sciendo

Proceedings of the 4th International Conference on Economics and Social Sciences (2021), ISSN 2704-6524, pp. 465-478

The 4th International Conference on Economics and Social Sciences
Resilience and economic intelligence through digitalization and big data analytics
June 10-11, 2021
Bucharest University of Economic Studies, Romania

Personal Data between Individual Protection and the General Interest

Dragoș Mihail MĂNESCU*

DOI: 10.2478/9788366675704-046

Abstract

Processing of personal data by national security institutions and bodies or by law enforcement agencies is carried out on the specific basis of special legislation, derogating from the Lex generalis (GDPR). This paper examines some of the challenges posed by the need to protect national security, to prevent, detect and combat crime and, at the same time, to respect and protect the lawful right of the individual to benefit from the protection of personal data and privacy and family life.

Keywords: GDPR, Directive 680/2016, automatic processing, profiling, artificial intelligence, personal data protection.

JEL Classification: K15, K20, M15.

1. General Considerations

The entire processing of personal data by the national security institutions and bodies or by the law enforcement agencies stands out as indispensable to allow the development of activities aimed at ensuring national security or of the national judicial system. The current international and national legal framework establishes a number of general exceptions to the principles of personal data protection, highlighting all the circumstances in which the processing of personal data by above-mentioned institutions is allowed, as well as the reasons for these exceptions, i.e., those related to national security, prevention, detection and combating of crimes, etc.

What must be kept in mind, however, is that the exceptions we refer to are not unlimited freedom, but rather a temporary limiting and reasonable derogation from the general principles governing access to personal data, principles expressed clearly and without equivocal in art. 5 in the *lex generalis*, i.e., GDPR[1]. This is because, as stated in the doctrine (Tzanou, 2017), data protection as a fundamental right must be able to function both positively and negatively. Thus, on the one hand, it should be

* Bucharest University of Economic Studies, Bucharest, Romania, dragoș.manescu@ drept.ase.ro.

able to regulate, channel and control power and, on the other hand, prohibit power (abuse).

As a result, the legislation does not leave to the said institutions the undifferentiated and general access and processing of personal data, without any control, surveillance or restriction. This is despite the fact that Directive 680/2016 does not, in turn, establish the principles governing its action, nor does it make any reference to transparency in the processing of personal data, which is otherwise understandable, on the one hand, if we refer to the specific institutions that come to implement it. Recommendation no. 26 of the Preamble to the directive under review speaks of the principles that need to be respected when processing such data[2], but such recommendations are important in the EU legal order, but not legally binding (Dumitru & Stoican, 2020) and therefore do not produce legal effects *per se*, but rather have the role of providing assistance in interpreting the legal text or in the face of legal gaps.

Similarly, Recommendation 38 of the Preamble refers to a specific right of the data subject[3], but the right to explanations is not found in the articles of the Directive in question, although it would be a right to post-factum explanations for automatic processing or profiling.

Thus, the processing of data (metadata[4]) and information by national security institutions will take place in the context of their efforts to prevent and combat crime, but in compliance with the provisions of EU Directive no. 680 / 27.04.2016[5] as transposed into the legislation of the Member States and in a manner necessary and proportionate to the purpose pursued. At the same time, we consider that the reporting to art. 8 of the ECHR[6] is needed, especially given that the European Court of Justice has treated the Convention as a source of inspiration, but which "does not prevent the provisions of Union law from providing more extensive protection" (Craig & Burca, 2011).

2. Background Analysis

The age of the Internet, the advancement of technology and information technology in general, and the increasingly widespread and less restrictive use of social media on a global scale have provided law enforcement institutions with the appropriate means to gather data and information needed for their activity, giving them the opportunity to collect and process efficiently and without the knowledge of data subjects, huge amounts of personal data that are latent and free in the online environment and beyond. But this unprecedented technological boom has created challenges both for law enforcement institutions and for the legislator / regulator, and especially for the beneficiaries of national security measures who are, at the same time, subjects of the process of collecting personal data.

