

THE SECURITY OF PERSONAL DATA OF USERS IN ONLINE SOCIALIZATION NETWORKS. LEGAL ASPECTS

Adrian C. MANEA¹

Abstract: *Starting from the freedom of expression of the person as a fundamental principle laid down in the Convention for the Protection of Human Rights and Fundamental Freedoms, the fundamental principle of the Internet law is unequivocally defined: the principle of the freedom of the Internet, together with other principles such as the principle of privacy protection, the principle of territorial jurisdiction or the principle of inter-state cooperation. The Internet and the information society in general also involve the processing of users' personal data, systems processing current data in various fields from education to health, from public administration to on-line trade, placing the individual above the general interest of the economic operator, thus respecting the individual's right to privacy in a global society.*

Key words: *Internet, personal data, network, protection, cyberspace.*

1. Introduction

The traditional branches of law seem to be clearly defined and individualized, including in terms of public and private law classification, and yet we find that the development of technology and the excessive computerization present in all fields, the increasingly frequent use of databases, either it relates to employees, students, pupils, or insurants in the health system or users of the social networking systems, this now entitles us to talk about the Internet law in relation to the individual rights in the sphere of human / citizen's private rights as naturally as about landing on the Moon.

In line with the international treaties and pacts regarding the fundamental human rights and freedoms adopted in the second half of the 20th century, we obviously will not find regulations on the freedom of expression on the internet or the rights of the individual as a user of the Internet, but due to the integration of the Internet among the mass means of communication and information, we will assimilate the stated rights related to the freedom of opinion / expression, thus achieving the coordinates of the Internet freedom principle related to which we will outline the rights of the individual as a user of the Internet.

Although we speak of the personal, individual rights of the individual / citizen as a user of the Internet, or as a subject of different databases accessed for a particular interest

¹ Transilvania University of Braşov, a.c.manea@unitbv.ro

(economic or commercial) or in a general interest, in the legal specialty study of Professor Robert Uerpmann-Witzack (2010, p.1245-1263), the principles of the Internet law are analyzed from the perspective of international law: the principle of internet freedom, the principle of privacy protection, the principle of territorial jurisdiction, the principle of interstate cooperation and the principle of cooperation of the parties concerned.

Technically, the internet has its origins in the 1960s, its economic and political importance becomes visible in the early 1990s (Uerpmann-Witzack, 2010, p. 1245), the reason regarding the globalization of the Internet and its development as a social phenomenon, especially through social networks and databases also imposing the need for its legal regulation from the perspective of the users' rights.

Although in the doctrine Dan Cimpoeru (2013, pp. 11-18) denies the inclusion of the Internet law in the field of the international law, defining it mainly as the totality of the legal norms regulating the social relationships established through the Internet, including institutions and norms specific to the many filiations of the law (the legal document in electronic form, the electronic signature, the electronic commerce, the electronic auctions, the electronic crime, etc.), we can not deny the existence of the virtual space (cyberspace) that crosses the borders of states and where the Internet users interact, their virtual actions interfering with their real, private life, so that a state jurisdiction over the cyberspace is required from the point of view of the citizenship or the point of accessing the internet.

Thus, from the point of view of the ever-expanding virtual space and to which individuals are directing most of their activities, either from the professional sphere or from their private life, we consider together with Professor Robert Uerpmann-Witzack that the Internet law integrates into the system of the public international law, which is why the cyber-space becomes the fifth element within the notion of state territory, alongside the soil, subsoil, territorial waters and the airspace of a state.

From this perspective, the states exercise their sovereignty also over the cyber-space, for which what has technically been introduced in the form of a country code in the definition of a domain (for example “.ro” code related to Romania) from a juridical perspective confirms its belonging to the cyber-space of Romania.

2. The Principle of the Internet Freedom and the Principle of Privacy

Mentioned by Professor Robert Uerpmann-Witzack (2010, p. 1247) as the first two principles of the Internet law, the two principles put side by side seem to be in antithesis but concern the protection of two fundamental rights of the individuals - the freedom of speech and the right to a private life - translated into a current information society that must not neglect its citizens / users.

