PERSONAL DATA PROTECTION ISSUE REFLECTED IN THE CASE-LAW OF THE CONSTITUTIONAL COURT OF ROMANIA

Valentina BĂRBĂȚEANU*

Abstract

Over the past few years, data privacy became more and more an issue that stirred on European level lots of debates and determined the adoption of a new set of rules, imposed with the compulsory force of a European regulation. Thus, the EU General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC and reshaped the way the data are managed in various fields of activity. In Romania, the Constitutional Court had to bring light over important areas that involved the use of personal data and developed a relevant case-law regarding the concordance with the essential standards implied by the protection of private life enshrined both in the Romanian Basic Law and in the European Convention on Human Rights. The paper intends to depict the main challenges that faced the constitutional review and the measure that the Romanian vision over this problem is consistent with the European landmarks set in this field.

Keywords: *right to privacy, personal data, European regulation, constitutional review, constitutional case-law.*

1. Introduction

The digital age that reigns nowadays has changed not only the way people interact, but also the way the states themselves position their legislation towards the technological progress. Day by day, due to the constant increase of accessibility of various kind of electronic devices, more efficient and attractive the electronic communications become and more complex and diverse are the tasks and activities that ordinary people can be involved in. Consequently, the higher becomes the risk of privacy breaches. The so-called 'datacraty' imposed its authority over the quasi-entirety of the social life[1]. In order to avoid the negative effects of exposure of the citizens' personal data, a set of rules meant to diminish this risk has been implemented at the European Union level.

The main idea that is in the core of all these rules is the protection of the right to respect for private life, also referred to the right to privacy. The right to personal data protection derives in a logical manner from the first mention right. Each state has also created a national system of protection, taking into consideration the European general framework.

This European framework also includes the Council of Europe's system, as well. In this regard, the European Convention on Human Rights (ECHR), one of the first major regulations at the European level, provides, in Article 8, that everyone has the right to respect for his or her private and family life, home and correspondence. Interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, pursues important and legitimate public interests and is necessary in a democratic society. An iconic judgement of the European Court on Human Rights recognised in 2017 that Article 8 of the ECHR, that grants the right to respect for private life also "provides for the right to a form of informational self-determination" (ECtHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 27 June 2017, para. 137).

Romania has embraced the European normative spirit. The legal provisions adopted to this end have made the object of the constitutional review performed by the Constitutional Court. It played an important role in correcting the deviations from the principles of the Romanian Basic Law which grants the right to private life, also keeping in mind the European philosophy in this field. The present paper will focus on the case-law of the Romanian Constitutional Court in the area of protection of personal data, trying to offer a comprehensive view on this topic. The paper will integrate the overview on the fore-said case-law with the case-law of Court of Justice of the European Union and other constitutional courts in Europe.

2. Content

2.1. Legal framework at the European level

A clear view over this topic requires a brief presentation of the legislative acts that regulates over the time and some of them still regulate the mechanism of personal data protection.

At the European level, the basic provisions in this field are represented by **Article 16 of the Treaty on the Functioning of the European Union** that recognize to everyone the right to the protection of personal data concerning them.

This right is further provided by **Charter of Fundamental Rights of the European Union** (the

* Asistant Professor, PhD, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: valentina_barbateanu@yahoo.com);

[1] Relevant in this direction is, for instance, the fact that the famous review "Pouvoir" has dedicated a whole number to this topic. See Pouvoir, La datacratie, no.164/2018.

Charter), **Article 8** (right to protection of personal data). It details its content, stressing, in the second paragraph, that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. It also grants to everyone the right of access to data which has been collected concerning him or her, and the right to have it rectified.

For quite a long period of time, **Directive 95/46/EC** on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2] (Data Protection Directive) has been the source of inspiration for all the member states in what concerns this issue. It has been in effect until May 2018, when the new General Data Protection Regulation entered into force.

Of great importance was also the **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.

The fore-said directives co-existed with the **Council Framework Decision 2008/977/ JHA** on the protection of personal data processed in the context of police and judicial cooperation in criminal matters[3], which was in effect until May 2018.

The overwhelming development of electronic communications raise the need of a more complex and more safeguarding set of rules. Thus appeared the **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 (the so-called General Data Protection Regulation (GDPR)[4]. It regulates the processing by an individual, a company or an organization of personal data relating to individuals in the European Union. It means that EU data protection rules apply also to organizations and other entities that are not established in the EU, if they process personal data and offer goods and services to data subjects in the Union or monitor the behavior of such data subjects.

