THE FIELD OF PERSONAL DATA PROTECTION - SPECIFIC AREA OF REGULATION

Veronica MOCANU,
master of Law, University lecturer at the chair "Theory and history of law", Faculty of Law

SUMMARY

Diversity and complexity of social relations are necessary to organize and regulate relations between people or groups of people and adopting new regulations in this regard. Information society is a new social reality that raise new types of relationships related to collecting, storing, processing, transfer and dissemination of various types of information. With the advent of these relationships, there is a need to build a adequate legal framework on the necessities and reality created. Regulation of these relations must be made taking into account the specific of this area, because behind these rules we achieve one of the main objectives of the State, namely, providing and guaranteeing fundamental human rights.

REZUMAT

Diversitatea şi complexitatea relaţiilor sociale fac necesară organizarea şi reglementarea raporturilor dintre oameni sau grupuri de oameni şi adoptarea noilor reglementări în acest sens. Societatea informaţională reprezintă o nouă realitate socială ce determină apariţia unor noi tipuri de relaţii legate de colectarea, stocarea, prelucrarea, transferul şi difuzarea diferitor tipuri de informaţii. Odată cu apariţia respectivelor relaţii, se creează şi necesitatea edificării unui cadru juridic adecvat necesităţilor şi realităţii create.

Starting from the idea that personal data protection law is a part of the information field, it should be mentioned that the regulation mechanism of data protection field also, must be seen from general to particular, especially from the fact, that to regulation of personal data field will be assigned characteristics similar to those of information society regulation, highlighting certain features.

Speaking about the regulation of informational society as a notion, we can mention that, it broadly means all regulations used by individuals partially or public authorities and/or private, to organize the relations regarding the exploration of the information. If we accept the idea that the society we live in is an informational one, then we can certainly mention that all normative-legal acts, social norms, including those of self-regulation, regulation and judicial practice forms the material law of the informational society.

Because the informational field is a specific one, we think that we need to start by defining the rules generally and setting the specific features.

If we start from the DEX definition, then regulation is defined as a process by which something is subject to some norms or regulation, are established legal relationships, are legalized and put in order. Most approaches state that the regulation involves a complex activity ordering the society through the establishment of rules imposed to follow.

Until recently, was accepted the idea that the regulation is a state task only, but now, due to the diversification of political, social and economic life, not every relationship should be targeted by the state as one needed to regulate, therefore appear different forms of self-regulation, which often become to be more effective and swift than some regulations emanating from public institutions.

In order to identify all aspects of a problem, it's necessary to address the matter from the systemic approach. Addressing the problem of personal data protection field regulation, it's necessary to take into account all currently existing regulations and their application in practice, used features and tools.

However, it's necessary to men-

tion that by its content, the regulation activity covers the whole range of instruments, legal acts and actions designed to streamline the human behavior.

By their essence, legal rules form a whole, being very closely linked together, even though they are different by content. They form a coherent and logical ensemble; therefore they join into a system. A state right appears to us not as an arithmetic sum of all given legal norms, but as a set of them organized, structured in a system based on certain principles, following a particular purpose.

Studying the law system has a theoretical and practical importance, namely: helps state organs in the development and improvement process of law to find and fill gaps in positive law, to eliminate obsolete regulations and to ensure the consistency between legal rules.

The law system is the basis of the legislation systematization, contribute to the classification of legal sciences and improve application and interpretation of law. The practice of personal data protection regulation may be approached differently, depending on the subjects involved in their development, the territorial scope of the regulations, its manifestation, used tools etc.

It should be noted that due to its specificity and requirements of globalization and standardization, protection of personal data should be regarded not only from national regulations point of view, but also from international ones.

Moreover, because of its specific condition in regulations studying this phenomenon, one of the issues that are necessary to approach as stringent, is determining the applicable law. Also, we note through this work and on the fact that personal data protection is a complex institution, its content being made both by material and procedural norms.

Inquiring the regulation of this area, it is necessary an analysis of standards and regulatory instruments.

The Russian literature, for example, approaches the issue of data protection regulation through the mandatory existence of the following four components:

- The existence of a framework law, which establishes the basic principles;

- The existence of sector laws, that guarantee and establish the mechanism to ensure the protection of personal data in a particular field;

- The existence of an organ or organ system empowered with control and supervision of data protection;

- The existence of corporate regulations, designed to ensure and to protect data in a unit;

At the contemporary stage, thanks to many efforts made both at national and international level, the governing system of personal data protection can be divided into national and international regulations.

At the moment, due to the specific condition of the regulated phenomenon, growing trends of globalization and uniformity, more often it's insisting on the existence of extraterritorial regulations that would be uniform and generally acceptable for any country.

