TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 26, 2021

A new decade for social changes

www.techniumscience.com

ISSN 2668-7798

Technium Social Sciences Journal
Vol. 26, 424-429, December, 2021
ISSN: 2668-7798
www.techniumscience.com

Brief explanations on EU Directive no. 68027.04.2016 in the field of personal data processing

Dragoș Mihail Mănescu

The Bucharest University of Economic Studies, Romania

dragos.manescu@drept.ase.ro

Abstract. The processing of personal data is regulated by Directive 680/2016 when it is carried out by national security institutions or by law enforcement bodies. The Directive establishes the general framework for exemption from the principles of personal data protection enacted by the GDPR, establishing a restrictive and reasoned temporary derogation, considered indispensable for carrying out activities aimed at ensuring national security or the national judicial system, as well as prevention, detection and combating crime.

Keywords. Directive 680/2016, GDPR, automatic processing, protection of personal data

1. General considerations

The unprecedented technological transformations enhanced by an exponential development of the Internet, global and relatively free access to information and technology, as well as the growing evolution of social media to the so-called metaverse[1], have put national security institutions in a position to have to adapt to these radical transformations but, at the same time, provided them with the necessary means to collect and process huge amounts of personal information existing online, obviously without the knowledge of the data subjects.

National security institutions or law enforcement institutions and bodies must act permanently and effectively for the four EU data surveillance directions in the fight against terrorism:

- supervision of electronic communications metadata;
- travel data monitoring;
- supervision of financial data;
- data surveillance on the internet[2].

At the same time, art. 8 of the European Convention on Human Rights[3] regulated the Right to respect for private and family life. In the context of regulating the protection of

[1] https://ro.wikipedia.org/wiki/Metavers: term commonly used to describe the concept of a future iteration of the Internet, consisting of shared 3D virtual spaces, connected in a virtual universe. This concept was probably first described in Neal Stephenson's 1992 novel Snow Crash

[2] Maria Tzanou, The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance, Hart Publishing, Oxford and Portland, Oregon, 2017, p. 5

[3] https://www.echr.coe.int/Documents/Convention_RON.pdf

Technium Social Sciences Journal
Vol. 26, 424-429, December, 2021
ISSN: 2668-7798
www.techniumscience.com

personal data in the European Union by Regulation (EU) 679/2016[4] which upgraded the legislation[5] in this field, the European legislator felt also the need to regulate specifically the field of action of the institutions and bodies that deal with national security and law enforcement. In order to do that, the legislator enacted EU Directive no. 680 / 27.04.2016[6] and established the obligation for Member States to transpose the directive into national legislation by May 6, 2018. Romania has responded to the above mentioned obligation of introducing the directive into the national legislation by enacting Law no. 363/2018[7] which adapted the provisions of Directive 680/2016 to the local specificity[8].

The applicable law, namely Directive 680/2016 or the General Data Protection Regulation (GDPR), will be established by analyzing the actors involved, public or private legal entities, the purpose of obtaining and processing data (are required in criminal proceedings or in economic or research and development), the nature of the data. Thus, we mention by way of example that the processing of personal data by a national security institution in investigations or court proceedings to prevent and combat crime, to protect public order and safety or to protect the rights of others are necessary and sufficient arguments to apply Directive 680/2016 while the processing of the same type of data for the purpose of developing software or in research and development projects will be regulated by the GDPR.

The situation is more complicated to assess from the point of view of the applicable legislation when the data are processed and transmitted in an anonymous form. This is the case with the obligation of confidentiality that determines the security institutions to anonymize the data that results from the investigation and prosecution of crimes and the data and information obtained in the prosecution activity. In this situation, none of the mentioned normative acts will be applicable, but the national legislation in criminal matters. In the event of such nuances or differences which may lead to divergent interpretations by the courts as to the applicable law, they will have to consider the incidence of the direct effect and, respectively the indirect effect of European law[9].

2. Brief considerations on the subject

Point no. 26 of the Preamble of the Directive 680/2016 states that "any processing of personal data must be legal, fair and transparent to the natural persons concerned".

[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).

[5] See also Simona CHIRICĂ, The main novelties and implications of the new general data protection regulation, Perspective of Business Law Journal, vol. 6, București 2017

[6] 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.

[7] Law no. 363 of 28 December 2018 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating, prosecuting and combating crime or the execution of punishments, educational and security measures, and on the free movement of these data. It entered into force on January 7, 2019.