To complete the European legal framework a last directive has been adopted: **Directive (EU) 2016/680** on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

All these European normative acts have shaped the member states of the EU have re-configured their national regulations in this field. Accordingly, Romanian Parliament has adopted several laws that took over the provisions of the cited directives.

2.2. CJEU's relevant case-law regarding the personal data protection issue:

The introduction in the European Union's normative acts wouldn't be complete if we do not mention the European Court's of Justice judgement that declared void the main directive dedicated to the protection of personal data.

Thus, Directive 2006/24/EC was declared invalid through ***the Judgment of Court of Justice of the European Union of 8 April 2014, pronounced in the joint cases C-293/12 — Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others — and C-594/12 — Kärntner Landesregierung and others***. Through the above-mentioned judgment, the European court found that the analyzed directive violated the provisions of Article 7, Article 8 and Article 52 (1) of the Charter of Fundamental Rights of the European Union**.**

The Court of Justice of the European Union concluded that the measures stipulated by Directive 2006/24/EC, although they are able to achieve the pursued objective, represent an interference with the rights guaranteed by Articles 7 and 8 of the Charter, which does not comply with the principle of proportionality between the taken measures and the protected public interest.

The Court noted in this regard that the data which made the object of the invalidated directive's regulation led to very precise conclusions on the private life of the persons whose data have been retained, conclusions that may relate to the habits of everyday life, the places of permanent or temporary residence, the daily movements or other movements, the activities, the social relations of these persons and the social environments frequented by them (paragraph 27) and that, in these conditions, even if it is prohibited to retain the content of the communications and pieces of information consulted by using an electronic communications network, those data retention can affect the use by subscribers or by registered users of the communication means stipulated by this directive and, therefore, their freedom of expression, guaranteed by Article 11 of the Charter (paragraph 28)**).**

The Court of Justice of the European Union also indicated that the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, caused by the provisions of Directive 2006/24/EC, was wide-ranging and must be considered as being particularly serious, and the circumstance that data retention and their subsequent use were performed without the subscriber or registered user being informed about this was likely to generate in the minds of the persons concerned the feeling that their private life makes the object of a constant supervision (paragraph 37)**.**

It was also alleged that Directive 2006/24/EC did not stipulate objective criteria to limit to the absolute

[2] Official Journal of EU, 1995, L 281.
[3] Official Journal of EU, 2008, L 350.
[4] Official Journal of EU, 2016, L 119.

minimum the number of persons who have access and can subsequently use the retained data, that the access of national authorities to stored data is not conditioned by the prior control performed by a court or by an independent administrative entity, limiting this access and their use to the absolute minimum for the achievement of the pursued objective and that the obligations of Member States to establish such limitations is not stipulated (paragraph 62).

2.3. The Constitutional Court's of Romania case-law regarding the personal data protection

2.3.1. One of the most worthy details to be mentioned when approaching this issue is the fact that prior to the fore-cited judgment of the CJUE, the Constitutional Court of Romania had rendered a decision, **Decision no. 1.258 of 8 October 2009[5],** by which it stated that the Law no. 298/2008 on the retention of data generated or processed by the providers of publicly available electronic communications services or of communications networks, which was the first transposition in the national legislation of the Directive 2006/24/EC, was inconsistent with the provisions of the Romanian Basic Law.

We notice the clairvoyant attitude of the Romanian Constitutional Court that has foreseen the radical solution adopted by the CJUE five years later. We also underline that on the 2nd of March 2010, soon after the Romanian Constitutional Court, Federal Constitutional Court of Germany has also rejected the German legislation requiring electronic communications traffic data retention that implemented the similar EU Directive[6].

By Decision no. 1.258 of 8 October 2009, the Court held that Article 1 (2) of Law no. 298/2008 also included in the category of traffic and location data for individuals and legal entities *"the related data necessary for the identification of the subscriber or registered user"*, without expressly defining what is meant by the phrase *"related data"*. It was indicated that the absence of precise legal rules that would determine the exact scope of those data needed to identify the user - individuals or legal entities, left room for abuse in the work of retention, processing and use of data stored by providers of publicly available electronic communications services or of public communications networks and that the restriction on the exercise of the right to intimate life, secrecy of correspondence and freedom of expression must also occur in a clear, predictable and unequivocal manner, as to be removed, if possible, the occurrence of arbitrariness or abuse of authorities in this area.

