

# THE PROTECTION OF PERSONAL DATA IN THE CONTEXT OF NATIONAL SECURITY PROTECTION MEASURES

Dan Constantin MĂȚĂ<sup>1</sup>

e-mail: danmata@uaic.ro

---

## Abstract

With the development of the information society, protection of personal data has become a current theme in the legal field. Rules to regulate access to this information have been adopted, both at international and national level, since the last two decades of the last century. Romania is no exception in this regard and has adopted a relevant legal framework in the field of private life and personal data protection. Most of these regulations in Romanian legislation are transposed general or sectorial EU directives. The issue of personal data protection has entered a new phase with the increment of challenges and threats specific to the current security environment. Investigating these normative developments, case law interpretations and doctrinal controversy are part of the current debate on the need to strike a fair balance between security and freedom. In this debate, the structural reform of the Romanian legislation on national security, including the one on the protection of personal data, appears necessary.

**Key words:** national security, personal data, private life

---

Personal data allow individual and social identification of a person. Their protection has become necessary given that the processing of personal data has grown exponentially with the development of the information society. Accepting that contemporary world is a "global village" has as one consequence the much easier access to personal data in order to ensure the free movement of ideas, people and goods. To eliminate abusive practices it is necessary to make special regulations to protect such data. Thus, on the one hand, it is prevented the arbitrary interference of public authorities with data within the scope of human personality, and, on the other hand, it is provided the necessary framework to protect such data from unauthorized use for the purpose of committing offences. The spectacularly evolving security challenges in today's society have amplified the use of personal data in specific measures and actions of national security protection. The analyses on this perspective represent the big dilemma between security and freedom which keep in a delicate balance the need to ensure security and the respect for human rights.

## MATERIAL AND METHOD

In Europe, the concerns for the protection of personal data are relatively late, since the

penultimate decade of the last century. On January 28<sup>th</sup>, 1981, the Council of Europe adopted the *Convention for the protection of individuals with regard to automatic processing of personal data* where such data are defined as "any information relating to an identified or identifiable individual" (Lisiević A., 2015, p. 11 ).

Subsequently, within the European Union, *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* had been adopted, which, in order to harmonize regulations, was transposed into national legislation. Within the spectacular development of information technology and data processing within European Union, new sectorial regulations for electronic communications have been adopted: *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector*; *Directive 2006/24/EC 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* (Zanfir G., 2015, p. 6). Other sectorial regulations were adopted on electronic commerce (*Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal*

---

<sup>1</sup> "Al.I. Cuza" University of Iași, Faculty of Law

*aspects of information society services, in particular electronic commerce, in the Internal Market*) and on standard contractual clauses (Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council).

The mechanism of personal data protection in the European Union was strongly reinforced with the adoption of the Charter of Fundamental Rights of the European Union on 7 December 2000 as an inter-institutional agreement representing a joint statement of the European Parliament, the EU Council and the European Commission (Murgu S., MN Stoicu 2012, pp. 21-22). Article 8 of this document states under marginal title *The protection of personal data*, a right of any individual to protection of his personal data. In developing this right, the Charter provides that personal data must be treated properly, only for the specified purposes and on the basis of the consent of that person or under another reason provided by law. Any person has the right to access the collected data concerning him and the right to have them rectified.

The Court of Justice of the European Union generated an ample case law on the interpretation of the concept of personal data, as defined in Directive 95/46/EC. Analyzing this case law, it results that the following information is regarded as personal data: the name of a person along with his phone number, with information on work conditions or recreational activities; the address of a person; daily work periods, rest periods and the corresponding periods not included in the work periods; the reference that a person was injured and is in sick leave; the amounts paid by certain bodies and their beneficiaries; income from work or from the natural person's capital and assets; biometrics; IP address; traffic and location data; date of birth, nationality, ethnicity, religion and language of the person (Zanfir G., 2015, pp. 22-23).

In the context of the efforts to accede to the European Union, Romania has adopted a relevant legal framework to the matters of private life and protection of personal data, in particular through the transposition into national law of the European directives mentioned above (Vlădoiu N. M., 2015, p. 187). The framework regulation in this matter is *Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data*, largely transposing the provisions of Directive 95/46/EC. In accordance with the provisions of this law, the following are personal data: "any information relating to an identified or identifiable natural

person; an identifiable person is one who can be identified, directly or indirectly, particularly by reference to an identification number or to one or more factors specific to his physical, psychological, economic, cultural or social identity". Processing of personal data is "any operation or set of operations which is performed upon personal data by automatic or non-automatic means, such as collection, recording, organization, storage, adaptation or modification, extraction, consultation, use, disclosure to third parties by transmission, dissemination or any other way, apposition or combination, blocking, erasure or destruction" (Lisievi A., 2015, p. 99).

