

Ethics and pragmatics of information Security and privacy in traditional and electronic libraries

Silvia Adriana Tomescu, PhD, Scientific researcher, Academy of Romanian Scientists, E-mail: silvia.tomescu@bcub.ro

Mihail Dumitrache, PhD, Scientific researcher, Academy of Romanian Scientists, E-mail: mihaildu@rotld.ro

Abstract

Romanian libraries are institutions strongly attached to the social environment, through which carry out the role of cultural and educational pole of the community. Any change at the social level affects more or less the internal mechanisms of the organization. Amendments to international law on the processing of personal data also have effects on these information structures. From this perspective, we intend to analyze, in a comprehensive way, the main areas of influence that privacy and privacy laws have upon the library. Thus, we investigated the library-user relationship, library-employee, and some of the ethics of information issues. Obviously, on a national scale, all these ideas will have a specific treatment after the unitary analysis of the intersection of legislation with the field of practical data activity. We consider that approaches related to the convergence of the personal data processing with the ethics of information and the main practical procedures that will be implemented in Romania have not only a theoretical justification but above all, became a prerequisite to act rightful.

Keywords: personal data, integrated systems, libraries, data protection

Argumentum

In the standpoint of the new EU Regulation 2016/669 on the protection of individuals, with regard to personal data processing, as a data controller, libraries need a new operational framework. Equally, the new legislation, which entered into force on the 25th of May 2018, requires public institutions that operate personal data to designate a person responsible for data protection. At this point, through a law applicable at European level, in most public and private institutions that manage data appeared a new occupation – "*data protection officer*" or DPO. All these regulations concern the protection of individuals as a *fundamental right*. (Regulamentul (UE) 2016/679). From this perspective, international bodies seek to harmonize international regulations and to provide universal structures to the new provisions.

Considered legitimately, data protection *confers rights and responsibilities* equally. Questions as: *what are the main legislative and infrastructure requirements? What risks can occur for beneficiaries and processing institutions?* raise factual organizational problems and later application issues. Data processing is characterized by *collection, recording, organization, archiving, adaptation, retrieval, consultation, transmission, use, dissemination*. A challenging research to make available answers to such a problem should start from:

- (a) The examination of the *personal data processing flow* – collection, registration, organization, archiving, adaptation, retrieval, consultation, transmission, use, dissemination;
- (b) The analysis of procedures, programs, policies, methods for recording and methods of personal data circulation in libraries;
- (c) Assessing users' perception about the methods personal data is used;
- (d) The analysis of organizational practices and privacy policy;
- (e) Institutional insertion in the context of *cyber threats*.

Identity management is accomplished through processes, tools and contracts that underpin the conception, maintenance, and removal / deletion of a digital identity, ascribed to people in order to secure access to an extensive set of systems and applications. Access control to data resources became there the primary characteristic of an identity management program in the online environment. Considering the human behavior in the virtual environment a reflection of the various existing and manifested standards of living in the physical world, activities involving the use and transfer of personal data became the subject to certain regulations. The *sensitivity of data* is given by their characteristics as: standard date, date of birth, height, civil status, studies, telephone number, photograph, while sensory data includes genetic information, health information, regressive or sexual orientation. According to 30 art., institutions are required to keep a record of the processing activities including:

- (a) The personal data operator and his identification data;
- (b) The purpose of the data processed and the types of persons involved;
- (c) Recipients (individuals or entities);
- (d) Deadlines for data deletion;
- (e) Technical and administrative security measures.

At the request of the supervisory authority, the operator shall make available the processing records. Concerning the institution's task in applying the security measures in the data processing, 32 art., specifies that the operator and the person empowered shall implement appropriate technical and organizational measures to ensure a security level as encrypting the data, ensuring its confidentiality, ensuring the resilience of processing facilities, assessing the periodic effectiveness of the implemented measures. It is specifically stated that the "*evaluation, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed*" must be considered in the assessment process (Article 32, paragraph 2.)

The 2015 Euro barometer reported highlighted the following on personal data protection:

- a) In the European Union 89% of the respondents asked considered data control to be very important, while 69% were concerned about the use of these data for various purposes;
- b) 86% of respondents interviewed in Romania considered the protection of personal data very useful in any state where the data operator is located, while 53% of Romanians consider that they have partial control over personal data.