Thus, there was an increasing need for the above-mentioned institutions and the legal framework governing their activity to be able to adapt promptly to rapid social and technological changes in order to ensure adequate protection for the security of the citizen and the rule of law, in parallel with the protection of the fundamental

rights and freedoms of citizens and related to the four directions of data surveillance at EU level in the fight against terrorism:

- supervision of electronic communications metadata;
- travel data monitoring;
- supervision of financial data;
- data surveillance on the internet (Tzanou, 2017).

This is the general framework in which the legislation regulating the processing of personal data by national security institutions, and by law enforcement institutions, respectively, was enacted, in this case EU Directive no. 680 / 27.04.2016 above-mentioned, transposed into Romanian legislation by Law no. 363/2018 (Sandru, 2021). We specify that when enacting Directive 680/2016, there was also taken into account the previous experience generated by the declaration as invalid by the European Court of Justice of Directive 2006/24 / EC[7] by decision in Related Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others[8].

In this context, art. 10 of Directive (EU) 2016/680, and art. 10 of law no. 363/2018[9], respectively, transposing the directive into Romanian law establishes the so-called special categories of personal data[10], which may be processed exclusively subject to conditions *sine qua non*:

- The processing must be expressly provided by law. This wording is much more restrictive than the one provided in Directive 680/2016, which talks about the need for processing to be authorized by European Union or national law, without specifying how to authorize or the extent of this authorization.

- The protection is necessary to defend the vital interests or concerns of the data subject / of another natural person, which is transposed into Romanian law under the wording regarding the need to prevent an imminent danger to life, bodily integrity or health. In assessing the severity of social danger, the Romanian legislator refers to the most important protected social values, namely life / health. As a result, the production of material damages, even significant ones, cannot be considered as representing a social danger sufficiently important to justify the processing of data from the special categories listed exhaustively by the legislator.

- If, however, the data subject has made public data manifestly, they can be freely processed by law enforcement institutions as it indicates that they assume the risk of processing. The following question arises: Did the European legislator also take into account the fact that, "artificial intelligence is increasingly able to obtain privacy from… freely and innocently shared information such as: where did you eat lunch, for example, or what, what you bought at the grocery store? - and it can lead to deeply sensitive and personal details" (Calo, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015350).

However, all these conditions must be corroborated by the need for the competent institutions to work in a well-defined case and, simultaneously, to provide adequate guarantees for protecting the natural rights and liberties of the person. Art. 10 does not specify the nature or extent of these guarantees. This task returns to art. 37 of the above-mentioned law. From the analysis of this article we

find that the legislator imposes an obligation on the operator who must document all cases of personal data breach and, in addition, keep the documents for a period of 5 years, as well as inform the jurisdictional authority without undue delay. At the same time, the same legislator introduces a random element in this process that is intended to be one of guaranteeing personal rights and freedoms. Thus, notification is not necessary if the breach of personal data security is not likely to pose a risk to the rights and freedoms of individuals (Art. 36 of Law no. 363/2018). However, the gravity and nature of this risk are to be assessed by the institution itself, which had to ensure that this infringement did not occur.

Probably out of the desire to provide other guarantees regarding the protection of privacy and personal data, the legislator also introduces a series of deadlines to be met regarding the deletion of personal data or the regular review of the need to store personal data (Art. 5 of Directive 680/2016). These terms represent, in fact, the assurance of a right to be forgotten, parallel to the right established by art. 17 to the GDPR. However, we believe that there must be sufficient enough safeguards to ensure, at all and any times, the effectiveness in eliminating the risk of abuse and misusage and against any unauthorized access or illegal use of personal data. Thus, a practical and extremely present aspect in the economic and financial life of any operator must be taken into account, namely the economic aspect that any operator will consider when determining the level of security measures it applies (i.e., the costs of implementing protection and security measures) or when irreversible destruction of all the data will be resorted to at the end of the retention period established by law.