The scope of application of Law no. 677/2001 is extremely broad, as it is applied to the processing of personal data carried out, in whole or in part, by automatic means, as well as to the processing by other means than automatic, of personal data which form part of a recording system or are intended to be included in such a system. In the area of electronic communications, processing is done in accordance with *Law no. 506/2004 concerning the processing of personal data and private life protection in electronic communications*. This law transposes Directive 2002/58/EC and applies to the processing of personal data relating to the provision of publicly available electronic communications through public electronic communications networks, including public networks of electronic communications which involve devices for data collection and identification.

In order to protect the fundamental rights and freedoms of natural persons, especially the right to private and family life, in relation to the processing of personal data and the free movement of such data, the National Supervisory Authority for Personal Data Processing was created. In accordance with Law no. 102/2005, this supervisory authority is organized as a public authority with legal personality, autonomous and independent from any other public administration authority, as well as from any natural or legal person in the private sector, and it exercises the attributions it was given by the provisions of Law no. 677/2001 (Lisievi A., 2015, p. 130).

A decisive step in the Romanian regulation of personal data protection was the entry into force of the new Civil Code on the 1<sup>st</sup> of October 2011. In the current paradigm of civil law "the individual is more than a natural person seen as a legal abstraction, holder of civil rights and obligations, the person becomes himself the subject of legal protection" (Zanfir G., 2015, p. 72). Within the title on the natural person, the Civil Code regulates in a separate chapter *The respect owed to the*

*human being and his inherent rights.* We identify within these norms multiple rights of the person (right to private life, right to his own image etc.) and the specification, contained in the Art. 77, that any processing of personal data by automated or non-automated means, can only be done in the cases and under the conditions provided by the special law (Lisiević A., 2015, pp. 96-97).

## RESULTS AND CONSIDERATIONS

In legal doctrine, scholars have pointed out that the rights to protection of personal data and to private life are two distinct concepts. This theory finds support in the provisions of the Charter of Fundamental Rights which, under the same title (*Freedoms*), provides in separate articles the right to respect for private and family life, residence and secrecy of communications (Art. 7) and the right to personal data protection (Art. 8). This difference was explained primarily by the fact that the right to private life is a substantive right, while the right to protection of personal data is a procedural right (Zanfir G., 2015, p. 11).

Without denying these differences, other authors underline the difficulty of separating the analysis of these two notions, given that sometimes "the concept of private life merges with the underlying principles of data protection" (Carp R., S. Șandru, 2004, p. 3).

Both the case law of the Court of Justice of the European Union and that of the European Court of Human Rights are relevant on this issue and from their analysis results a nuanced interpretation of these differences. Thus, in its judgment of 8 April 2014, in the joined cases *Digital Rights Ireland Ltd (C-293/12)* and *Kärntner Landesregierung (C-594/12)*, which have invalidated Directive 2006/24/EC, the Court of Justice of the European Union reminded that "the protection of personal data, resulting from the explicit obligation stated in Article 8 para. (1) of the Charter, is of particular importance for the right to private life consecrated in Article 7 of the Charter" (point 53). However the two categories of rights are different, so the specific interferences in the exercise of two fundamental rights were highlighted: "the retention of data in order to ensure an eventual access by the competent national authorities to it, as provided for by Directive 2006/24, regards directly and specifically private life and, thus, the rights guaranteed by Article 7 of the Charter. Furthermore, such retention of data falls under Article 8 of the Charter since it constitutes processing of personal data in the sense of this article and must, therefore,

meet the necessary requirements of data protection arising from the mentioned Article" (point 29).

The primary role in the European protection of personal rights is held by the European Court of Human Rights. The judgement of 6 September 1978 ruled in *Klass v. Germany case* is a foundation of a rich case law on the protection of personal data. In this sentence the Court held, as a principle, that secret surveillance activities of citizens carried out by the intelligence services are tolerable in accordance with the European Convention only to a strictly necessary extent to safeguard democratic institutions. Another relevant decision in this matter is that delivered on 26 March 1987 in *Leander v. Sweden case* where the Court held that the registration by a public authority of data concerning the private life of an individual as well as their use and the refusal to grant the possibility for them to be challenged is a violation of the right to private life, guaranteed by Article. 8 para (1) of the Convention (Bénéjat M., 2013, pp. 555-556).

