©LUMEN Proceedings

8th LUMEN International Scientific Conference Rethinking Social Action.
Core Values in Practice | RSACVP 2017 | 6-9 April 2017 |
Suceava – Romania

Rethinking Social Action.
Core Values in Practice

Relevant Aspects regarding Personal Data Protection in the Romanian Constitutional Case-Law

Crina Mihaela VERGA

https://doi.org/10.18662/lumproc.rsacvp2017.89

How to cite: Verga, C. M. (2017). Relevant Aspects regarding Personal Data Protection in the Romanian Constitutional Case-Law. In C. Ignatescu, A. Sandu, & T. Ciulei (eds.), *Rethinking Social Action. Core Values in Practice* (pp. 977-991). Suceava, Romania: LUMEN Proceedings
https://doi.org/10.18662/lumproc.rsacvp2017.89

© The Authors, LUMEN Conference Center & LUMEN Proceedings.
Selection and peer-review under responsibility of the Organizing Committee of the conference

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 Unported License, permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

©LUMEN Proceedings

8th LUMEN International Scientific Conference
Rethinking Social Action. Core Values in Practice |
RSACVP 2017 | 6-9 April 2017 | Suceava – Romania

Relevant Aspects regarding Personal Data Protection in the Romanian Constitutional Case-Law

Crina Mihaela VERGA[1]*

Abstract

The topic addressed is of particular importance given that IT crime (cybercrime) is steadily increasing and it is difficult to control it due to the rapid expansion of the developments in the field. In this paper, we, firstly, define the notions of "cybercrime" and "personal data". Then, we extensively present some relevant decisions, delivered by the Constitutional Court of Romania, on issues related to the IT field. The interesting aspects of the Constitutional Court's vision on this area, which is the topic of this research, are highlighted in the presentation. The subject under analysis is very topical, because, by two decisions of the Constitutional Court, Law no.289/2008 and Law no.82/2012 were declared entirely unconstitutional and, until the time of the study, they have not been replaced with adequate legislation.

Keywords: personal data, Constitutional Court, Romania.

1. Introduction

The paper aims, firstly, to explain the notions of "cybercrime" and "personal data". In the second part of the paper, some relevant decisions of the Constitutional Court on the field of personal data protection are especially presented and commented in detail. These decisions have concerned the constitutionality's control of the Law no.289/2008 and the Law no.82/2012. After examining, the Constitutional Court have declared

[1] Lecturer Ph.D., "George Bacovia" University, Bacau, Romania, crina_verga2000@yahoo.com

https://doi.org/10.18662/lumproc.rsacvp2017.89
Corresponding Author: Crina Mihaela VERGA
Selection and peer-review under responsibility of the Organizing Committee of the conference

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 Unported License, permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

them unconstitutional, in their entirety, as they violated the fundamental rights regarding the intimate, private and family life, the secrecy of correspondence and the freedom of expression.

It is to be noted that, at present, the legislation on the matter declared unconstitutional has not been replaced by the Romanian legislator with another corresponding to the opinion expressed by the Constitutional Court.

2. Problem Statement

The notion of "cybercrime" refers to all infractions related to information technology, crimes characterized by ease and various forms of commission, facilitated by the very rapid and continuous evolution of the analyzed field.

The extension more and more diversified of illicit acts in the IT field, due to the difficulty to control the domain and the very varied ways of committing specific infractions, has led some authors to emphasize the need for "the emergence of cyber-criminal law, which is to replace the application of criminal law to the cyber-society, in the near future") [1].

The field of cybercrime encompasses criminal acts referring to "personal data". According to the *Convention for the protection of individuals with regard to automatic processing of personal data*, an international document adopted within the Council of Europe in Strasbourg on the 28th of January 1981 [2], personal data means "any information relating to an identified or identifiable individual". According to Law no.677/2001, "an identifiable individual is a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, psychological, economic, cultural or social identity"[3]. Therefore, one considers the information relating to a particular, targeted person.