A series of clarifications are required:

Technological developments have allowed data and information to be stored for a very long time, even longer than the natural life of human memory. This longevity of digital files allows law enforcement institutions to perform automated searches that are virtually unlimited in time. Hence the growing interest of such institutions to create databases and archive information. However, there are cases when it is preferable to have such a "forgetfulness" of personal data of individuals (Blanchette & Johnson, 2002) such as, for example, the situation of juvenile offenders who would thus have the chance to start life again in relation to state institutions and their records. As a result, we believe that a number of principles should be discussed that should govern the right to use and store personal data, such as the principles of necessity and proportionality that should be related to the need for law enforcement institutions to conduct efficient and accurate legal investigations. At the same time, the purpose of long-term retention of evidence should be analyzed in relation to the degree of social peril of the offence under investigation, its general complexity and, also, the damage that could be done to the subjects of long-term investigation, especially if it is a social reintegration. In this regard, the opinion of the ECHR, which unanimously considered that the indefinite retention by the British police of biometric data (DNA profile and fingerprints) and photographs of a person convicted of a crime punishable by imprisonment, must also be taken into account as a breach of art. 8 concerning the right to private and family life (Gaughran v. The

United Kingdom)[11]. Thus, the Court considered that without respecting the necessary proportionality to the legitimate objectives assigned to such storage mechanisms, the advantages provided by them would be harmed by the serious infringements which they would cause to the rights and freedoms that States must guarantee under Convention[12] of persons in their custody. At the same time, the Court considered that the United Kingdom should have established effective safeguards for the applicant concerned, including a real capacity, not a hypothetical one, to assess the process of keeping his data in view of the nature of the crime, the age of the person concerned, also the elapsed period of time along with the current personality of that person"[13].

In the same context, we must observe the solution adopted by the CJEU on 21.12.2016 in a specific case[14] who stated that "Member States may not impose a general obligation to retain data by providers of electronic communications services"[15] but rather established a new solution - "targeted retention (retention of data)" as a tool able to effectively support the fight against serious crime (Grabowska-Moroz, 2021). Thus, the Court stated that, although EU law precludes a general and non-discriminatory possession of traffic and position data, Member States may provide, as a precautionary measure, for the targeted retention of such data only for the purpose of combating serious crime, provided that this retention be (as regards the categories of data to be retained, the means of communication involved, the data subjects and the chosen retention period) limited to what is regarded as strictly necessary. Also, the access of the above-mentioned data to the national authorities must be subject to certain conditions, including previous review from the independent authority on retention of the data in the European Union[16].

Regarding the automated data processing, respectively the process automation methods used in the OSINT (Open Source Intelligence) activity, art. 11 of the same directive establishes the obligation for Member States to ensure that a decision based solely on automatic processing, including profiling, which has a negative legal effect on the person concerned or which significantly affects him, is prohibited. *Per a contrario*, processing which has no harmful effect or which does not cause major damage is permitted. The issue of assessing the intensity and extent of the effects remains, and these are considered to be adequately assessed through the intervention of the human operator. The following issues arise: profiling is allowed, unless decisions are made solely on the basis of automatic assessment or result in discriminatory decisions based on these profiles. However, the legislator does not talk in these articles about how to calibrate the profiling that may be based on discriminatory criteria or result in decisions of a discriminatory nature or lacking fairness and clarity.

Thus, it should be noted that the technical process by which a development of analytical tools based on algorithms is required, necessarily involves the use of various data sets, obtained by increasingly sophisticated means and methods such as body worn video cameras, so-called crowdsourced images, CCTV images, traffic video recordings, etc. This data will be processed automatically and will result in a materialized analysis in the form of an investigation report. In the context of criminal

proceedings, we believe that in order to ensure a fair and non-discriminatory or random assessment, the outcome of the investigation should not be assessed in isolation and, at the same time, both the video recordings and their analysis or investigation report should be assessed together in court (Leroux, 2004).