[8] See also Simona Șandru, Data Retention in Romania în Law, Governance and Technology Series Issues in Privacy and Data Protection 45, European Constitutional Courts towards Data Retention Laws, Springer Nature Switzerland AG 2021, p. 189-202

[9] See also Ovidiu Ioan Dumitru, Andreea Stoican, European Union Law, Lecture Notes, Ed. ASE, București 2020, p. 41-50 and p. 157

Technium Social Sciences Journal
Vol. 26, 424-429, December, 2021
ISSN: 2668-7798
www.techniumscience.com

At the same time, art. 10 of Directive (EU) 2016/680 provides the conditions under which special categories of personal data[10] may be processed, respectively:

- the processing must be expressly provided by law;
- the processing of data is necessary in order to ensure the protection necessary to protect the vital interests of the data subject or of another natural person;
- in the event that the data subject has made the data public, manifestly;

All these provisions must be corroborated with the provisions of art. 11 of the same directive, which provides that States shall provide adequate safeguards for the protection of the rights and freedoms of the individual in the event of a decision based solely on automatic processing, in particular if significant.

In para. 3 of the same article, the Directive provides that it is prohibited to create profiles that result in discrimination against individuals on the basis of special categories of personal data and information.

Profiling, respectively automatic processing is allowed by Directive 680/2016 if it is done with ensuring adequate guarantees for the protection of rights and freedoms of the data subject: at least, but not only that, the right to obtain human intervention from the operator. At the same time, a substantial distinction must be made between individual surveillance and mass surveillance[11], especially in view of the exponential increase in the computing power, storage and analysis of technological means. In this context, we can say that security measures aimed at banning individual abuses will ensure, on one hand, intrinsic protection against widespread abuse, arbitrariness and, why not, against dictatorial decisions and behavior made by some institutions of force. On the other hand, it will represent the guarantee of the protection of the fundamental and legitimate rights of the citizens, as they are regulated and protected by art. 2 of the Treaty on European Union[12].

Another important aspect is the right to be forgotten. Thus, as art. 17 of the GDPR establishes the right to be forgotten, also art. 5 of Directive 680/2016 establishes appropriate deadlines for the deletion of personal data or for a regular review of the need to store personal data, this right being, in our opinion, part of all the guarantees that states must provide for protection of the personal data of the data subject. However, the reference to these time limits is vague and does not allow the establishment of exact time limits and no differentiation of the retention process according to elements such as the gravity of the crime, the specific elements of its commission, the degree of social danger and the characteristics of the perpetrator.

At the same time, in order to ensure additional legal guarantees, it is necessary to keep the data within the borders of the European Union, thus making it possible to better control and manage them[13].

---

[10] Art. 10 of Directive 680/2016: racial or ethnic origin, political opinions, religious denominations or philosophical beliefs, trade union affiliation, processing of genetic data, processing of biometric data for the unique identification of a natural person or processing of health or life data sexual orientation and sexual orientation of an individual

[11] Independent High Level Expert Group on Artificial Intelligence set up by the European Commission in June 2018 (AI HLEG), Ethical Guidelines for Reliable Artificial Intelligence (AI), p. 45, (https://ec.europa.eu / digital-single-market / en / high-level-expert-group-artificial-intelligence)

[12] https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_1&format=PDF: art. 2 of the Treaty on European Union: the values of respect for human dignity, liberty, democracy, equality, the rule of law, and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society characterized by pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men.

[13] https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf: Related causes C-293/12 și C-594/12 Digital Rights Ireland and Seitlinger and others: Lastly, the Court states that the directive does not require that the data be retained within the EU. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried

Technium Social Sciences Journal
Vol. 26, 424-429, December, 2021
ISSN: 2668-7798
www.techniumscience.com

Moreover, we believe that the correct, relevant, objective assessment of personal data obtained by law enforcement agencies in criminal proceedings, must be made in court[14] both in detail and as a whole, in particular but also in general (through the so-called analysis or investigation report) in order to create an unequivocal picture of it, based on current, accurate and complete data transmitted by those bodies[15]. In addition to that, more and more sophisticated technical methods and means are used and, why not recognize, sometimes difficult to understand from a technical point of view, both for obtaining data and information and for their analysis and interpretation by specialized institutions of the state.

The legal guarantees granted to the data subjects for the protection of their personal data are generally two:

- according to the obligation of the operator to inform: the operator has to provide the data subject with the necessary information that will enable the data subject to assess whether an infringement of his rights has taken place and the extent of that infringement or the damage suffered. Including the subsequent actions of the data subject, his recourse to a relevant judicial remedy or the actions of the state control or judicial authorities will be based on the data provided by the controller itself.

- Control of the supervisory authority following its notification by the personal data controller of a breach of the security of this type of data. It should be noted that the law regulates that the notification is not required if the breach of personal data security does not have the potential to create a high risk to the rights and freedoms of the individual[16]. The setting of the limits that characterize the high risk compared to a common risk remains under debate.