The European Court held that Article 8 of the Convention is also applicable when data are stored in a "secret registry" by the intelligence services with the possibility to be used for an unlimited period of time. In this respect, in *Rotaru v. Romania case* (Judgment of 29 March 2000), the Court ruled as a violation of the right to private life the practice of the intelligence service (in this case, the Romanian Intelligence Service) to use data and personal information (education, political activities, criminal record) systematically collected and retained by state agents several decades ago (Selejan-Guțan B. Rusu HA, 2006, p. 233).

Similar interpretations to those in the European or conventional case law can be seen in the case law of the national constitutional or administrative courts of some European countries. Such an example is France, where the State Council ruled in a judgment of 16 April 2010 on the processing of personal data within the centralized processing system of information on national security. In the motivation of this judgment the State Council advanced the premise that processing data concerning the struggle against espionage and terrorism by the intelligence services is "a measure which, in a democratic society, is necessary to national security and public safety", reason for which it must also be proportional to the purpose and nature of these data (Ganger MA, 2011, pp. 297-298). Also in France, the constitutional court includes the right to protection of personal data into the right to private life, thus ensuring its constitutional value ((Bénéjat M., 2013, p. 562).

Given these case law interpretations, it is important to establish to what extent the mentioned principles also apply in the matters of personal data retained within specific intelligence gathering activities carried out by state bodies with attributions of national security. This issue is significant given that Art. 2 para. (7) of Law no. 677/2001 stipulates that this rule "does not apply to the processing and transfer of personal data carried out in the course of national defense and national security, within the limits and restrictions established by law". Law no. 506/2004 contains a similar provision in Art. 1 para. 4 letter a).

Under Art. 13 of *Law no. 51/1991 on Romania's national security* if there are threats to the national security, the state bodies with responsibilities in this field have the following possibilities: a) to request and obtain objects, documents or official information from public authorities or institutions, or to request them from legal persons of private law or from natural persons; b) to consult specialists or experts; c) to receive notifications or written information; d) to capture some operative moments by photographing, filming or other technical means, or make individual findings on public activities carried out in public places, if this activity is done occasionally; e) to request the 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 law; f) to carry out specific activities for the collection of information, which involve the restriction of some fundamental human rights and freedoms, conducted under the law.

The public bodies with attributions of national security are: the Romanian Intelligence Service, the Foreign Intelligence Service, the Protection and Guard Service as well as the Ministry of Defense, the Ministry of Interior and the Ministry of Justice, through specialized internal structures. In carrying out their activities, each of these bodies has a specific regulatory framework. Thus, *Law no. 14/1992 on the organization and functioning of the Romanian Intelligence Service* states in Art. 9 that in order to establish the existence of threats to national security, the intelligence services may: a) request and obtain objects, documents or official information from public authorities or institutions, or to request them from legal persons of private law or from natural persons; b) consult specialists or experts; c) receive notifications or written information; d) capture some operative moments by photographing, filming or other technical means, or make individual findings on public activities carried out

in public places, if this activity is not done systematically; e) obtain 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 law.

Given the content of personal data and the specific activities carried out by the intelligence services in order to safeguard national security, it is evident the need to recognize some guarantees in the processing of personal data, which would avert the risk of arbitrariness and abuse of power. In this respect, it has been stressed that in the matter of the processing of personal data in the area of national security, one must take into consideration the demands of the constitutional provisions on private and family life (Art. 26) and the secrecy of correspondence (Art. 28) as well as those of Art. 8 of the European Convention on Human Rights and of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Zanfir G., 2015, pp. 17-18).

The Constitutional Court of Romania developed in the past years a constant case law on providing effective guarantees to personal data protection. In *Decision no. 440 of 8 July 2014 regarding the exception of unconstitutionality of the provisions of Law no. 82/2012*, the Court reminded that "limiting the exercise of some personal rights, in consideration of some collective rights and public interests aimed at national security, public order and criminal prevention, has always been a sensitive operation in terms of regulation, being necessary to maintain a fair balance between individual interests and rights, on the one hand, and those of the society, on the other hand" (point 48). Among the many aspects of unconstitutionality (such as the extent and seriousness of the interference with certain fundamental rights, the lack of clarity and predictability of the law) the Constitutional Court also emphasized that "the law does not provide objective criteria which would limit to strictly necessary the number of people having access and later using the retained data, that the access of national authorities to the stored data is not conditioned in all cases by a prior review by a court or an independent administrative entity, which would limit such access and use to what is strictly necessary in achieving the objective" (point 57).

Theoretically accepting the constitutionality of retention and storage of personal data, the Constitutional Court reiterated its objections to state bodies with attributions with national security having access to these data. The Court held that the

requests for access to the retained data in view of their use for the purposes prescribed by law "are not subject to authorization or approval by the court, thus deprived of the guarantee of effective protection against potential abuse and any illicit access and misuse of such data" (point 63). Consequently, following the admission of the exception of unconstitutionality of the provisions of Law no. 82/2012, the judiciary bodies and those with attributions with national security no longer had access to the data retained and stored up to that moment, nor the possibility of accessing and using the data retained by providers for billing, payments for interconnection or other commercial purposes.

As a result of this situation, following a legislative initiative agreed by all political parties, Parliament adopted *Law no. 235/2015 for the amending and supplementing of Law no. 506/2004 concerning the processing of personal data and protection of private life in electronic communications*. By the provisions of this law it was established that the requests of the state bodies with attributions in the field of defense and national security for access to traffic data, equipment identification data and location data must comply with the procedure stated by *Law no. 51/1991 concerning national security of Romania*.

This means that the representative of the state body with attributions in the field of national security must elaborate, in writing, the proposal for authorization and submit it to the General Prosecutor's Office by the High Court of Cassation and Justice. After analyzing this proposal in terms of legality and validity, the General Prosecutor or his legal substitute, requests in writing the High Court of Cassation and Justice President's authorization for access to traffic data, equipment identification data and location data. The request is examined in the Council Chamber by one of the judges specially appointed by the President of the High Court of Cassation and Justice. If the judge finds that the request is justified he authorizes the access, by motivated ruling, and issues a warrant which specifies, among other, the bodies granted access and the duration of the authorization.

## CONCLUSIONS

The analysis of the Romanian legislation on the protection of personal data against abusive interference in the context of national security protection measures reveals a series of imperfect and contradictory solutions. The dynamic of the security environment, especially due to the radicalization of terrorism, justifies, in the vision of intelligence services, taking drastic measures in order to safeguard democratic values. Within security practices, personal data are a useful tool in order to identify potential criminals. On the other hand, civil society invokes the Big Brother anguish, asking for firm guarantees in order to protect individuals from abuse and arbitrary practices. The role of the legislator lies between these lines and he is to promote appropriate measures in accordance with the interpretations and principles generated by international and constitutional case law.

## REFERENCES

- Bénéjat, M., 2013** - *Les droits sur les données personnelles*, în Saint-Pau J.-C. (sous la direction de), *Droits de la personnalité*, LexisNexis, Paris.
- Carp, R., Șandru, S., 2004** - *The Right to Private Life and Protection of Personal Data, From Community Acquis to the Romanian Legislation*, All Beck Publishing House, Bucharest.
- Granger, M.A., 2011** - *Constitution et sécurité intérieure, Essai de modélisation juridique*, Préfaces de Jean-Louis Debré et Olivier Lecucq, LGDJ, Paris.
- Lisievi, A. (ed.), 2015** - *The Protection of Personal Data and the Right to Private Life, Collection of Normative and Interpretative Documents*, Universul Juridic Publishing House, Bucharest.
- Murgu, S., Stoicu, M.N., 2012** - *The Legal Framework for the Protection of Human Rights in National and International Law*, 4<sup>th</sup> Edition, Cordial Lex Publishing House, Cluj-Napoca.
- Selejan-Guțan, B., Rusu, H. A., 2006** - *ECHR Decisions in Cases against Romania (1998-2006)*, Hamangiu Publishing House, Bucharest.
- Vlădoiu, N.M., 2015** - *Propaedeutics to the Law of Information Society*, Universul Juridic Publishing House, Bucharest.
- Zanfir, G., 2015** - *The Protection of Personal Data, The Rights of the Targeted Person*, C.H. Beck Publishing House, Bucharest.