European and national legislation, respectively, provide for different legal implications and procedures, depending on the parties involved in the exchange or transfer of data, public or private legal persons. At the same time, the nature of the data processed (commercial information, audio-video materials, data from operational records or criminal records) and the intended purpose are important, as they may vary from judicial proceedings / criminal investigation to research and development. All these elements will establish the applicable law, i.e., Directive 680/2016 or the General Data Protection Regulation (GDPR).

Last but not least, it should be remembered that there are situations in which the processing is carried out in circumstances that do not fall within the scope of personal data protection legislation, respectively when it comes to the processing and sharing of anonymized data, in which case none of the above-mentioned normative acts, national criminal law or criminal procedure legislation may become incidents. In this situation, the obligations of personal data controllers are rather enshrined in national law and, consequently, may be transferred from one Member State to another or depending on the nature of the data, historical, operational, data based on facts or based on personal assessments (Art. 7 of Directive 680/2016). Thus, in the criminal process, law enforcement authorities/agencies will be obliged, based on the presumption of innocence, to comply with the obligations of confidentiality and secrecy regarding data and information obtained in the investigation and prosecution of specific crimes, the access being restricted to those who have a legitimate interest in accessing information, controls and procedures may be imposed to monitor and restrict access to personal data, in the framework of the procedure for ensuring respect for the right to protection of personal data.

The European legislator also introduces an exception, namely the situation where automatic processing is considered to be:

1. Authorized by Union / national law applicable to the operator;
2. The legislation provides adequate defenses for the birthrights and liberties of the data subject, respectively at least the above-mentioned right to obtain the specified human intervention from the operator. We tie-up that the right to obtain an intervention in the sense of human analysis so that the decision is not taken only on the basis of automated analysis, is a minimum right / guarantee that must be provided to the person concerned by the reference legislation. At the same time, however, the legislator does not have practical measures to ensure this human intervention or to provide clear and undeniable guarantees designed to remove profiling on the above-mentioned discriminatory criteria, which are strictly prohibited by law, but leaves this behavior to the operators, as it results from art. 12, respectively 13 of the mentioned national law. In this context, we believe that it was imperative that appropriate, practical measures be put in place to protect the already mentioned rights, freedoms and legitimate interests of the data subject, beyond the

obligation to respond to data subjects' requests for such processing, in particular that it is about the creation of profiles that result in discrimination of individuals based on the special categories of personal data mentioned above, a ban clearly established by art. 11 para. 2, 3 of the European legislation, respectively the Transposition Law no. 363/2018. This is because, in the absence of the data subject's request or the risk posed by a security incident, we do not find a specific obligation to inform the operator. Thus, art. 13 sets the minimum but also the maximum limits of the content of the information to be supplied to the data subjects, but does not stipulate the way the data of the subjects are processed or regarding the existence of an automatic decision.

In the context of the rapid evolution of Artificial Intelligence systems and the challenges posed by this mode of processing that create gray or unaddressed areas in the current regulation, a situation specific to each data-intensive technology, regulations such as GDPR or Directive 680/2016 will always be behind the new advances in technology, or "just because it is too difficult for regulatory change to keep pace with technology" (Fosch Villaronga & Kieseberg & Tiffany, 2018). Therefore, we believe that the right of data subjects to information should also include the right to know whether their data have been processed by processing and analysis tools based on AI systems. Thus, we agree with the view expressed in the doctrine[17] that Article 13 (2) (d)[18] may apply under subject to the provisions of Article 13 (3)"[19] which, moreover, do not differ from those referred to in the relevant basic regulation, namely Article 23 (1), (a), (c), (d) and (i), from the GDPR, stating that Member States "may" (according to Article 13 (4)) list the categories of processing subject to the restrictions referred to in Article 13 (3). Added to this is the need to differentiate between the identification of a natural person and the detection and tracing of a natural person, as well as between individual surveillance and mass surveillance[20].