Guaranteed by the international treaties and conventions, the freedom of expression of the person in the 21st century develops a new dimension - the freedom of communication over the Internet - in the context of the European Court of Human Rights (ECHR, 10th March 2009) stated that the Internet archives are subject to article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, according to which *any person has the right to the freedom of expression, right which includes the freedom of opinion and to receive or communicate information or ideas without the interference of public authorities and without taking into account the borders.*

Although the texts of the international treaties do not explicitly mention the notion of Internet in the regulations regarding the freedom of expression, given that the Internet

becomes a means of communicating and expressing the users' opinions, presently the Internet community becoming an opinion-maker, we consider that article 19 point 1 of the International Treaty on Civil and Political Rights is also applicable to internet communication, any person having the *freedom to seek, receive and disseminate information and ideas of any kind, regardless of frontier, in oral, written or printed, artistically or by any other means of his/her choice.*

Without the need for interaction or geographic location of the members of a virtual community, the interpersonal relationships have evolved from the need for socialization and real and direct support among the members of a community, publicly manifested, to virtual relationships in community networks whose basic unit has become the individual located in an intimate, private space. Transposed into the public-private relationship, the development of interpersonal relationships in the virtual communities was supported by the Internet and the communication networks that made it possible to interconnect individuals in the private home environment, withdrawn into their privacy and geographically separated, into a common framework, publicly accessible to all members alike through the information that circulates and is accessible to the members of the respective community (Manea, 2015, p. 166).

Thus, although it may be personal data about the privacy of the user, the information thus posted on a virtual social networking site becomes, in principle, accessible to the public, and in the sphere of defining the public, through the setting systems of each site, the user can choose between the general public and the restricted audience, the latter represented by the group of friends and acquaintances.

The information circulating and being collected on the Internet from a common global infrastructure perspective that provides a broad range of economic, scientific, political and social activities represents an enormous amount of data about the users of the Internet networks, networks that collect, store and process this data, thus ensuring the freedom of expression for each user. In this context, there has been a growing need for legal and technical rules, harmonized at the level of cyberspace, to ensure the legal protection of human rights and the security of its personal data.

3. The Notion of *personal data*

From a legal point of view, both the definition in article 3 (a) of Law No.677 / 2001 for the internal law, as well as that contained in article 2 of Directive 95/46 / EC, encompass the notion of personal data, any information relating to an identified or identifiable natural person, for which including the sounds of the voice of the person concerned or images with a person represent personal data.

Thus, the identification of a particular person is made by reference to his / her surname and first name as well as civil status data (gender, date of birth, personal numeric code, home address, etc.), although some of this data is not strictly individual in relation to a person, and may be found in other people, so that corroborated, it can identify a particular person (for example, the surname is common to all members of a family, but there are also common surnames although there are no blood relations between people, as the date of birth is common to all the people born on the same day, month, year).

The only strictly personal and individual datum that can not be encountered in another person, even if there is identity regarding the other data, is the personal numerical code assigned from birth to each person in the National Register of Identification, representing

a significant number individualizing uniquely a natural person and is an instrument for the verification of the data regarding the civil status of the physical person and the identification in certain computer systems by the authorized people (article 6 paragraph 2 of Government Emergency Ordinance no.97 / 2005).

Returning to the definition of personal data in the above-mentioned normative acts, *an identifiable individual* means the possibility of identifying a person directly or indirectly in particular by reference to an identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity, which is why, together with the development of communications technology and the emergence of the personal mobile phones and e-mail accounts, the phone numbers and e-mail accounts have also become factors for identifying a certain individual thus entering in the scope of the legal protection of personal data.

From this perspective, Directive 2002/58/EC (Directive on privacy and electronic communications) was adopted at the level of the European Union, respectively at national level through the transposition of the Community normative framework, Law no.506/2004 was adopted, according to which the identification data is subject to the legal regime for the protection of personal data in the system of electronic communications of the users of the respective system without the need for them to be subscribers of the electronic communications service (these are the users of telephone numbers associated with phone cards) .

The same regulatory acts define the electronic mail as the *service consisting in the transmission over a public electronic communications network of text, voice, sound or image messages that can be stored on the network or in the terminal equipment of the recipient until the receipt (article 2, paragraph 1, letter g of Law No.506 / 2004 and article 2 letter h of Directive 2002/58 / EC), this becoming personal datum associated with the user authenticating on an online network by using the e-mail account.*

Taking into account both the express provisions of the normative act (art. 1 paragraph 3 of the Law no. 506/2004) as well as from the perspective of the technical way of creating an e-mail address (by introducing in the online electronic communications system of other personal data requested by the provider that administers the network), it should be noted that Law no.506 / 2004 is the special rule that is complementary to the general framework regulating the legal regime regarding the protection of individuals with regard to the processing of personal data in Law no.677 / 2001.

Unlike the European norms, the Romanian legislator defined (art. 3 letter h of Law no. 677/2001), in order to eliminate the confusion regarding the personal data sphere, the anonymous data as that data which, due to the origin or specific processing mode, can not be associated with an identified or identifiable person. From this legal perspective, pseudonyms or nicknames used informally represent anonymous data and do not benefit from the legal protection regime regulated by Law no.677 / 2001.