As with the EU survey, 71% of Romanians are concerned about the risks of the use of personal data for other purposes (Centrul European al Consumatorilor din România).

Information Ethics

"It seemed that when people entered the computer center they left their ethics at the door"
(Don Parker, 1968)

Ethics in this scientific field involves responsibility and decision. New ICT developments have enabled a new type of ethics, *computer ethics*, which regulate parameters and types of activities, and how they are being developed in the social-technological interaction.

Obviously, before any notable beliefs, the global force is ensured by the governance of the law. The design of computer systems must have the whole idea of *good* for the collective and individual use. The technological component of any entity that processes personal data should aim to preserve *integrity* and *identity* through *access policies*. Personal data is, beyond any other undertone, a reference to privacy that is not advertised or negotiated. E-commerce as well as events related to the Big Brother phenomenon has demonstrated how vulnerable are electronic communications systems and, implicitly, how exposed the human being is. Newer social-media networks – the recent *Facebook- Cambridge Analytica* scandal has emphasized how easily we give up or even do not take ethical principles into account when, over them, economic or political interests transcend. In fact, it has been demonstrated that the most easy to acquire data and privacy agreements are related to the use of software applications, web pages whose "terms and conditions" or "confidentiality clauses" are dealt with "agree" - a well-understood formula without careful, and engaged reading.

There is an ethics of system and program makers as well as an ethics of operating agents or system and network users. The entire work environment from design to exploitation must take into account ethical principles and code of conduct. Even though the last decades have promoted freedom of information, expression, and access to information, they need a well-regulated framework, and the type of behavior in these spheres is desirable to be guided, outlined by ethical principles and norms.

The main attributes that define the area of information and communication technology are *exclusive, private, accessible, and secure*. Safety provides not only the accuracy of the information but also the protection of the environment where it is taken out. The ethics of data production use, organization and dissemination through the Internet must be a

critical research and insight aiming at socio-philosophical thinking, communications technology theories and approaches, system theory, etc.

Aspects of the Processing of Personal Data in Libraries

According to the GDPR, libraries as public authorities, institutions governed by public law, will have to entitle a person responsible for the personal data processing. The institutional responsibility of libraries for the personal data processing lies in prevention and control actions. In the information, communication and circulation of documents flow, library will have to become an entity that *collects, stores, views, modifies, uses, deletes and transfers data* within the limits of the legislation and the working procedures developed. The directives on how data is processed have as a primary term the consent of the person, the consent that can be revoked. Libraries use multiparty data to define relationships or behaviors.

Protection of Data in Relationship Library - Employee

If a legal person, publicly owned, such as library, processes personal data for the purpose established by Government Decision no. 500/2011 on the general register of employees, it has the status of *personal data operator*. All institutions processing employee data according to Government Decision no. 500/2011 have the duty to observe: *the right to information* (Article 12), *the right of access to data* (Article 13), *the right to interfere with the data* (Article 14), *the right to object* (Article 15) *not to be subject to an individual decision* (Article 17) and the right to *appeal to justice* (Article 18), *ensuring the confidentiality and security of the processed data* (Articles 19 and 20). The designated person in charged with data operation in the employee register shall be the *data controller's empowered person* (Protecția datelor personale și registrul general de evidență a salariaților) and the specific activity must be mentioned in the *employment contract* as well as in the *job description*. The 677/21 November 2001 law institutes the rights of individuals with regard to information, access, transfer, data interference and the right to appeal to justice, for which libraries must outline physical, electronic, and electronic records of processing, storage and physical archiving for work.

An extremely important aspect to be regulated at organizational level through specific work procedures stands the *circulation of personal documents* (applications, study papers) or institutional (contracts) containing personal data through Document System Management - DMS software, securing access to accounts and documents and monitoring software to eliminate risks. Perhaps an inquiry of the appropriateness and legality of stating a *confidentiality clause* in certain employment contracts would support the security of *personal data* as well as *privacy*.