However, the legislator comes to complete, to a certain extent, these provisions with a series of technical and procedural provisions that we find in art. 7, 35-37 of the national law or in other disparate provisions of Directive 680/2016 and the law transposing into Romanian law, but we it consider insufficient.

In parallel, we cannot fail to state that, although apparently both normative texts, the mentioned directive and the transposition law have the same meaning, there are differences between them that can lead to different interpretations from the courts that will have to resolve possible conflicts tasked with reporting on the direct or indirect effect (Dumitru & Stoican, 2020) of European legislation and the aim pursued by the enactment of that Directive (to harmonize the relevant provisions of the Member States), also related to the aim pursued by the main legislation, namely the EU Regulation) no. 679/2016 (GDPR)[21], which came to regulate and update the legislation in the field (Chirica, 2017).

It should be mentioned that, as stated above, art. 13 sets out measures that can be considered both control and protection of data subjects, namely the fact that, at their request, the operator makes available to data subjects a set of information (additional information may be provided, but not less than that). In this context, the solution of

the ECHR in the case of Liberty and others v. The United Kingdom[22], which found that an internal act of the United Kingdom (The Interception of Communications Act of 1985), based on which data belonging to civil liberties organizations were intercepted, was a violation of the same Article 8 of the above-mentioned European Convention on Human Rights, as it allowed an excessively wide scope of action of the authorities to intercept communications without providing guarantees against abuse of power.

The provision of this kind of information to the targeted subject will enable the individual to assess whether we find ourselves in the presence of a breach of the subject right to the protection of personal data and/or of his or her distinctly regulated right to privacy. Without correct information of the data subject, he / she will not be able to pertinently establish his / her future actions or to exercise his / her right to an effective judicial remedy, as provided by art. 53-54 of Directive 680/2016. In their turn, the courts called to decide on possible cases of violation of the law, respectively the compliance of the operators with the principles of legal and fair processing provided in art. 4 para. 1 lit. a of the same directive will not be able to fulfill this obligation knowingly. Last but not least, also on the basis of the information provided by the operators, respectively the institutions in the field of national security, it will be possible to establish whether a system has been established illegally, which winds up in discrimination of individuals on the basis of special categories of individual data referred to in Article 10 (Art. 11, para. 3 of Directive 680/2016).

Likewise, as provided by art. 36 of Law no. 363/2018, "the operator who finds a breach of data security, shall notify the supervisory authority without undue delay". At the same time, the controller is obliged to fill in the data subject regarding the security incident notified to the supervisory authority only if the breach of security is likely to pose a high risk to the rights and freedoms of personas. However, the phrase "high risk" is encountered in the content of art. 39 of the analyzed law.

We consider, however, that the provisions of para. 4 of the above-mentioned article according to which the supervisory authority notified by the operator according to the obligations provided in art. 36, is, in fact, the real guarantee for the fair information of the person concerned about the incident and the possibility of suffering an injury. According to the provisions of art. 35, "the controller or, as the case may be, the person authorized by the controller is obliged to carry out an assessment of the risks incident to the intended processing", therefore the aim is the mandatory implementation of an obligation regarding an anticipatory analysis that must take place before the personal data processing procedure of the data subject. We agree with the view expressed in the doctrine that the scope of evaluations must be even wider in the sense that evaluations of the impact on data protection must be carried out, even before the implementation of high-risk technologies (Lilian, 2020).