Likewise, the Constitutional Court noted the same ambiguous wording, not compliant with the rules of legislative technique, also as concerns the provisions of Article 20 of Law no. 298/2008, reading as follows, *"In order to prevent and counteract threats to national security, State bodies with responsibilities in this area, in the terms set forth by the laws governing the activity of protection of national security, can have access to data retained by service providers and public electronic communications networks"*. The legislature does not define what is meant by *"threats to national security"*, so that in the absence of precise criteria of delimitation, various actions, information, or normal activities, of routine, of natural and legal persons can be considered, arbitrarily and abusively, as having the nature of such threats. Recipients of the law may be included in the category of suspects without knowing it and without being able to prevent, by their conduct, the consequences that their actions may entail and that the use of the expression *"can have"* also leads to the idea that the data covered by Law no. 298/2008 are not retained solely for the use thereof only by State bodies with specific powers to protect national security and public order, but also by other persons or entities, since they *"can have"*, and not just *"have"*, access to such data, according to the law.

By the same decision, the Constitutional Court has found that Law no. 298/2008, as a whole, established a rule regarding the continuous retention of personal data, for a period of 6 months as from the time of their interception. Or, in the matter of personal rights, such as the right to personal life and the freedom of expression, as well as of processing of personal data, the widely recognized rule is to ensure and guarantee their observance, respectively of confidentiality, the State having, in this respect, mostly negative obligations, of abstention, by which should be avoided, insofar possible, its interference in the exercise of such right or freedom. It was underlined that exceptions are restrictively allowed, in the terms expressly provided by the Constitution and the applicable international legal instruments in the field, and Law no. 298/2008 represents such an exception, as it results from the title itself.

The Court has also found that the obligation to retain data covered by Law no. 298/2008, as an exception or derogation from the principle of protecting personal data and confidentiality thereof, by its nature, extent and scope, deprived this principle of content, as it was guaranteed by Law no. 677/2001 for the protection of individuals concerning the processing of personal data and free circulation of such data and Law no. 506/2004 on the personal data processing and protection of private life in the electronic communications sector. Or, it is widely recognized in the caselaw of the European Court of Human Rights, for example, by Judgment of 12 July 2001, rendered in *the case of Prince Hans-Adam II de Lichtenstein v. Germany*, paragraph 45, that the Contracting States under the Convention on Human Rights and Fundamental Freedoms have assumed such obligations to ensure that the rights guaranteed by the Convention are practical and effective not theoretical and illusory,

[5] Published in the Official Gazette of Romania, Part I, no. 798 of 23 November 2009.
[6] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.

the legislative measures adopted following the effective protection of rights. But the legal obligation that requires the continuous retention of personal data makes the exception to the principle of effective protection of the right to personal life and freedom of expression, absolute as a rule. The right appears to be regulated in a negative fashion, its positive side losing its predominant character.

Therefore, the regulation of a positive obligation on a continual limitation on the exerciser of the right to a private life and secrecy of correspondence cancels the very essence of the right by removing the guarantees applying to its exercise. Natural and legal persons, mass users of publicly available electronic communications services or of public communications networks are continually subject to the interference in the exercise of their personal rights to private correspondence and free expression, without any possibility of a free, uncensored manifestation, only under the form of direct communication, to the exclusion of the main means of communication currently used.

Likewise, through Decision no. 1.258 of 8 October 2009, the Court held that in a natural logic of this analysis the examination in this case of the principle of proportionality was also necessary, which represents another mandatory requirement needed to be respected in cases of limitation on the exercise of the rights and freedom strictly provided for by Article 53 (2) of the Constitution. This principle states that the extent of restriction must be in line with the situation that led to its implementation and also that it must cease once that cause determining it disappeared. Law no. 298/2008 requires retention of data continuously from the time of entry into force, respectively of its application (i.e. 20 January 2009, respectively 15 March 2009 as concerns traffic data of location corresponding to the services of access to Internet, email and Internet telephony), without considering the need to terminate the restriction once the cause that has led to this measure has disappeared.

The Court held that, although Law no. 298/2008 referred to data of a predominantly technical nature, the same were retained in order to provide information and the person and his private life. Even though according to Article 1 (3) of the law, it shall not apply also to the content of communication or information accessed while using an electronic communications network, the other data stored, aimed at identifying the caller and the called party, namely the user and recipient of information communicated electronically, of the source, destination, date, hour and duration of a communication, type of communication, the communication equipment or devices used by the user, the location of mobile communication equipment, as well as of other "related data" — undefined in the law —, were likely to prejudice, to interfere with free expression of the right of communication or expression.