The above-mentioned convention lists the data protection principles, which refer to: quality of data; data security; special categories of data that may not be processed automatically, unless national laws provide appropriate safeguards; ensuring data security; additional safeguards for the data subject. Each State Party undertakes to establish appropriate sanctions and remedies for violations of national provisions giving effect to the basic principles of data protection.

According to the *Council of Europe Convention on cybercrime* [4], the conduct of specific investigations or criminal proceedings must be subject to the conditions and guarantees stipulated by the national law, which must

ensure *adequate protection of the human rights and freedoms*, in particular the rights arising from the acts adopted at the level of the Council of Europe and by the other relevant international instruments on human rights, which *must incorporate the principle of proportionality* (Article 15, paragraph 1).

At European Union level, *Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of private life in the electronic communications sector* [5], seeks to ensure the right to confidentiality of personal data. *Such data must be deleted or made anonymous*, except for information used for the purpose of billing or interconnection payments, when they are no longer required for the purpose of transmitting a communication. The Directive establishes that, under certain conditions, Member States may limit the scope of this rule. Thus, the necessary restrictions imposed by the guaranteeing of national security, defense, public security or the prevention, investigation, detection and prosecution of the infractions or the unauthorized use of electronic communications systems are determined.

This Directive has been transposed into the national legislation by the *Law no.506/2004* on the processing of personal data and the protection of private life in the electronic communications sector, as subsequently amended and supplemented.

On the matter, there was *adopted Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006* [6], which aimed at the harmonization of Member States' legislation on the retention of certain data generated or processed by the providers of publicly available electronic communications services and of public communications networks. The Directive guarantees the availability of such data for the prevention, the investigation, the detection and the prosecution of serious crimes such as the infractions related to the organized crime and the terrorism. For this purpose, the providers have to keep the traffic data, the location data as well as the related data necessary to identify the subscriber or user.

In 2014, Directive 2006/24/EC was declared invalid by the *judgment of the Court of Justice of the European Union of 8 April 2014* in joined cases C-293/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Other*s - and C-594/12 - *Kärntner Landesregierung and Others* [7]. Thus, the CJEU appreciated that "the Directive under consideration violates the provisions of Article 7, Article 8 and Article 52 (1) of the Fundamental Rights' Charter of the European Union".

The Directive 2006/24/EC was transposed, for the first time, into national legislation by the Law no.298/2008 and, subsequently, by the Law no.82/2012, both of them declared unconstitutional in their entirety by two

decisions of the Constitutional Court, which will be further discussed in detail.

Internally, the Law no.677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, as subsequently amended and supplemented [8], identically takes over the definition of *personal data* developed by the Convention for the protection of individuals with regard to the automatic processing of personal data, adopted at the Council of Europe on 28 January 1981.

The Law no.506/2004 on the processing of personal data and the protection of private life in the electronic communications sector [9] takes over the same meaning of the phrase *personal data* as that provided by the Law no.677/2001.

The study reveals that it is particularly useful for the Romanian legislator to assimilate the views expressed by the Constitutional Court and to adopt the corresponding legislation appropriate to them, as well as to the European legislative framework on the matter.

3. Research Questions/Aims of the research

The research questions envisage studying the current Romanian and European legislation concerning the personal data protection.

In the meantime, the article aims to present the Romanian constitutional case-law in the field mentioned above.

The purpose of the study is to emphasize on the one hand the inconsistency between the existing legislation and the Romanian constitutional jurisprudence on the matter. On the other hand, the article has mentioned the transposition's lack of the European Union's legislation into the Romanian law.

4. Research Methods

As main research methods, we have used qualitative and quantitative analysis, as well as comparative and the systemic methods.

The comparative approach aims at detecting the similarities and differences concerning the personal data protection, examined in the light of both legal provisions and jurisdictional practice in Romania. Therefore, the first part analyses the personal data protection from the perspective of legislation and doctrine and the second emphasizes different aspects of practice of the Constitutional Court in this field.