Clearly, needs relating to the protection of public order and safety, investigations and proceedings of a judicial nature or the protection of the rights of others are necessary but also sufficient grounds for Member States to adopt legislative measures (following an ordinary or special legislative procedure), which are to allow

a postponement, restriction/omission of delivering the information to the data subject. It is clear that the categories of processing may be covered, in whole or in part, by such actions, but provided that such action is a necessary and proportionate proceeding in a self-governing society, having regard to fundamental rights and by the legitimate interests of the natural person. We consider that when we talk about a "democratic society" we must unmistakably refer to the values that are being provided in art. 2 of the TEU[23], despite the increasingly obvious challenges on the part of some Member States[24] to respect these principles and the rule of law as they are governed by European law[25]. At the same time, reference should be made, as mentioned above, to the fact that, in a solution, the European Court of Justice stated that although EU law precludes a general and non-discriminatory retention of traffic and location data, Member States may provide, as a precautionary measure, for the targeted retention of such data only for the purpose already mentioned (of combating serious crime, provided that such retention is, as regards the categories of data to be retained, the means of communication involved, the data subjects and the duration chosen for storage) limited to what is rigorously necessary. The access of the retained data to the national authorities must be subject to certain conditions, including prior review by the independent authority and retention of the data in the European Union (https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf).

3. Conclusions

There are, of course, a number of conclusions of a theoretical nature, but especially practical:

1. Personal data controllers must be constantly aware that the processing of data by or using automated systems will almost always lead to the use of personal data and, as a consequence, may constitute a breach of the provisions on the right to privacy, the protection of the above mentioned personal data or fundamental right of confidentiality. The ECFR (https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf) has explicitly enshrined these rights as two fundamental and, simultaneously, distinct rights. The right to have respect for private and family life ensures and guarantees to any person, in fact, protection for home life over and above the privacy assumed by the legal institution of the family, but also on communications (Art. 7 of the European Charter of Fundamental Rights). On the other hand, this right, as regulated by that Charter, guarantees everyone the right to the protection of such data concerning them. Here is a clear distinction that limits the scope of the notion of personal data.

2. As technological developments are extremely rapid and the technical characteristics of new technologies are often difficult to understand, the legislator and policy makers will find themselves in a situation where they have to take into account both potential violations[26] through unregulated technologies, as well as the effect resulting from the interconnection of different surveillance, collection, processing data analysis systems. In this contexture, it should be highlighted that the use of unregulated technologies for obtaining evidence has been classified by the

ECHR as a violation of the right to privacy[27]. Nevertheless, the areas of data protection and privacy have been frequently invoked to challenge the EU's executive action (Craig & Burca, 2011) and to call for the active intervention of the European Commission as an exponent of the executive branch.

3. In the absence of a binding, coherent and coordinated legal framework, clear and detailed guarantees provided by the above-mentioned legal mechanism to ensure an adequate level of legal protection for those who have access to personal data, on the one hand, and mechanisms for supervising, sanctioning and resolving disputes, on the other hand, the access and exchange of personal data and not only, carried out in a timely, rapid and efficient manner, between cross-border competent institutions will remain an unequivocally regulated or even unregulated reality (Dumitru, Chirieac, 2/2020). We consider that, beyond the letter of the law and the specifics of the legislation of the European Union, its spirit must be taken into account in all situations and, consequently, in the interpretation of each concrete case, it is necessary to refer to the provisions of art. 4 para. 2 of the TEU. Note especially the closing part of this paragraph ("In particular, national security remains the sole responsibility of each Member State"). We therefore agree with the opinion[28] that EU law, including the CFREU (the Charter of Fundamental Rights of the European Union: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN), should not apply to matters concerning the national security of the Member States of the EU. This is an important thing to keep in mind at all times, the challenges that Member States face in terms of protecting national security and the specific threats to it that may come from both inside and especially from outside. And as long as there is not yet a unified approach to security in the European Union, as long as we are not talking about a common defense policy or a unified, rapid and coherent approach to threats to the security of the Union as a whole and of the Member States as immanent divisions, we believe that it must remain the responsibility of national states to adopt the best solutions to prevent and combat these types of threats. Ultimately, it must not be forgotten that the European legislator adopted this normative act in the form of a directive, so that its provisions apply within the limits and conditions implemented in national legislation, as they have been adapted to local specificities.