As indicated above, the system governing the protection of personal data can be approached not only from the territorial perspective, but also in terms of regulatory authorities involved in the used mechanisms. Thus, regardless of the territorial aspect, depending on the involved authorities involved both in international and national regulations, to them can be attributed as components the following regulatory forms:

Public normative regulations, referring to them:

- Fundamental regulations (regulations that states basic principles, guarantees the insurance and achievement of the main human rights and freedoms. Such regulations are found in the Con-

stitution and in fundamental international documents);

- Basic regulations (regulations underlying a particular area, establishes the scope, principles of the given area, they usually takes the form of organic and ordinary laws, ex. Law on personal data protection);

- Sector regulations (detailed regulations for certain sectors are usually embodied by law);

- Institutional regulations (regulations establishing organs, powers, functions; they are materialized usually through decisions, orders, decrees);

Normative voluntary regulations (self-regulation) require the existence of a system of rules voluntary developed, in order to establish relations, organization of certain internal activities, which are represented by contracts, codes of conduct, internal regulations or security projects.

Technical regulations require the existence of rules established by scientific means, based on technical conditions data, established for conducting a technical process; Thus, in order to approach the complete problem of personal data protection regulation field, we propose the detailed analysis of each type of regulation.

Public normative regulations

In fact, the distinction between the types of regulation proposed above derives from the type of the engaged actors, used mechanism and legal force. Being one of the main forms of ordering personal data processing relations, public normative regulation, still remains as the most rigid and efficient form of regulation, being primarily due to the coercive force with which legal norms are endowed and state involvement in their development, implementation and realization.

Public normative regulations are composed by legal rules derived from the public authority, so, public normative regulations get the characteristic features of the legal norm. Thus, we can highlight the following features proper to normative regulations in general and to personal data protection regulations in particular:

- State character;
- Coercive character;
- General and impersonal character;
- Compulsory character;

Thus, due to its pervasive and imperative nature, public normative regulation becomes an urgent necessity. General interest which is protected by this form of regulation, justifies government's intervention by its authorities at all stages of regulation and enforcement.

So, when the state initiated the development of databases and once it's the manager of some complex information resources regarding to its individuals and their creation is grounded with the idea that they would be a way to optimize public expenses and the activity of these units, such country should be a regulatory body responsible for ensuring safety of personal data of its individuals.

However, it's necessary to mention that due to the exclusive powers, only the state can provide fully and he is and must be the guarantor of personal data protection. One of the exclusive powers to which were referred above is also attracting to criminal liability. Approaching constitutional norms as rules that are part of the data protection regulation field, we can say that usually, they have a scope to consecrate the fundamental principles and refer to privacy and confidentiality.

These have a very general character, and refer to person, family and private life. The content of the right to privacy, family and private, includes the person's right to family protection and to be respected, the right to dispose itself, the right to identity and to own image, so, in the light of this content it may be customized and the right to personal data protection.

Because of recent occurrence, personal data protection law, although it is recognized in many international acts as a fundamental one, though it's not expressly regulated in the most Constitutions. Although the problem of these relations is issued as quite important and current, the legislators are abstained however, from the inclusion of some provisions regarding personal data protection field in the fundamental acts.

The most floated argument is that protection of personal data is a part of the privacy area and this subject is sufficiently regulated in many aspects. Romanian doctrine of the constitutional law, for example, founded this right as a part of the inviolabilities category, being also considered a "human right", under its aspect of privacy right and privacy respect.

Starting from the idea that personal data is an element of private life, we will agree the idea that it's not the situation to take measures to modify the constitutions when they include provisions that ensure private life concerns, privacy and/or confidentiality.

Thus, once there is awareness and use of personal data as an inherent right of human person and there's no the possibility of its valorization from constitutional perspective, we consider more necessary to take measures and to work toward improving the framework and the sector regulations.

Following mentioned above, we state on the idea that however, in the conditions of existence of constitutional guarantees relating privacy insurance, legal basis of data protection with personal character is determined by the basic law, such law as Data protection Act. (Law on personal data protection). Such laws are often called framework laws because by their content, they determine the sphere of actions and contribute to the institution formation.

In our example, personal data protection law creates the personal data protection institution and the right to personal data protection. Also, framework laws establishing the principles, goals and regulations structure, establish control and oversight bodies, giving powers and functions, specify the relationships scope and identify the subjects, rights and obligations governing the development and implementation mechanism.

Another category of regulations within normative regulations are sector regulations, these being some of the basic and additional regulations and are intended to establish rules in a particular field.

In the context of our study, sector regulations come as a complement to basic law and set standards for a specific area, such as trade, education, health and others.