It was indicated that the legal guarantees for use in particular cases of data retained — concerning the exclusion of content of the communication or information consulted, as object of data storage, by the prior and reasoned authorization of the president of the court entitled to judge the offence for which criminal proceedings have been initiated, as provided by Article 16 of Law no. 298/2008 and implementing penalties covered by Articles 18 and 19 of the same — were not sufficient and adequate as to remove the fear that personal rights, of private type, are not violated, so that their occurrence would take place in an acceptable manner.

Thus, the Constitutional Court did not deny the purpose in itself considered by the legislature in adopting the Law no. 298/2008, in that it is an urgent need to ensure adequate and effective legal means, consistent with the continuous process of modernization and technologization of the media, so that crime can be controlled and prevented. This is the reason for which individual rights cannot be exercised *in absurdum*, but can be subject to restrictions that are justified by the aim pursued. Limiting the exercise of certain personal rights in consideration of collective rights and public interests, aimed at national security, public order or prevention of crime, was always a sensitive operation in terms of regulation, so as to maintain a fair balance between the interests and rights of the individual, on the one hand, and those of the society, on the other. It isn't less true, as noted by the European Court of Human Rights in the Judgment of 6 September 1978 rendered in *the case of Klass and others v. Germany*, paragraph 49, that taking surveillance measures, without adequate and sufficient guarantees, can lead to "destruction of democracy on the ground of defending it".

2.3.2. Another decision that had a very strong echo in the society was the **Decision no. 440 of the 8th of July 2014** on the exception of unconstitutionality of the provisions of Law no. 82/2012 on the retention of data generated or processed by providers of public electronic communications networks and by providers of publicly available electronic communications services, as well as for the amendment and supplementing of Law no. 506/2004 on personal data processing and protection of private life in the sector of electronic communications[7].

The Court noted that the Law no. 82/2012 represented the second transposition into national legislation of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. In its analisis, the Court considered necessary for a precise understanding of the retention of the data mechanism, to distinguish between two different stages. Noting that the data in question relate mainly to traffic and location data of persons and data necessary to identify a subscriber or registered user, the mechanism covered involves two stages, the first being that of the retention

[7] Published in the Official Gazette of Romania, Part I, no. 653 of 4 September 2014.

and storage of data and the second, that of access to the data and their use.

The retention and storage of data, which is the first operation from the chronological point of view, is in the responsibility of providers of public communications networks and publicly available electronic communications services. This operation is a technical one and it is conducted automatically on the basis of software as long as the law obliges providers designated by law to retain those data. Whereas both under Directive 2006/24/EC and under Law no. 82/2012, the purpose of the retention and storage is a general one and thereby ensuring national security, defense, prevention, investigation, detection and prosecution of serious crime, retention and storage not being linked and determined by a particular case, it appears as obvious the continuing nature of the obligation of providers of public electronic communications network and service providers to retain data on the entire period expressly provided for by the legislative framework in force, namely for a period of 6 months, under Law nor.82/2012. At this stage, as only the retention and storage of a mass of information are concerned, identification or location of those who are subjects of electronic communications are not actually carried out, this will take place only in the second stage, after being granted access to the data and their use.

The Court stated that given the nature and specificities of the first stage, since the legislature considers necessary the retention and storage of data this operation by itself is not contrary to the right to personal, family and private life, or to the secrecy of correspondence. Neither the Constitution nor the Constitutional Court case-law prohibit preventive storage of traffic and location data, but on condition that access to the data and their use be accompanied by guarantees and be made in compliance with the principle of proportionality.

Consequently, the Court considered that only in relation to the second stage, that of access and use of such data, it arises the question of compliance of legal regulations with the constitutional provisions. Examining the provisions of Law no. 82/2012, concerning the access of the judiciary and other State bodies with tasks in the field of national security to data stored, the Court found that the law did not give the necessary guarantees for protection of the right to personal, family and private life, secret correspondence and freedom of expression of individuals whose stored data are accessed.

As it was stated earlier, under Article 1 of Law no. 82/2012, prosecution bodies, courts and State bodies with tasks in the field of national security have access to data retained under this law. However, according to the provisions of Article 18 of Law no. 82/2012, only the prosecution bodies are obliged to comply with the provisions of Article 152 of the Code of Criminal Procedure, as this requirement does not cover also the State bodies with tasks in the field of national security, which can access these data in accordance with "special laws", as provided by Article 16 (1) of Law no. 82/2012. Therefore, only the request by the prosecution bodies to the providers of public communications networks and providers of publicly available electronic communications services for the transmission of retained data is subject to the prior authorization of the judge of freedoms and rights.