4. We also consider that the provisions of the GDPR and of Directive no. 680/2016 will outline, mandatorily, through the obligations established for the operators, the direction of development of AI, machine learning and NLP as well as of the eventual and subsequent technological developments specific to this field of application.

5. Last but not least, the entire legal framework governing the protection of individual data and privacy must be constantly harmonized with the principles of the so-called Area of Freedom, Security and Justice (AFSJ)[29], which can be a step forward in creating global data protection rules (Casagran, 2017).

References

[1] Grabowska-Moroz, B. (2021). *Data Retention in the European Union în Law, Governance and Technology Series Issues in Privacy and Data Protection 45*, *European Constitutional Courts towards Data Retention Laws*, Springer Nature Switzerland AG.

[2] Blasi Casagran, C. (2017). *Global Data Protection in the Field of Law Enforcement An EU Perspective*, Routledge, London.

[3] Fosch Villaronga, E., Kieseberg, P. and Tiffany, L. (2018). Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten*, Computer Law and Security Review* 34.

[4] Blanchette, J.-F. and Deborah, G. J. (January 2002). Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness, *The Information Society* 18, no. 1 https://doi.org/10.1080/01972240252818216.

[5] Mitrou, L., University of the Aegean (2019). Data protection, artificial intelligence and cognitive services. Is the general data protection regulation (GDPR) "artificial intelligence-proof"?, Available at SSRN: https://ssrn.com/abstract=3386914 or http://dx.doi.org/10.2139/ssrn.3386914.

[6] Tzanou, M. (2017). *The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance*, Hart Publishing, Oxford and Portland, Oregon.

[7] Dumitru, O. I., Chirieac, R. (2020). Societățile holding în cadrul reglementărilor de schimb automat de informații*, Revista Pandectele Române [*Holding companies within the regulations for automatic information exchange*, Pandectele Române Magazine]*, nr. 2/2020.

[8] Dumitru, O. I., Stoican, A. (2020). *European Union Law, Lecture Notes*, ASE Publishing House, Bucharest.

[9] Leroux, O. (July 2004). Legal Admissibility of Electronic Evidence*, International Review of Law, Computers & Technology* 18, no. 2, https://doi.org/10.1080/1360086042000223508.

[10] Craig, P., de Búrca, G. (2011). *EU Law. Text, Cases, and Materials*, Fifth edition, Oxford University Press, Oxford.

[11] Calo, R., Artificial Intelligence Policy: a primer and roadmap, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015350.

[12] Chirică, S. (2017). The main novelties and implications of the new general data protection regulation, *Perspective of Business Law Journal*, vol. 6, Bucharest.

[13] Șandru, S. (2021). *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.

[14] Working Document on surveillance of electronic communications for intelligence and national security purposes adopted on 5 December 2014.

[15] 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.

[16] Article 29 Data Protection Working Party, (29 November 2017 *), Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)*, http://ec.europa.eu/ newsroom/just/document.cfm?doc_id=48804.

[17] https://www.europarl.europa.eu/news/ro/press-room/20180906IPR12104/statul-de-drept -in-ungaria-parlamentul-cere-ue-sa-actioneze.

[18] https://ec.europa.eu/romania/news/20200429_stat_de_drept_polonia_ro.

[19] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L0680.

[20] https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506- fd71826e6da6.0001.02/DOC_1&format=PDF.

[21] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403: ro:PDF.

[22] https://app.justis.com/case/pg-and-jh-v-united-kingdom-app-no-4478798/overview/ c4utoZeZm1Wca.

[23] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-69188%22]}.

[24] https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-200817%22]}.

[25] https://www.echr.coe.int/documents/convention_ron.pdf.

[26] https://www.legal-tools.org/doc/315a62/pdf/.

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

[28] https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf.

[29] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12012P/TXT&from =EN.