Considering the high social cohesion force it generates in virtual social networks, from the perspective of online processing of personal data in this type of electronic network, a special attention is given to the so-called *sensitive data, namely the data indicating the racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in a trade union / party, or data on the state of health or sexual life of the users.* This sensitive personal data may only be published with explicit consent of the individual regarding the processing for each type of sensitive data and in accordance with the purpose of each processing, even if the data was used in the configuration of the user's

electronic profile (typically the forms for creating profiles must state that it is optional to fill in the form with these personal data categories).

Obviously, if after the profile is made, the user distributes such sensitive data on his/her account, the operator can not be penalized if, after the voluntary disclosure of the person concerned, he processes such personal data, until the right of opposition of the person concerned is exercised.

4. General Rules on the Processing of Personal Data and the Rights of the Natural Person Concerned. Aspects Specific to Online Networks

From a technical and legal point of view, the processing of personal data is any operation or set of operations that is performed on the personal data by automatic or non-automatic means (both database operations and operations in scripted form by using some registers/workbooks (such as collecting, recording, organizing, storing, adapting or modifying, extracting, consulting, using, disclosing to third parties by transmission, dissemination or any other way, joining or combining, blocking, deleting or destroying it.

Given the large scope of operations circumscribed to the concept of data processing, the legislator regulated (art. 5 of Law no.677 / 2001, art.6 Directive 95/46 / EC) conditions and principles in which operators (natural or legal persons) can process the personal data, namely: the principle of good faith and legality, the condition of the specified, explicit and legitimate purpose for the data collection to be presented to the data owner, the use of current / updated data in relation to the purpose of collecting / processing and the condition of identifying the people targeted strictly for the time necessary to achieve the purposes for which data is collected and in which it will be further processed.

From the perspective of these legal conditions, any processing of personal data implies the express, unambiguous and conformable consent of the person concerned by informing him/her of the purpose of the processing by the operator (art.5 Law no.677 / 2001). In accordance with this legitimacy condition of the processing of data, the person concerned must be informed directly by the operator prior to obtaining the consent, of a series of information such as: a) the identity of the operator and his representative, if any; b) the purpose of data processing; c) additional information, such as: recipients or categories of data recipients; whether the provision of all required data is mandatory and the consequences of the refusal to provide them; the existence of the rights provided for by this law for the person concerned, in particular the right of access, the interference on the data and of opposition, and the conditions under which they may be exercised; d) any other information the procurement of which is imposed by the provision of the supervisory authority, taking into account the specificity of the processing (article 12 of Law No. 677/2001, article 10 and article 11 of Directive 95/46 / EC).

The right to information of the person concerned must also be ensured if the data is not obtained directly from the data subject, in which situation the same information previously mentioned must be provided to the data subject by the operator either at the time of collection or at the latest until the first disclosure, if it is intended to disclose it to third parties, unless the person concerned already possesses that information.

For the purpose of ensuring the right to information, certain online networks require the user who identifies / authenticates in the database by entering certain personal data an express consent to the processing of data by the respective electronic communications

service provider in accordance with the stated purpose of the activity carried out through that network.

This agreement is made by ticking in a field especially made on the site to confirm the consent of the person concerned, or by using certain programs to ensure that personal data is not entered / retrieved from an automated / electronic system, these steps being mandatory to take before authenticating online.

After creating a user account associated with the personal data of a target person, access to the network is made by using a user and a password, which become in relation to the user-accessed network, specific personal data associated with a single user in order to be identified in connection to the personal data associated with the account. These technical operations are also used as security systems for accessing databases by the online network users, some networks restricting the possibility of simultaneously accessing an online account from two different terminals by using the IPs of the computers on which the connection is made.

Any person concerned has the right to obtain from the operator, on request and free of charge for a request per year, the confirmation that the data relating to him / her is processed or not, right ensuring that the data used by the operator concerned is current and comply with the stated purpose of the processing (the right of access regulated by article 13 of Law No. 677/2001).

Dealing with the personal data of the user, another right granted to the person concerned is the right to intervene on his / her own data, a right exercised at the request of the person concerned and provided free of charge by the operator (art.14 of Law no.677 / 2001 and art.12 Directive 95/46 / EC).

Thus, at the date of the written request from the person concerned for data interference, operators must ensure: 1) the rectification, updating, blocking or deletion of data the processing of which is considered and notified by the data subject to be inconsistent with the legal provisions, in particular the incomplete or inaccurate data; 2) the transformation into anonymous data of data whose processing is not in compliance with the legislation, as notified by the person concerned; 3) notification to third parties to whom the data of the person has been disclosed in either of the above two ways, if such notification does not prove to be impossible or does not involve a disproportionate effort to the legitimate interest that might be harmed in its absence.

In order to ensure and guarantee these rights, providers of electronic communications services and online network administrators must notify users and permanently maintain on the site notices regarding the conditions for exercising the rights that ensure the protection of users' personal data.

Although at the time of giving the consent regarding the use of personal data by an operator, he was authorized to use the data of the target person in agreement with the purposes of the activities declared for processing, the law grants *ex nunc* the right of the target person to oppose at any time, from well-founded and legitimate reasons relating to his/her particular situation, that the data relating to him/her should be subject to processing after notifying the opposition, that is to say, the right to object, free of charge and without any justification, to the processing of the data which is intended to be processed for the purpose of direct marketing on behalf of the operator or a third party or disclosed to third parties for such purpose (article 15 of Law No.677 / 2001 and article 14 of Directive 95/46 / EC).

5. Conclusions

The safe and secure processing of information is an essential element of user trust in social networking systems, for which it has meanwhile been noticed the increase and decrease of the users' confidence in different online communication system operators by increasing / decreasing the number of accounts / active profiles of users.

Operators should apply the appropriate technical and organizational measures in order to ensure the protection of personal data both at the time of designing the processing system (i.e. at the moment of launching a social networking) and in the processing itself (during the functioning of the social network) with the purpose of preventing any unauthorized processing.

An important element of social network profile configurations is the access regime of the personal data associated with that profile, for which operators and network administrators must establish and predetermine restrictions on access to such data that each person in cause associate with his/her profile, thereby giving his/her consent to access intimate details by members of that network or by third parties in relation to the online network.

Networking services must establish implicit configurations that favour the protection of users' privacy, in accordance with the rights granted to individuals by legislation to ensure the protection of personal data processing, but allow network users to freely and explicitly accept any accessing of the content of their profile that exceeds the limits of the user's agreed contact list in order to reduce the risk of third-party illegal processing of personal data.

References

- Cimpoeru, D. (2013). *Dreptul Internetului* [Internet Law], Second Edition. București: C.H. Beck.
- Manea, C.A. (2015). Social Networks and Information Security in Virtual Environment Communication at the Organizational Level. In *The International Scientific Conference Globalization, Intercultural Dialogue and National Identity GIDNI 2015*, Târgu Mureș, p.165-172.
- Uerpmann-Witzack, R. (2010). Principles of International Internet Law. In *German Law Journal*. Vol.11 No.11. Charlottesville: German Law Journals Inc. Available at: https://epub.uni-regensburg.de/21561/1/Uerpmann_PrinciplesIII_GLJ_Vol_11_No_11_1245-1263.pdf . Accessed: 23.03.2017.
- *** *Convention for the Protection of Human Rights and Fundamental Freedoms* Roma 04.11.1950. Available at: <http://www.echr.coe.int>. Accessed: 20.03.2017.
- *** Directive 2002/58/EC of the European Parliament and of the Council concerning the processing the personal data and the protection of privacy in the electronic communications sector, published in Official Journal no.201 from 31 July 2002.
- *** 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 the Directive 2002/58/EC, published in Official Journal no.105 from 13th April 2006.

- *** Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, published in Official Journal no.281 from 23 November 1995
- *** ECHR, 10th march 2009. *Fourth Section. In the case of Times Newspapers Ltd. (nos.1 and 2) vs.The United Kingdom.* Judgment of 10th March, Application 3002/03 and 23676/03. Available at: [https://www.article19.org/resources.php/resource/3114/en/echr:-times-newspapers-ltd-\(nos.-1-and-2\)-v-the-united-kingdom](https://www.article19.org/resources.php/resource/3114/en/echr:-times-newspapers-ltd-(nos.-1-and-2)-v-the-united-kingdom). Accessed: 20.03.2017.
- *** Emergency Ordinance no.97/2005 on the registration, domicile, residence and identity papers of the Romanian citizens, published in Official Gazette no.641 from 20 July 2005, republished in Official Gazette no.409 from 10 June 2011.
- *** Law no.506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, published in Official Gazette no.1101 from 25 November 2004.
- *** Law no.677/2001 for the protection of individuals with regard to the processing of personal data and the free movement of such data, published in Official Gazette no.790 from 12th December 2001.
- *** *The International Covenant on Civil and Political Rights* 16th December 1966 General Assembly of the United Nations approved by Decree no.212/31.10.1974 (Official Bulletin no.146/20.11.1974)