Requests for access to data retained for use for a purpose designated by law made by State bodies with tasks in the field of national security are not subject to authorization or approval of the court, thereby lacking the guarantee of effective protection of the data retained against the risk of abuse and against any unlawful access and use of such data. That situation is liable to constitute an interference with the fundamental rights to personal, family and private life and secrecy of correspondence and thus contravene the constitutional provisions which enshrine and protect these rights.

Having examined the "special laws in the matter", mentioned in Article 16 (1) of Law no. 82/2012, the Court found that State bodies with tasks in the field of national security can access and use data stored without the need for court authorization. Thus, Law no. 51/1991 on the national security of Romania establishes, in Article 8, the State bodies with tasks in the field of national security, i.e. the Romanian Intelligence Service, the Foreign Intelligence Service and the Protection and Guard Service and in Article 9 it states that the Ministry of National Defense, the Ministry of the Interior and the Ministry of Justice organize own intelligence structures with specific tasks in their respective areas of activity. The Court also noted that, according to Article 13, let. e) of the law, the bodies responsible for national security, while there is a threat to national security of Romania, as defined in Article 3 of Law no. 51/1991, may request the obtaining of data generated or processed by providers of public electronic communications networks or providers of publicly available electronic communications services, other than their content, and retained by them according to the law, and neither this Article nor Article 14 of the law provides that such a request must be authorized by a judge.

The Court noted, moreover, that according to Article 9 of Law no. 14/1992 on the organization and functioning of the Romanian Intelligence Service *"in order to determine the existence of threats to national security provided for in Article 3 of Law no. 51/1991 on national security of Romania, as amended, intelligence services may carry out checks in compliance with the law, by: [...] e) obtaining data generated or processed by providers of public communications networks and providers of publicly available electronic communications services other than their content, and retained by them in accordance with the law".* But, like the provisions of Law no. 82/2012 and of Law no. 51/1991, the provisions of Law no. 14/1992 do not impose the obligation of such

intelligence service to obtain the authorization of the judge to have access to data stored.

At the same time, the Court noted that Law nor.1/1998 on the organization and operation of the Foreign Intelligence Service, provides in Article 10 (1) that *"the Foreign Intelligence Service is allowed to use undercover legal persons established in accordance with the law, to use specific methods, to establish and maintain appropriate means for obtaining, verification, assessment, protection, recovery and storage of data and information relating to national security"*, and, according to paragraph (3) of the same Article, *"use of the means of obtaining, verification and recovery of data and information must not adversely affect any rights or fundamental freedoms of citizens, private life, honor or reputation or to make them subject to unlawful restrictions"*. Furthermore, according to Article 11 of Law no. 1/1998, *"the Foreign Intelligence Service shall be entitled, under the conditions laid down by law, to request and obtain from the Romanian public authorities, economic agents, other legal persons and natural persons the information, data and documents necessary for the performance of its tasks"*. The Court therefore found that Law no. 1/1998 does not regulate in a distinct manner the access of the Foreign Intelligence Service to data retained by providers of public communications networks and providers of publicly available electronic communications services, this access is however covered by Article 13 of Law no. 51/1991, unencumbered therefore by the prior authorization of a court.

However, the lack of such authorization has been criticized, inter alia, by the Court of Justice of the European Union by the Judgement of 8 April 2014, i.e. such lack is equivalent to the insufficiency of procedural safeguards necessary to protect privacy and other rights enshrined in Article7 of the Charter of fundamental rights and freedoms and the fundamental right to the protection of personal data, enshrined in Article 8 of the Charter (par. 62). III. For all of those reasons, the Court upheld the exception of unconstitutionality and noted that the provisions of Law no. 82/2012 on the retention of data generated or processed by providers of public electronic communications networks and by providers of publicly available electronic communications services and amending and supplementing Law no. 506/2004 concerning the processing of personal data and the protection of privacy in the electronic communications sector are unconstitutional.

In what concerns the effect of this decision, the Constitutional Court itself has stressed (paragraph 78 and 79) that at the publication in the Official Gazette of Romania, Part I, of this decision, becoming lacked of legal basis from the point of view of the European law, as well as of the national law, the activity of retention and use of data generated or processed regarding the supply of publicly available electronic communications services or of public communications networks. Specifically, it means that since the publication of the decision of the Constitutional Court of Romania, the providers of public electronic communications networks and of publicly available electronic communications services *do not have the obligation anymore, nor the legal possibility to retain certain data* generated or processed within their activity *and to put them at the disposal of judicial bodies* and of those with powers to protect national security. By exception, these providers can only retain the data necessary for invoicing or payments for interconnection or other data processed for marketing purposes only with the prior consent of the individual whose data are processed, as stipulated by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and protection of confidentiality in the sector of public communications (Directive on confidentiality and electronic communications), in force.

Accordingly, until the adoption by the Parliament of a new law on data retention, to comply with constitutional provisions and exigencies, as they were highlighted in this decision, the judicial bodies and State bodies with powers to protect national security do not have access anymore to data that have been already retained and stored pursuant to Directive 2006/24/EC and to Law no. 82/2012 in view of their use within the activities defined by Article 1 (1) of Law no. 82/2012. Likewise, the judicial bodies and those with powers to protect national security lack a legal and constitutional basis for the access and use of data retained by the providers for invoicing, payments for interconnection or for other commercial purposes, to be used within the activities for the prevention, research, discovery and criminal prosecution of serious crimes or for the settlement of cases with disappeared persons or for the execution of an arrest warrant or a penalty enforcement warrant, precisely because the character, nature and different purpose thereof, as stipulated by Directive 2002/58/EC. Moreover, even Law no. 82/2012 establishes at Article 11 that these latter retained data are exempted from the legal provisions, having another legal regime, being submitted to the provisions of Law no. 506/2004 on the processing of personal data and the protection of private life in the sector of electronic communications.

2.3.3. Another important decision is **Decision no. 461 of 16 September 2014** on the objection of unconstitutionality of the provisions of the Law amending and supplementing Government Emergency Ordinance no. 111/2011 on electronic communications[8].

The Emergency Ordinance implements a number of directives regulating the authorization of electronic communications networks and services. It essentially regulates the rights and obligations of providers of electronic communications networks and services, the

[8] Published in the Official Gazette of Romania, Part I, no. 775 of 24 October 2014.

regime of limited resources, the rights of end-users, the universal service, the obligations of providers of electronic communications services and networks with significant market power.

The changes envisaged by the new regulation are aimed at the registration of users of prepaid cards, the identification of users connected to Internet access points provided by legal persons, the collection and storage of data concerning the users of communications services, the conditions for specific technical operations and corresponding responsibilities incumbent upon providers of electronic communications services, the personal data retention period and the imposition of penalties for breaches of legal obligations. The legislative initiative was motivated by the need to adopt measures to facilitate criminal investigation activities or those aimed at identifying, preventing and countering risks or threats to national security.

By the impugned rule, the legislature has expressly regulated the data necessary to identify a subscriber or user, by providing, in addition to the name and telephone number or communications service identifier, the personal identification code, the series and number of the identity document and the issuing country with regard to individuals, respectively the tax identification code, with regard to legal persons. It should be stressed that Law no. 82/2012 did not provide the obligation to retain the personal identification code, the series and number of the identity document, respectively the tax identification code needed to identify a subscriber or a user, and the database set up according to the provisions of Article 4 of this law refers, both for fixed line and mobile telephone networks and for Internet access services, electronic mail and voice over Internet Protocol, only to the telephone number, as well as to the subscriber or registered user's name and address. Therefore, in the light of the reasons held by the Court in Decision no. 1.258 of 8 October 2009, the challenges on the accuracy and foreseeability of rule no longer subsist as the new rule precisely determines the area of the data necessary for the identification, but, by taking into account the supplementing of data required to the subscriber or to the user, as well as their strictly personal nature, the amending legal provisions should have been properly supplemented by provisions ensuring high standards in terms of their protection and security throughout the entire process of retention, storage and use, precisely so as to minimize the risk of infringement of the right to personal, family and private life, the secrecy of correspondence, as well as the citizens' freedom of expression. However, the Court noted that the Law amending and supplementing Government Emergency Ordinance no. 111/2011 does not make any change regarding the protection of these rights, therefore the reasons on which the decision of unconstitutionality of Law no. 82/2012 was based, are all the more justified in this case.

The amending rule widens the category of persons who must identify the users of electronic communications services, by expressly providing the obligation of legal persons providing Internet access points to public to retain the users' identification data: the telephone number or the identifier of the communications service with advance and subsequent payment; the surname, forename and personal identification code, the series and number of the identity document, respectively the issuing country – for foreign persons; the identification data obtained through bank card payment; any other identification procedure which, directly or indirectly, ensures that the user's identity is known. The retention obligation is doubled by the obligation to store the data for a period of 6 months as from the time of their retention.

The Court noted that currently, legal persons providing public Internet access points are private legal entities, especially in commercial and recreational facilities, cafeterias, restaurants, hotels, airports etc., or legal persons governed by public law – public institutions that give citizens direct and rapid access to information of public interest (including those distributed on their own webpages), like town halls, educational institutions, health clinics, public libraries, theatres, etc. The imposition of the obligation incumbent upon such persons to retain and store personal data requires, correlatively, the specific regulation of adequate, firm and unequivocal measures, ensuring citizens' trust that the manifestly personal data that they make available are recorded and kept confidential. In this respect, the law merely establishes the measures of retention and storage of data, without amending or supplementing the legal provisions with regard to the guarantees that the State must provide in the exercise of its citizens' fundamental rights.

However, the regulatory framework in such a sensitive field must be clear, predictable and devoid of confusion, so as to remove, as much as possible, the possibility of abuse or arbitrariness in relation to those called upon to apply the legal provisions.

The Court mentioned that the provision that identification is achieved through "any other identification procedure" ensuring, directly or indirectly, that the user's identity is known, represents an imprecise regulation likely to create the prerequisites for certain abuses committed in the process of retention and storage of data by the legal persons covered by this rule.

Data retention and storage clearly constitutes a limitation of the right to the protection of personal data, respectively of the constitutionally protected basic rights relating to personal, family and private life, secrecy of correspondence and freedom of expression. Such a limitation may operate solely in accordance with Article 53 of the Constitution, which foresees the possibility of restricting the exercise of certain rights or freedoms only by law and only if necessary, as the case may be, to protect national security, public order, public health or morals, citizens' rights and freedoms,

for conducting a criminal investigation, preventing the consequences of a natural disaster or an extremely severe catastrophe. The restriction measure can be ordered only if necessary in a democratic society, it should be proportional to the situation having caused it and applied without discrimination and without infringing upon the existence of such right or freedom.

However, given that the measures adopted by the law subject to constitutional review are not accurate and foreseeable, that the interference of the State in the exercise of the abovementioned rights, although laid down by law, is not clearly, rigorously and exhaustively formulated so as to offer confidence to citizens, that its strictly necessary nature required in a democratic society is not fully justified, and that the proportionality of the measure is not ensured through the regulation of appropriate guarantees, the Court ascertained that the provisions of the Law amending and supplementing Government Emergency Ordinance no.111/2011 on electronic communications violate the provisions of Article 1(5), Articles 26, 28, 30 and 53 of the Constitution. Therefore, the limitation of the exercise of such personal rights by considering certain collective rights and public interests related to national security, public order or criminal prevention, breaks the right balance which should exist between the individual interests and rights, on the one hand, and those of the society, on the other hand, as the impugned law cannot regulate sufficient guarantees to ensure the efficient protection of data against the risks of abuse and any unlawful access or use of personal data.

2.4. Relevant decisions rendered by foreign constitutional jurisdictions in the matter of personal data protection

This sesitive issue concerned many other constitutional courts which performed a consistent constitutional review of the respective legislation. In this regard, are considered particularly relevant the decisions of the Federal Constitutional Court of Germany, of the Czech Constitutional Court and of the Supreme Administrative Court of Bulgaria.

By the **Judgment of 2 March 2010, the Federal Constitutional Court of Germany** declared unconstitutional the provisions of Articles 113a and 113b of Law on the new regulation of the telecommunications surveillance of 21 December 2007, and of Article 100g of the Criminal Procedure Code of Germany, indicating that they violate Article 10 (1) of the Constitution of Germany on the secrecy of telecommunications.

As for the unconstitutionality of the provisions of Articles 113a and 113b of the Law on the new regulation of the telecommunications surveillance of 21 December 2007 it was indicated that the storage without a special occasion of traffic data in telecommunications does not make the object of the strict prohibition of preventive storage of data according to the case-law of the Federal Constitutional Court and that, if attention is paid to this intervention and it is adequately realized, the proportionality requirements can be met.

It was underlined the importance of the storage of traffic data of the telecommunications sector for preventive purposes, but also the necessity of certain regulations sufficiently strict and clear on the security of data and the limitation of their use, in order to ensure transparency and legal protection. It was emphasized however that such storage represents a wide-ranging interference even while the content of the communications does not make the object of storage, as the retained data make possible a detailed knowledge of the intimate sphere of the individual, especially as concerns the social or political affiliation, preferences, inclinations and weaknesses of individuals, allowing the preparation of some relevant profiles and creating the risk of submitting some citizens, who give no reason to be submitted to investigations, to be exposed to such actions.

It was found that the provisions of Articles 113a and 113b of the Law on the new regulation of the telecommunications surveillance of 21 December 2007 violates the principle of proportionality, not being accomplished the constitutional requirements referring to data security and the transparency of their use, nor those on the protection of individuals. To this effect, it was hold that the impugned legal provisions refer only to the necessary diligence, generally, in the field of telecommunications, but relativize the security requirements, leaving them at the choice of the telecommunications operators, who are not required to comply with sufficient high standards in ensure the security level and for which higher penalties are established for breach of the storage obligation than for the violation of the security data.

It was also held that the provisions of Article 100g of the Criminal Procedure Code also allow the access to data in other cases than the individual ones, without the judge's agreement and without the person concerned being informed, for which reason they are unconstitutional.

Similarly, the **Constitutional Court of the Czech Republic, through Decision of 22 March 2011**, found the unconstitutionality of the provisions of section 97 paragraphs 3 and 4 of the Act no. 127/2005 on the electronic communications and amendments referring to related normative acts (Act on electronic communications) of the Decree no. 485/2005 on data retention regarding the traffic, location, date and duration of communications, as well as the form and method of delivery of these ones to authorized authorities.

In the content of this decision the Court held that the impugned texts do not offer to citizens sufficient guarantees regarding the risk of abusive use of stored data and arbitrary. It was found that the examined normative acts do not define at all or insufficiently and ambiguously define the rules on the compliance with the requirements on the security of data retention and restriction of third parties' access to retained data. On

this occasion is was underlined the importance in the context of the current level of development of the society of traffic data retention in the field of communications, but also the need to maintain a balance between public and individual interests. By the same decision it was also found the lack of definition of the means that should be put at the disposal of the affected persons in order to benefit of an efficient protection against arbitrary and abusive use of stored data.

Finally, **the Supreme Administrative Court of Bulgaria**, through **Decision no. 13.627 of 11 December 2008**, has annulled an Article of the national law on data retention that allowed the Ministry of Internal Affairs the access to retain data in the computers' ter qa3minals and, also, the supply of access to such data to security services and to other law enforcement institutions, without the authorization of a judicial body, motivating that the annulled legal provisions did not provide any guarantee for the protection of the right to private life and that no mechanism was established in order to guarantee this protection against illegal interferences, so as to avoid the breach of honor, dignity or reputation of an individual.

3. Conclusions

The emergence of the massive computer use and the huge variety of activities based on the internet services brought unexpected risks to the right to respect for private life. Consequently, the need to protect it has led to the new set of rules meant to focus on the collection, storage and use of personal data.

The new General Data Protection Regulation (GDPR), acronym that already entered into the linguistique patrimony of all member states of the European Union[9], is the most recent and also modern instrument meant to provide a set of guarantees in what concerns the privacy of the individuals when it comes to processing and storage of their personal data.

The role of constitutional jurisdiction is crucial in improving and strengthening of all the safeguards attached to the right to the private life, intimacy and, last but not least, freedom of consciousness. Their statements bring light over the legal provisions and benefit to the quality of legislation. Accordingly, the Constitutional Court of Romania has already proved its important role in high-lightening the values of democracy, in respect of fundamental human rights. Considering the outstanding process of technical development, the chances of further requests of reviewing the constitutionality of subsequent normative acts are significant. The Court will have to keep in mind both the European compulsory regulation and also the national Basic Law's provisions granting the full exercise of fundamental human rights.

References

- Pouvoir - La datacratie, no.164/2018;
- Augustin Fuerea, *Aplicarea Regulamentului General privind Protecția Datelor*, în Dreptul nr.7/2018;
- European Court of Human Rights case-law:
- Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 27 June 2017;
- Court of Justice of the European Union case law:
- Judgment of 8 April 2014, pronounced in the joint cases C-293/12 — Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others — and C-594/12 — Kärntner Landesregierung and others;
- Constitutional Court of Romania case law:
- Decision no. 1.258 of 8 October 2009, by which it stated that the Law no. 298/2008 on the retention of data generated or processed by the providers of publicly available electronic communications services or of communications networks;
- Decision no. 440 of the 8th of July 2014 on the exception of unconstitutionality of the provisions of Law no. 82/2012 on the retention of data generated or processed by providers of public electronic communications networks and by providers of publicly available electronic communications services, as well as for the amendment and supplementing of Law no. 506/2004 on personal data processing and protection of private life in the sector of electronic communications;
- Decision no. 461 of 16 September 2014 on the objection of unconstitutionality of the provisions of the Law amending and supplementing Government Emergency Ordinance no. 111/2011 on electronic communications.

[9] Augustin Fuerea, Aplicarea Regulamentului General privind Protecția Datelor, în Dreptul nr.7/2018, p.101.