The comparative method has been used to distinguish between the current legislation adopting on the matter in Romania and other European organisations.

At the same time, the above-mentioned method allows us to understand how the personal data protection has evolved both in the Romanian and the European legislation and to appreciate his direction at present.

In our exposure, the systemic method is very useful because of its overall approach to various issues related to the protection of personal data.

5. Findings

Relevant constitutional case-law on the protection of personal data

§5.1. Decision no. 962 of the Constitutional Court of 25 June 2009

By Decision no.962 of 25 June 2009 [10], the Constitutional Court ruled that the provisions of Article 91 of the Criminal Procedure Code, which regulated the conditions and cases of interception and recording of calls or communications made by telephone or by any electronic means of communication, were constitutional, as they are justified in a democratic society threatened by an increasingly complex criminal phenomenon, by the need to ensure national security, to defense public order or to prevention of the crimes.

§5.2. Decision no.1258 of the Constitutional Court of 8 October 2009

Law no.298/2008 was declared not in accordance with the fundamental law by the Constitutional Court's Decision no.1258 of 8 October 2009 [11], as it was found in violation of the fundamental rights related to the intimate, private and family life, the secrecy of correspondence and the freedom of expression.

Thus, Bucharest Tribunal – The Commercial Section, notified the Constitutional Court with the unconstitutionality's exception of the provisions of Aricles1 and Article 15 of the Law no.298/2008.

Law no.298/2008 [12] establishes for the providers of public electronic communications services and networks the obligation to retain certain data generated or processed in the framework of their activity, for making it available to the competent authorities for use in the investigation, detection and prosecution of serious crimes (Art.1).

The aforementioned law imposes on providers of publicly available electronic communications services and networks and of public

communications networks the obligation to store for a period of *6 months the traffic and location data of individuals and legal entities*. This data is needed to "track and identify" *the source, destination, date, time and duration* of a communication, the *type* of communication, the *equipment* or device used by the user and the *location* of the mobile communication equipment.

Law no.298/2008 stipulates that the providers of public communications networks and of publicly available electronic communications services are under the obligation to immediately provide, upon the request of the competent authorities and on the basis of the authorization issued according to the law, the data retained under this law, except for cases of force majeure (Article 15).

The law under analysis refers to the *traffic and location data* of individuals and legal entities as well as the *related data necessary* to identify the registered subscriber or user. The Constitutional Court rightly noted that the ordinary legislator did not define the phrase *related data* in the content of Law no.298/2008, nor did it explain the meaning of the phrase "*threats to national security*" provided in Art.20. The Constitutional Court therefore concluded that *the lack of precise legal regulation* that would accurately determine the sphere of the data necessary for the identification of users, individuals or legal entities, or the sphere of those specific actions threatening national security, might lead to abuses in the retention, processing and use of stored data.

By analyzing the practice of the European Court of Human Rights on the matter and in accordance with its own case-law, the Constitutional Court noted that *the law must be, at the same time, accessible and predictable*.

Examining the provisions of the Law no.298/2008, the Court fairly observed that the provisions of Art.91[1] of the Criminal Procedure Code allowed for audio and video interceptions and recordings under certain strict conditions, from the moment of obtaining the reasoned authorization of the judge, for a limited period of time which might not exceed 120 days, for the same person and for the same action. The normative act under analysis imposes the obligation *to retain the data permanently, for a period of 6 months from its interception*; thereby, the data can be used, with the motivated authorization of a judge, for a period of time in the past and not in the future. Thus, *the legal obligation requiring the continued detention of personal data turns the exception to the principle of effective protection of the right to private life and free expression in an absolute rule*. At the same time, *the above-mentioned obligation also violates the principle of proportionality*, which requires the measure restricting a right to be proportional to the situation that led to its application and, at the same time, to stop with the cessation of the determining cause.

On the same line, the Court also holds that legal guarantees regarding the concrete use of the retained data are not sufficient and adequate to remove the fear that personal, private rights are not violated.

The Constitutional Court has judiciously noted that it was not the justified use, under the conditions regulated by Law no.298/2008, in itself which unacceptably damaged the exercise of the right to privacy or freedom of expression, but the legal, continuous obligation, generally applicable, of the data storage.

The Constitutional Court did not deny the purpose in itself considered by the legislator when adopting the Law no.298/2008, that it was imperative to ensure adequate and effective legal means [...] so that the criminal phenomenon could be controlled and countered.

Limiting the exercise of the right to privacy, to secrecy of correspondence and of the freedom of expression must take place in a clear, predictable and unequivocal manner so as to remove, to the highest extent, the possibility of the arbitrariness or the abuse by the authorities in this field.

The Constitutional Court stated that a most precise regulation of the scope of Law no.298/2008 was all the more necessary particularly in view of the complex nature of the rights subject to limitation and of the consequences which a possible abuse of public authorities would have on the private life of its addressees.

Following the examination of this decision, we notice that the lack of clear and predictable provisions of the law under consideration, the imposition of some restrictions on the exercise of fundamental rights (the right to intimate, private and family life, the right to secrecy of correspondence, the freedom of expression), which do not comply with the conditions established by Article 53 of the Constitution, as well as the lack of effective guarantees of the rights concerned affect the exercise of these rights.

§5.3. Decision no.440 of the Constitutional Court of 8 July 2014[13]

As a consequence of an unconstitutional exception submitted *ex officio* by Constanța Court - The Criminal Section and of one submitted *ex officio* by Târgoviște Court, the Constitutional Court effectuated the constitutional control of the provisions of the Law no.82/2012 and of Article 152 of the Criminal Procedure Code.

The Constitutional Court ruled that Law no.82/2012[14] was the transposition into Romanian law of the Directive 2006/24/EC, which had been invalidated by the European Union's Court of Justice by the above-mentioned decision of 8 April 2014.

The Court found that, in *Law no.82/2012 and Law no. 298/2008*, the cases in which the judicial authorities or national safety authorities had access to the data generated or processed by the providers of public communications networks and the providers of publicly available electronic communications services were those aimed at preventing, investigating, detecting and prosecuting "*serious crimes*". These infractions are defined by both laws, but the content of the concept of "*serious crime*" is much wider in Article 2 letter e of the Law no.82/2012 than that mentioned in the provisions of the Law no.298/2008.

The Court noted that the current regulation applies to "traffic and location data of individuals and legal entities, as well as to *data necessary* to identify a registered subscriber or user." Thus, the Law no.82/2012 removed the word "*related*" from the phrase "necessary related data" existing in the previous regulation; however, this change preserved the imprecise nature of the wording, because the legislator did not define what was meant by "the data necessary for identification of a subscriber or registered user".

Like the previous legislative regulation, the Law no.82/2012 established "the obligation of the providers of public communications networks and of publicly available electronic communications services to retain certain data generated or processed in the course of their activity, in order to provide it to the criminal prosecution bodies, courts and state bodies with responsibilities in the field of national security". In this case, the continuity of the retention of data constituted a reason for declaring the provisions' unconstitutionality of the Law no.298/2008 and therefore also of the Law no.82/2012. Also, limiting the exercise of the right to intimate, private and family life, of the secrecy of correspondence as well as of the freedom of expression must take place in a *clear, predictable and unequivocal manner,* to remove, as much as possible, the possibility of arbitrariness.

In demonstrating the unconstitutionality of the law under examination, the Constitutional Court also notes that the criticized law does not contain clear and precise rules on the content and application of the measure of data retention, as well as on the access to and use of traffic, location and other necessary data. Thus, the persons whose data had been retained did not benefit from sufficient guarantees ensuring effective protection against any unauthorized access or use.

It was also noted that only the request by the criminal prosecution bodies to providers of public electronic communications networks and services to transmit retained data is subject to the prior authorization of the judge of rights and liberties. The requests for access to the retained data for their use for the purpose of the law demanded by the national security

bodies are not subject to the court's authorization and thus there was no effective protection of the retained data against any arbitrariness.

The Constitutional Court judiciously noted that *the lack of a real mechanism for controlling the activity of electronic communications operators by an independent authority is equivalent to the lack of effective guarantees* to ensure the protection of the retained data.

The Romanian Constitutional Court also referred to the decisions of the Federal Constitutional Court of Germany, the Constitutional Court of the Czech Republic and the Supreme Administrative Court of Bulgaria, which declared unconstitutional certain provisions of special laws in the field of information and communication technology because they had damaged some rights provided and guaranteed by the fundamental act, the arguments put forward being similar.

The Constitutional Court concluded that the interference in the fundamental rights concerning intimate, private and family life, the secrecy of correspondence and the freedom of expression is to *a great degree* and must be regarded as *particularly serious*.

§5.4. Decision no.461 of the Constitutional Court of 16 September 2014 [15]

The Law amending and supplementing Government Emergency Ordinance no.111/2011 on electronic communications subjected to the prior constitutionality control concerns: the registration of prepaid card users; the retaining and storage of data of communications service users; the conditions for carrying out specific technical operations; the corresponding obligations of the providers of electronic communications services; the penalties for the violation of the legal obligations.

The aforementioned law provides for: the obligation of legal entities providing Internet access points to the public to identify the users connected to these access points; the obligation to store for a period of 6 months from the date of their retention the personal data obtained by retaining the user identification or telephone number, by bank card payment or by any other identification procedure that directly or indirectly ensures knowledge of the user's identity.

Although the criticized law modifies the regulatory framework on electronic communications, the Constitutional Court has rightly noted that from examining the arguments put forward by the initiator of the bill in the "*Explanatory Memorandum*", the opinion of the Legislative Council as well as the changes made by the provisions of the law, it results that, *in reality, the normative act supplements the legal framework regarding the retention of data generated or*

processed by the providers of publicly available electronic communications services and of public communications networks regulated by Law no. 82/2012. Thus, it was noticed the defective manner in which the legislator understood to apply the technical legal norms necessary for the drafting of normative acts.

The law appealed to the Constitutional Court defines precisely *the sphere of the data necessary to identify a subscriber or a user*; thus, the criticisms regarding the clarity and predictability of this provision have been removed. The Constitutional Court rightly found that the rules, on supplementing strictly personal data requested from the subscriber or user, should have been supplemented with provisions to ensure increased standards of security of them. However, in this case, the criticized law did not provide additional guarantees for the protection of the rights concerned. Therefore, in this case, the reasons for the unconstitutionality of the Law no.82/2012 are even more justified.

Moreover, the law under the control of the Court extends the sphere of the legal subjects having the obligation to retain and store the data generated or processed by the providers of the public communications networks and of publicly available electronic communications services.

Also, in the case of electronic communications services for which payment is made in advance, the modifying rules from the examined law only refer to filling in a standard form made available to the user by the supplier. This way, the legislator does not accurately determine the sphere of persons that provide the standard form, which can lead to abuses.

At the same time, the Court has noted that the user's obligation to fill in the standard form does not have a correspondent correlative obligation on the part of the person collecting personal data of guaranteeing the confidentiality, security and use of such data for the purpose of the law. The same situation exists in the case of the obligation to retain the users' identification data set up for legal entities making available Internet access points to the public. Therefore, the persons collecting such data have no responsibility in this sense.

The Constitutional Court has concluded that the interference of the state in the exercise of the rights relating to the intimate, private and family life, to the secrecy of correspondence and to the freedom of expression, although provided for by the law, *is not formulated in a clear, rigorous and exhaustive manner as to give confidence to citizens; the strictly necessary character in a democratic society is not fully justified and the proportionality of the measure is not ensured by the provision of appropriate guarantees.*

Disagreeing with the solution given by the majority of judges, a separate opinion has also been expressed. According to the latter, there is no justification for a legal difference in registration between prepaid card users

and telephone subscribers who are subject to registration and identification under the law. The reason for imposing such an obligation is also the possibility of taking certain measures to combat the criminal phenomenon. It was also considered that the interference with the fundamental rights concerned in this case is in line with the provisions of Article 53 of the Constitution. We are in agreement with the majority solution emphasized above because we believe that its arguments are fully justified.

Thus, the results of this study refers to: the examination of the Romanian and European legislation regarding the personal protection data; the examination of the Romanian constitutional case-law on the matter; the lack of concordance between the legislation and the constitutional practice in the field; non-agreement of existing legislation with the Constitutional Court's decisions until the moment of the article's elaboration; non-agreement of the Romanian law in the field with the existing European legislation.

6. Discussions

This study is relevant, as it underlines the necessity for the Romanian legislator to adopt a legislation corresponding to the opinions expressed by the Constitutional Court in its decisions made in the field.

This obligation of the Romanian Parliament must be respected, because the decisions of the Constitutional Court are mandatory for all public institutions and shall be effective only for the future.

In this sense, the effects of a decision are different, as this is the result of an objection or exception of unconstitutionality. Thus, when processing an exception of unconstitutionality, the provisions of the laws in force, which are found to be unconstitutional, shall cease their legal effects within 45 days of the publication of the Constitutional Court's decision if, in the meantime, the Parliament cannot bring into line the unconstitutional provisions with the provisions of the Constitution. For this limited length of time, the provisions found to be unconstitutional shall be suspended de jure (Article 147 paragraph 1, Romanian Constitution) [16].

When processing an objection of unconstitutionality, after which some legal provisions were declared unconstitutional, before the promulgation thereof, the Parliament is bound to reconsider those provisions, in order to bring them into line with the decision of the Constitutional Court (Article 147 paragraph 1, Romanian Constitution).

Until now, the Parliament has not complied with the decisions pronounced by the Constitutional Court on this matter.

In the process of drafting appropriate legislation on the matter, the Romanian legislator has also to adopt a legislation transposing the specific European Union acquis in the field, by virtue of Romania's quality as a European Union's member state.

In this quality, Romania has to respect the following principles, the basis of the European Union's institutional system activity: the supremacy of the European Union's law; the direct and immediate application of the European Union's law. By virtue of these principles, the European Union's legislation in the field has to be transposed into the Romanian law.

In 2014, the Directive 2006/24/EC, the legal framework on the matter, was declared invalid by the judgment of the Court of Justice of the European Union of 8 April 2014, because it "violates the provisions of Article 7, Article 8 and Article 52 (1) of the Fundamental Rights' Charter of the European Union". This directive was replaced by the Directive 2016/680 of the 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 the infractions or the execution of criminal penalties, and on the free movement of such data.

Romania has the obligation to transpose this above-mentioned directive into national legislation until 6th of May 2018.

7. Conclusions

By declaring Directive 2006/24/EC invalid by the Court of Justice of the European Union and as a result of the unconstitutionality's declaring of the Law.298/2008 and of the Law no.82/2012, the activity of retaining and using data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks has remained legally unfounded at national level. This situation has undesirable consequences in the area under consideration, such as: the lack of legal obligation for providers of public electronic communications networks and providers of publicly available electronic communications services to process and store such data and make them available to the judicial bodies or to those with responsibilities in the field of national security [17] (the Romanian Intelligence Service, the Foreign Intelligence Service and the Protection and Guard Service); the impossibility of the judicial bodies or those having national security responsibilities to access and use such data for the purpose of preventing, detecting and investigating serious crimes.

Therefore, internally, the field of personal data protection remains governed only by the legislation existing prior to the transposition of Directive 2006/24/EC into national law: Law no.677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data; Law no.506/2004 on the processing of personal data and the protection of the private life in the electronic communications sector.

At present, at EU level, the area under investigation is governed by: EU Regulation 2016/679 (General Data Protection Regulation) [18]; Directive 2016/680 of the Parliament and of the Council of 27 April 2016 [19]. In accordance with the principles of primacy and direct and immediate application of EU law, Member States are required to transpose into their national legal systems the above-mentioned Regulation until 25th of May 2018 and the above-mentioned Directive until 6th of May 2018.

References

[1] Florescu V, Florescu G. Analysis of computer crimes incriminated in the legislation in force and from the perspective of the new Criminal Code. The Romanian Journal of Informatics and Automation 2012, 22(2): 21-38.

[2] Convention for the protection of individuals with regard to automatic processing of personal data, adopted in Strasbourg on 28 January 1981, ratified by Law no.682 of 28 November 2001 on the ratification of the Convention for the protection of individuals with regard to automatic processing of personal data, Official Journal of Romania, Part I, no.830 of 21 December 2001.

[3] Law no.677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Romanian Official Journal, Part I, no.790 of 12 December 2001, as subsequently amended and supplemented.

[4] Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001, ratified by Law no.64/2004, the Official Journal of Romania, Part I, no.343 of 20 April 2004.

[5] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, the Official Journal of the European Union no. L 201 of 31 July 2002.

[6] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive

2002/58/EC, the Official Journal of the European Union no. L 105, Special issue, 13/vol.53.
[7] Judgment of the Court (Grand Chamber) of 8 April 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria)) — Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12), the Official Journal of the European Union no. C 175/6 of 10 June 2014.
[8] Law no.677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, the Official Journal, Part I, no.790 of 12 December 2001, as subsequently amended and supplemented.
[9] Law no.506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, the Official Journal, Part I, no.1101 of 25 November 2004, as subsequently amended and supplemented.
[10] Constitutional Court's Decision no.962 of 25 June 2009, the Official Journal, Part I, no.563 of 13 August 2009.
[11] Constitutional Court's Decision no.1258 of 8 October 2009 regarding the unconstitutional exception of the Law no.298/2008 on the retention of the data generated or processed by the providers of publicly available electronic communications services and of public communications networks as well as for amending the Law no.506/2004 on the processing of personal data and the protection of private life in the electronic communications sector, the Official Journal, Part I, no.798 of 23 November 2009.
[12] Law no.298/2008 on the retention of the data generated or processed by the providers of publicly available electronic communications services and of public communications networks as well as for amending the Law no.506/2004 on the processing of personal data and the protection of private life in the electronic communications sector, the Official Journal, Part I, no.780 of 21 November 2008
[13] Constitutional Court's Decision no.440 of 8 July 2014 regarding the exception of unconstitutionality of Law no.82/2012 on the retention of the data generated or processed by the providers of public communications networks and providers of publicly available electronic communications services, as well as for amending and supplementing the Law no.506/2004 on the processing of personal data and the protection of private life in the electronic communications sector and Art.152 of the Criminal Procedure Code, published in the Official Journal Part I, no.653 of 4 September 2014.
[14] Law no. 82/2012 on the retention of the data generated or processed by the providers of public communications networks and providers of publicly available electronic communications services, as well as for amending and supplementing the Law no.506/2004 on the processing of personal data and

the protection of private life in the electronic communications sector, the Official Journal, Part I, no.406 of 18 June 2012.
[15] Constitutional Court's Decision no.461 of 16 September 2014 regarding the unconstitutionality's objection of the Law amending and supplementing Government Emergency Ordinance no.111/2011 on electronic communications, the Official Journal, Part I, no.775 of 24 October 2014.
[16] Revised Romanian Constitution, the Official Journal, Part I, no.767 of 31 October 2003
[17] Art.8 of Law no.51/1991 on the National Security of Romania, republished in the Official Journal, Part I, no.190 of 18 March 2014.
[18] 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, the Official Journal of the European Union L 119/1 on 4 May 2016 .
[19] 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 the infractions or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, the Official Journal of the European Union L 119/89 on 4 May 2016.