It is certain that an anticipatory assessment of the possible risks posed by the processes and procedures used by law enforcement institutions will reduce, without guaranteeing elimination, the risk of incidents or high-risk violations of the rights and freedoms of persons, including that of the protection of personal data. Certainly, testing the processes, technologies or means used by these institutions at a pre-implementation stage and based on the anonymized data sets will have the above-mentioned result.

3. Conclusions

Without in any way minimizing the importance of the work carried out by the institutions in the field of national security, as expressed in the doctrine, in recent years there has been a growing availability of both the General Court and the European Court of Justice to revise and even repeal EU legislation for violations of fundamental rights, in parallel with a strong assertion of the priority of fundamental rights in EU law over EU secondary legislation and even over the most important rules of international law[17].

At the same time, we consider that personal data controllers in general, and even more so those working in cases in the field of national security, must analyze the possible risks to

out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.

[14] Olivier Leroux, 'Legal Admissibility of Electronic Evidence', International Review of Law, Computers & Technology 18, no. 2 (July 2004): p. 193–220, https://doi.org/10.1080/1360086042000223508.

[15] Art. 7 para. 2 of Directive 680/2016: Member States shall ensure that competent authorities take all reasonable steps to ensure that personal data that are inaccurate, incomplete or out of date are not transmitted or made available. To this end, each competent authority shall verify, as far as possible, the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information shall be added to enable the receiving competent authority to assess the accuracy, completeness, reliability and timeliness of personal data.

[16] Art. 36 of Law no. 363/2018 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating, prosecuting and combating crime or the execution of penalties, educational and security measures, and on the free movement of such data

[17] Paul Craig, Gráinne de Búrca, EU Law. Text, Cases, and Materials, Fifth edition, Oxford University Press, 2011, p. 378

Technium Social Sciences Journal
Vol. 26, 424-429, December, 2021
ISSN: 2668-7798
www.techniumscience.com

data subjects both from the perspective of the legislation enshrined in Directive 680/2016 but also taking into account the principles enshrined in the European Charter of Fundamental Rights[18], which expressly regulates in Article 8 the right to the protection of personal data and the principles which must underpin their processing.

At the same time, it should be noted that the areas of data protection and privacy have been frequently invoked to challenge the EU's executive action and call for the active intervention of the European Commission as an exponent of the executive branch[19].

As a result:

1. the strict, unequivocal and within determined or determinable regulation of the processing of personal data, but also
2. the access and exchange of such data between the competent cross-border institutions, as well as
3. the standardization and implementation of a coherent system of checks and balances,

will bring, on the one hand, the protection of citizens at the individual level and, on the other hand, will limit the oscillation of society and the judiciary between granting increased prerogatives and powers to national security institutions and the limitation of those powers up to a level that is inappropriate to the performance of specific actions aimed at protecting the same society or the same individuals whose rights it has an obligation to respect.

At the same time, we must not forget the national specificities and the notable differences between situations of an operational and judicial nature when we talk about threats to existing national security at Member State level, which will lead to the application of specific, tougher measures and means, or more malleable, since, as specified in art. 4 para. 2 of the Treaty on European Union, "In particular, national security remains the sole responsibility of each Member State." Perhaps this is one of the reasons why the European legislator preferred to regulate this matter by a directive and not by a regulation, as it did in the case of the GDPR, in order to allow the transposition legislation to be anchored to national specificities.

References

[1] Paul Craig, Gráinne de Búrca, EU Law. Text, Cases, and Materials, Fifth edition, Oxford University Press, Oxford, 2011
[2] Maria Tzanou, The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance, Hart Publishing, Oxford and Portland, Oregon, 2017
[3] Ovidiu Ioan Dumitru, Andreea Stoican, European Union Law, Lecture Notes, Editura ASE, București 2020
[4] Simona Şandru, Data Retention in Romania în Law, Governance and Technology Series Issues in Privacy and Data Protection 45, European Constitutional Courts towards Data Retention Laws, Springer Nature Switzerland AG 2021
[5] Simona CHIRICĂ, The main novelties and implications of the new general data protection regulation**,** Perspective of Business Law Journal, vol. 6, București 2017
[6] Olivier Leroux, 'Legal Admissibility of Electronic Evidence', International Review of Law, Computers & Technology 18, no. 2 (July 2004), https://doi.org/10.1080/1360086042000223508

[18] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:ro:PDF
[19] Paul Craig, Gráinne de Búrca, EU Law. Text, Cases, and Materials, Fifth edition, Oxford University Press, 2011, p. 379

[7] Independent High Level Expert Group on Artificial Intelligence established by the European Commission in June 2018 (AI HLEG), *Ethical Guidelines for a Reliable Artificial Intelligence (AI)*, (https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence)
[8] https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_1&format=PDF
[9] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:ro:PDF
[10] https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf