of law does not give states a free hand to interfere with the rights of those in their jurisdiction. Governments will always need to demonstrate that the measures they have taken to counter threats to national security have been justified in the light of the text of the Convention and the interpretations of the two Community courts by its judgments.

NOTES:

1 Edward Snowden, North American whistleblower who made public the classified mass surveillance program conducted by the US.

2 *European Parliament resolution of 12 March 2014 on the surveillance program of the US National Security Agency (NSA), the surveillance bodies of the various Member States and their impact on the fundamental rights of EU citizens and on transatlantic cooperation in the field of justice and security of Internal Affairs (2013/2188 (INI))*, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52014IP0230&from=RO, accessed on 12.03.2021.

3 *Judgment of the Court (Grand Chamber)*, 8 April 2014, Electronic communications - Directive 2006/24/EC - Publicly available electronic communications services or public communications networks services - Retention of data generated or processed in connection with the provision of such services – Validity – Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union In Joined Cases C-293/12 and C-594/12, Requests for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, http://curia.europa.eu/juris/liste.jsf?num=C-293/12 , accessed on 12.03.2021.

4 *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*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2006.105.01.0054.01.ENG&toc=OJ%3AL%3A2006%3A105%3ATOC, accessed on 12.03.2021

5 *Judgment of the Court (Grand Chamber)* of 6 October 2015. Maximillian Schrems v Data Protection Commissioner. Request for a preliminary ruling from the High Court (Ireland). Reference for a preliminary ruling - Personal data - Protection of individuals with regard to the processing of such data - Charter of Fundamental Rights of the European Union - Articles 7, 8 and 47 - Directive 95/46/EC - Articles 25 and 28 - Transfer of personal data to third countries - Decision 2000/520/EC - Transfer of personal data to the United States - Inadequate level of protection - Validity - Complaint by an individual whose data has been transferred from the European Union to the United States - Powers of the national supervisory authorities. Case C-362/14. Digital reports (Court Reports - general) at http://curia.europa.eu/juris/liste.jsf?num=C-362/14, accessed last 12.03.2021.

6 *Council Decision (EU) 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of 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*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D0920, accessed on 12.03.2021.

7 *2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament*

and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) Official Journal L 215, 25/08/2000, https://eur-lex.europa.eu/legal content/en/ALL/?uri=CELEX%3A32000D0520, accessed on 12.03.2021.

8 *Judgment of the Court (Grand Chamber)* of 21 December 2016. Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others. Requests for a preliminary ruling from the Kammarrätten i Stockholm and the Court of Appeal (England & Wales) (Civil Division). Reference for a preliminary ruling - Electronic communications - Processing of personal data - Confidentiality of electronic communications - Protection - Directive 2002/58/EC - Articles 5, 6 and 9 and Article 15(1) - Charter of Fundamental Rights of the European Union - Articles 7, 8 and 11 and Article 52(1) - National legislation - Providers of electronic communications services - Obligation relating to the general and indiscriminate retention of traffic and location data - National authorities - Access to data - No prior review by a court or independent administrative authority - Compatibility with EU law. Joined Cases C-203/15 and C-698/15, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN, accessed on 12.03.2021.

9 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), https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=ENhttps://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=EN, accessed on 12.03.2021.

10 *Tele2 Sverige AB (C 203/15)*, para. 109.

11 *Ibidem*, para. 110.

12 *Judgment of the Court (Grand Chamber)* of 6 October 2020 La Quadrature du Net and Others v Premier ministre and Others Requests for a preliminary ruling from the Conseil d'État (France) and Cour constitutionnelle (Belgium) Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Providers of electronic communications services – Hosting service providers and Internet access providers – General and indiscriminate retention of traffic and location data – Automated analysis of data – Real-time access to data – Safeguarding national security and combating terrorism – Combating crime – Directive 2002/58/EC – Scope – Article 1(3) and Article 3 – Confidentiality of electronic communications – Protection – Article 5 and Article 15(1) – Directive 2000/31/EC – Scope – Charter of Fundamental Rights of the European Union – Articles 4, 6, 7, 8 and 11 and Article 52(1) – Article 4(2) TEU Joined Cases C-511/18, C-512/18 and C-520/18, http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6166350 and Judgment of the Court (Grand Chamber) of 6 October 2020 Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others Request for a preliminary ruling from the Investigatory Powers Tribunal – London Reference for a preliminary ruling – Processing of personal data in the electronic communications sector – Providers of electronic communications services – General and indiscriminate transmission of traffic data and location data – Safeguarding of national security – Directive 2002/58/EC – Scope – Article 1(3) and Article 3 – Confidentiality of electronic communications – Protection – Article 5 and Article 15(1) – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 11 and Article 52(1) – Article 4(2) TEU Case C-623/17, http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6063852, accessed on 12.03.2021.

13 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62018CC0511, accessed on 12.03.2021.

14 *Case of Klass and others vs. Germany*, 1978, para. 34 and next, https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22695387%22],%22itemid%22:[%22001-57510%22]}, accessed on 13.02.2021.

15 *Case of Amann vs. Switzerland*, 2000, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58497%22]}, accessed on 13.02.2021.

16 *Case of Rotaru vs. Romania*, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-148906%22]}, accessed on 13.02.2021.

17 *Case of Kennedy vs. UK*, 2010, para. 151; *Case of Rotaru vs. Romania*, 2020, para. 52; *Case of Amann vs. Switzerland*, para. 50; *Kruslin vs. France*, 1990, para. l27; *Case of Malone vs. UK*, 1984, para. 67 and 68; *Case of Leander vs. Sweden*, 1987, para. 51, etc.

18 *Case of Rotaru vs. Romania*, http://legislatie.just.ro/Public/DetaliiDocumentAfis/25965, accessed on 13.02.2021.

REFERENCES

*** *Decizia 2000/520*, O.J. L 215/7 (2000), https://eur-lex.europa.eu/legal content/en/ALL/?uri=CELEX%3A32000D0520

*** *Decizia Consiliului (UE) 2016/920, din 20 mai 2016, privind semnarea, în numele Uniunii Europene, a Acordului dintre Statele Unite ale Americii și Uniunea Europeană privind protecția informațiilor personale referitoare la prevenire, investigație, detectare și urmărirea penală a infracțiunilor*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D0920.

*** *Directiva 2002/58/CE, din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice* (Directiva privind confidențialitatea și comunicațiile electronice), https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

*** *Directiva 2006/24/EC privind reținerea datelor generate sau prelucrate în legătură cu*

furnizarea de servicii de comunicații electronice accesibile publicului sau a rețelelor de comunicații publice și de modificare a Directivei 2002/58 / CE, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2006.105.01.0054.01.ENG&toc=OJ%3AL%3A2006%3A105%3ATOC.

*** *Hotărârea Curții (Marea Cameră)*, din 21 decembrie 2016, Tele2 Sverige AB (C 203/15) v Post-och telestyrelsen, și Secretarul de Stat al Departamentului de Interne (C 698/15) împotriva Tom Watson, Peter Brice și Geoffrey Lewis, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN.

*** *Hotărârea Curții (Marea Cameră)*, din 21 decembrie 2016, Tele2 Sverige AB (C 203/15), paragraful 109.

*** *Hotărârea Curții (Marea Cameră)*, din 6 octombrie 2015, C-362/14 Maximillian Schrems împotriva Data Protection Commissioner, http://curia.europa.eu/juris/liste.jsf?num=C-362/14.

*** *Hotărârea Curții (Marea Cameră),* din 8 aprilie 2014, C-293/12 și C-594/12 Digital Rights Ireland, EU:C:2014:238, http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

*** *Rezoluția Parlamentului European*, din 12 martie 2014, referitoare la programul de supraveghere al Agenției Naționale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre și la impactul acestora asupra drepturilor fundamentale ale cetățenilor UE și asupra cooperării transatlantice în materie de justiție și de afaceri interne (2013/2188(INI)), https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52014IP0230&from=RO.

[Council of Europe], *Manual de legislație europeană privind protecția datelor*, Agency for Fundamental Rights of the European Union, 2014.

Ausloos J., *The Right to Erasure in EU Data Protection Law*, Editura Oxford University Press, 2020.

Bîrsan C, *Convenția europeană a drepturilor omului. Comentariu pe articole*, Edition 2, C.H. Beck Publishing House, 2010.

Bradford Anu, *The Brussels Effect. How the European Union Rules the World*, Editura Oxford University Press, 2020.

Deleanu I., „Accesibilitatea şi previzibilitatea legii în jurisprudenţa Curţii Europene a Drepturilor Omului şi a Curţii Constituţionale a României", *Dreptul* no. 8, 2011.

Duminică R., *Criza legii contemporane*, C.H. Beck Publishing House, Bucharest, 2014.

Solove D., Schwarts P., *Privacy Law Fundamentals*, Edition 4, Publishing House of International Association of Privacy Professionals (IAPP), 2017.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6166350și cauza C-623/17 Privacy International, lahttp://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6063852

https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58497%22]}

https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22695387%22],%22itemid%22:[%22001-57510%22]}

http://legislatie.just.ro/Public/DetaliiDocumentAfis/25965

https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-148906%22]}