In the accounting and human resources departments procedures and regulations must state: (a) The purpose of the processing (drawing up employment contracts, decisions, calculating salaries, contributions transfers, certificates issue); (b) The length of the data processing (usually as long as the employee has a contract with the institution plus a period of document archiving according to the legal provisions); (c) System auditing

(integrated systems, accounting software, document management software); (d) Managing security incidents.

The systems must meet the two features: *privacy by design*, programs with their own design come with data security tools and *privacy by default systems* which provide users with the ability to retain privacy control.

The institution responsible for the proper implementation of these provisions is the National Authority for Personal Data Processing Supervision, ANSPDCP; the library as data controller, will have to notify it about the designation of the Data Protection Officer.

Data Protection in the Library - User Relationship

In the environment of the new cyber-attacks of the data leakage process, institutions are required to *prevent, monitor and detect* vulnerabilities through technology mitigation and highly skilled staff. In the Romanian libraries, personal data is recorded and processed based on a Declaration/Commitment made in agreement with the organization and operation regulations, all of which being archived for a number of years. Integrated library systems such as Aleph, Vubis, Tinlib, used at national level, etc., have different characteristics and parameters, access policies. Equally, EVACC the accounting documents management system of ("Carol I" Central University Library) is used in the professional work environment, so, it is necessary to develop procedures regarding the document track, access rights, editing and visualization rights. In order to grant the rules and procedures at organizational system, it is essential to institute: (a) Services / offices processing personal data; (b) Identity deposits; (c) Types of users; (d) Data sharing activities; (e) Attributes "critical", "confidential".

As a conclusion, we can say that good governance is needed to access these data types and to monitor the compliance of data processing. There are frequent shortcomings in the national libraries system, as well as countless unexpected situations, generated by the lack of technology, the qualified staff, and the minimum necessary budget.

For this reason, the problems faced by many libraries are related to the fluctuation of staff, lack of high skilled IT specialists who do not cope with the low pay levels; as a consequence, managers of these institutions are set in a very delicate circumstance to replace specialists and launch training sessions, to cover these issues. The existence of several integrated software, as is the case of BCU "Carol I", thus multiple data stores, increases the effort to manage access to personal data.

In order to broadly harmonize the existing problems, it is necessary to organize the plan and *access areas, access policies* and *types of users* (category of librarian and category of reader), to introduce the specifications related to data processing in the employees' job descriptions, initial and ongoing training, special situations (marketing/statistics) in which personal data are produced and used, recalibration of official documents with the new legal provisions in force.

International Legislation:

- EU 2016/679 General Data Protection Regulation applicable from May 25, 2018;
- Charter of Fundamental Rights of the European Union;
- EU Data Protection Directive (Directive 95/46 / EC);
- Digital Agenda for Europe;
- IFLA Statement on Privacy in the Library Environment;
- LAW no. 506 of 17 November 2004 on the processing of personal data and the protection of privacy in the electronic communications sector
The Romanian Parliament adopts this law.

Proposals and Conclusions

- Elaboration of internal working procedures specific to each entity;
- Comparative study of software;
- Grant ROF and Code of Ethics;
- Completion of job descriptions with specific data processing tasks;
- Obligation to keep confidentiality on personal data;
- Continuous training on data security and specific legislation.

References

Centrul European al Consumatorilor din România [online]. Retrieved March 4, 2017 from <http://www.eccromania.ro/53-dintre-romani-considera-ca-au-control-partial-asupra-datelor-personale-furnizate-line/>

Parker, D. (1968). Rules of Ethics in Information Processing. *Communications of the ACM*, March 1968, vol. 11, nr. 3, p. 198-201.

Protecția datelor personale și registrul general de evidență a salariiților [online]. Retrieved May, 17, 2017 from http://www.dataprotection.ro/?page=Protectia_datelor_personale_si_registrul_general_de_evidenta_a_salariatilor&lang=ro.

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016, privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) [online]. Retrieved May, 27, 2016 from: <http://eur-lex.europa.eu/legal-content/ro/TXT/?uri=C„ELEX:32016R0679>.

Tomescu, Silvia; Dumitrache, Mihail. Ethics and Pragmatics of Information. Security and Privacy in Traditional and Electronic Libraries În: *Information and Communication Sciences Research*. Editura Universității din București, vol 22, 2018, p. 41-46.