[30] https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf: Press release No 54/14 Luxembourg, 8 April 2014.

[31] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-87207%22]}.

[1] 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).

[2] "any processing of personal data must be lawful, fair and transparent to the individuals concerned".

[3] The right to "specific information and the right to obtain human intervention, in particular to express the individual point of view, to receive an explanation of the decision taken following such an assessment, or to challenge the decision".

[4] The so-called data about data. See art. 2 of Directive 2002/58 / EC of 12 July 2002 on the processing of personal data and the protection of confidentiality in the public communications sector (Directive on confidentiality and electronic communications) as well as art. 3 of the Proposal for a Regulation on the protection of privacy and the protection of personal data in electronic communications and repealing Directive 2002/58 / EC (Regulation on confidentiality and electronic communications).

[5] 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.

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

[7] Directive 2006/24 / EC[7] on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58 / EC.

[8] https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf: Press release No 54/14 Luxembourg, 8 April 2014.

[9] 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.

[10] "racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union affiliation, processing of genetic data, processing of biometric data for the unique identification of to a natural person or the processing of health data or data on the sexual life and sexual orientation of a natural person".

[11] Gaughran v. The United Kingdom (Application no. 45245/15), 13.02. 2020, First Section, https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-200817%22]}.

[12] European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ ENG.pdf%23page=9.

[13] Gardel v. France (Application no. 16428/05), 17.12.2009, https://www.legal-tools.org/doc/315a62 /pdf/.

[14] Case C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for Home Affairs v. Tom Watson and others.

[15] https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf: Press Release No 145/16 din 21.12.2016.

[16] See also the ruling CJUE in Related Causes C-293/12 and C-594/12 Digital Rights Ireland și 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 out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.

[17] Article 29 Data Protection Working Party, (29 November 2017) *'Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)'*, p. 15, http://ec.europa.eu/newsroom/just/document .cfm?doc_id=48804.

[18] Directive 680/2016, art. 13, para. 2 lit. d:) where necessary, additional information, in particular when personal data are collected without the knowledge of the data subject.

[19] Member States may adopt legislative measures to postpone, restrict or omit the provision of information to the data subject in accordance with paragraph 2 in so far as such a measure constitutes a necessary and proportionate measure in a democratic society, taking into account take into account the fundamental rights and legitimate interests of the natural person, in order to:

(a) avoid obstruction of official or legal investigations, inquiries or proceedings;

(b) not prejudice the prevention, detection, investigation or prosecution of criminal offenses or the execution of sentences; (c) protection of public security;

(d) protection of national security;

(e) the protection of the rights and freedoms of others.

[20] 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).

[21] 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).

[22] https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-87207%22]}: Case of Liberty and Others v. The United Kingdom, Application no. 58243/00, Strasbourg, 1 July 2008.

[23] 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.

[24] https://www.europarl.europa.eu/news/ro/press-room/20180906IPR12104/statul-de-drept-in-ungaria-parlamentul-cere-ue-sa-actioneze.

[25] https://ec.europa.eu/romania/news/20200429_stat_de_drept_polonia_ro.

[26] To be seen AFFAIRE VETTER c. FRANCE (Requête no 59842/00) Deuxième Section, 31.05. 2005, (https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-69188%22]}).

[27] To be seen P.G. and J.H. v. the United Kingdom - 44787/98 Judgment 25.9.2001 [Section III] (https://app.justis.com/case/pg-and-jh-v-united-kingdom-app-no-4478798/overview/c4utoZeZm1Wca).

[28] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf: Working Document on surveillance of electronic communications for intelligence and national security purposes adopted on 5 December 2014, p. 22.

[29] Regulated since the entry into force of the Amsterdam Treaty in 1997, it is a collection of internal affairs and justice policies. It is regulated in art. 3 para. 2 of the Treaty on European Union and art. 67-89 of the Treaty on the Functioning of the European Union.