The necessity for such regulations is argued by the possibility of multifaceted and specific regulation of a field in part, taking into account, all circumstances and field characteristics. The practice show that usually by sector regulations is attracted the attention to specific areas. Thus, sector regulation of the European space, has a starting point.

Recommendations of the Committee of Ministers of the European Council, among them being able to be listed the following: profiling 19 (Rec. (2010) 13), collecting and processing of medical data (Rec. (97) 5), data used in telecommunications services, particularly in telephony services (Rec. (95) 4), personal data held by public authorities and communicated to third parties (Rec. (91) 10), personal data used for payment transactions and other related (Rec. (90) 19), epidemiological data collection and primary health care (Rec. (89) 4), data used for employment purposes (Rec. (89) 2), personal data used in the police sector (Rec. (87) 15), processed data on social security (Rec. (86) 1), used data for direct trade (Rec. (85) 20), the use of personal data for statistical goals and scientific research (Rec. (83) 10), medical databases (Rec. (81) 1), the exchange of information between authorities from different states (Rec. (80) 13) [2].

Institutional regulations are usually evidenced by decisions, directives and orders requiring the establishment of some bodies or mechanisms. In the case of personal data protection field, institutional regulations have a special importance, because they involve the establishment of monitoring bodies and control of personal data protection, which is a requirement to follow in the context of achieving the protection of personal data as a social, legal and political phenomenon.

Voluntary normative regulations (self-regulation)

Voluntary normative regulations (self-regulation) are a reality of the contemporary society, they often are materialized in the areas of regulation where the government was not concerned or did not sufficiently concerned. Thus, voluntary rules are an effective way of ordering the behavior of individuals involved in a structure, regardless the organizational form or the ownership, it's important that the content of these regulations do not conflict with national, international legislation, if it's ratified.

Governmental organizational norms are like legal norms, even drawing penalties for their failure, but cannot be confused with the legal norms, because they lack that, what is essential, namely: their protection and coverage through public power and the coercive force of the state. Some authors call them quasi - legal norms. Nongovernmental social organizations activity and their acts must comply with the laws of the country, to be a part of the existing legal order.

Usually, voluntary rules are relating to the establishment of principles and/or rules of intern conduct, the adoption of codes of conduct, the establishment of control organs and their regulation or developing and implementing projects of personal data security, the establishment of relationships and guarantees by signing contracts.

One of the most commonly used forms of voluntary regulation of personal data protection field is the ethic code.

There is no universally accepted definition and content of the ethic code, legal form or power; they vary from a state to state. The law on data protection in the Netherlands for example, establishes that the codes of ethics are a totality of rules or regulations concerning the processing of personal data and are adopted at the organization or in a particular sphere and have a compulsory character.

Analyzing the variety of existing ethic codes, generally we identify two types of codes, one aiming the regulation of data processing per unit and the second type having as a goal the regulation of personal data in a certain sphere of human activity such as banking sphere, insurance, medicine or even in a particular region.

For the second type of codes it's characteristic the existence of a sector supervisory body, represented by the union, federation, congress, etc. In the case of voluntary sector regulations the unit are fully sanctioned, such sanctions may be the exclusion from the union, deprivation of any privileges or the denial of access to common databases etc.

In the situation of ethic codes per unit, usually, the most serious sanction is the dismissal and it's applied individually, in some countries including the U.S., the disciplinary sanction in the field of personal data damage it may attract the criminal liability. The pioneer of ethic codes development regarding data protection is considered the company American Express, which in 1970 developed a set of rules to ensure personal data protection and being compulsory for its employees under the sanction of dismissal.

Currently there is a tendency of ethic codes of regulation, so this practice was followed in Australia, Norway and Ireland. Thus, in Ireland, the body of control and data protection supervisory has in

its competence the evaluation of contents of ethic codes and in the case they match perfectly the legal regulations of data protection, then it may be submitted to Parliament for confirmation and granting the status of sector law.

Another version of corporate regulation of personal data protection is developed in Germany; it assumes the obligation imposed by law to develop ethic codes on data protection in companies with more than four employees, who have the jurisdiction and powers of personal data processing.

In Switzerland were developed regulations through which all organizations that have in their activity tasks related to data use or processing, are required to hold in the staff a person responsible for controlling and monitoring the use and processing of personal data, with both control obligations and as well as creation of security projects.

In Norway is followed the version of self-regulation by stimulation, so the law on personal data protection establishes that sector associations are entitled to develop ethic codes to ensure the protection of personal data and in the absence of such initiatives of self-regulation, empowers the supervisor organ with the development of protection regulations for particular sectors.

Thus, in order to avoid state involvement, sector associations have produced a record of sector ethic codes on data protection. Moreover, at the moment we are at a stage when the role of voluntary regulations was widely acknowledged by the European bodies.

In his concept of personal data protection system reform, the Council of Europe and reform advocates give a special importance to voluntary regulations. So, under new rules proposed to European Community member states, the supervisors encourage the development of conduct codes, intended to contribute to the smooth implementation of normative regulation and which should promote norms for processing data in a fair and transparent way, public and the concerned persons information, compliance subject applications in the exercise of their rights, informing and protecting children in the context of data processing, the promotion of mechanisms of monitoring and compliance with legal regulations by operators which adhere to the Code, promoting extrajudicial procedures and other procedures to dispute resolution in disputes between operators and data subjects regarding the processing of personal data, without prejudicing the rights of data subjects.

In order to establish a control over the conduct codes and to promote the uniform application of legislation, reform advocates recommend to Member States to adopt regulations under which the associations and other bodies representing categories of operators or persons authorized by operators wishing to establish conduct codes or to modify and extend the existing conduct codes, can present them to issue an act from the supervisory authority in that Member State.

The supervisory authority may issue an opinion on compliance with this Regulation of the draft code of conduct or amendments thereof. In the sense of indicated above, the supervisory authority will seek data subjects views or their representatives on these projects.

Moreover, through new reforms the European community doesn't stop at the encouraging the adoption of conduct codes, but is taking action for the establishment of minimum necessary standards of protection to be observed by each data operator. This will be achieved by imposing the imperative of adopting corporative rules. Thus, member states will have to improve their laws to enforce corporative rules as binding rules and to state that they must refer at least to the structure and contact data of the group of companies

and members of its composition, data transfer or the set of transfers, including the categories of personal data, type of processing and processing purposes, concerned persons categories and identifying the third country or third concerned countries, record the general principles of data protection, limitation of processing scope, the obligation to indicate the legal basis for data processing, adopting measures to ensure data security, the recording of data subject's rights and means to exercise these rights including the right not to be the object of a measure based on profiling, the right to complain to the relevant supervisory authority and to the competent courts of the Member States, in accordance with article, the right to obtain compensation and, where appropriate, compensations for violation of mandatory corporate rules, indicating the acceptance of the agreement to be responsible for any breach of binding corporate rules [1, p. 73].

So, in the case when respective reforms will be adopted and the Republic of Moldova will continue the desire for European integration should be to connect our legislative system to requirements listed above.

Concluding on the practices of developing ethic codes to regulate certain relationships concerning the processing of personal data, we mention that they usually occur being driven by the following logics:

- have as a goal the normalization of relations of which regulation the state bothered;

- have as a goal the achievement of norms, developed by the state;

- come to complete the existing legislation, becoming some related regulations;

- have as a goal the prevention of state intervention in regulating the behavior of data operators from a particular field;

The reason of codes development, largely determines in a big measure their form, so the codes aimed for normalization of relations which bothered State regulation, usually have a general content based on principles and definitions, codes designed to achieve state developed standards have a much more complex content, making them viable tools to protect personal data because they provide mechanisms, guidelines, sanctions etc.

Due to different regulatory practices through codes, in specialty literature was formed two lines, one, that supports ethical regulations and other regulations, denying the effectiveness of these regulations. To form their own opinions, we will read both skeptics and optimists ideas, so, the arguments in favor of adopting regulatory codes of conduct as forms of personal data processing are:

- Ethic codes are some viable, dynamic and flexible tools;

- Conduct codes may contain provisions quite thorough, which cannot be realized by law;

- Ethic codes are adopted by professionals who know the processing techniques and methods of damage;

- They are pointing directly toward the operator; they can easily become a handbook;

- Through codes it may regulate data processing in very narrow areas;

- The use of codes in the regulation of data processing, doesn't prejudice public regulations, contrary, they come as a complement;

The arguments against the use of ethic codes as a form of regulation of the relationships of personal data processing are:

- Data protection regulation through codes in the absence of government regulations is dangerous;

- Conduct codes that are developed by professionals, can confuse the content of certain terms and may mislead the operators;

- Personal data holders don't know about the existence of conduct codes within the companies,

so in the case of prejudice they do not know where to address;

- The existence of ethic codes implies the existence of control bodies, which also involves the formation of additional expenses;

Concluding the above indicated, we consider conduct codes a way of regulating complementary relationships of personal data processing.

Also, we insist that ethics codes should have a richer content than definitions and principles, they must assume the regulation of mechanisms to prevent personal data acts of fraud, and they must regulate forms of punishment to be viable, practical and not formal ones.

Conduct codes should not transcribe data protection law regulations; they must move further to be a continuation of public regulations.

Also, because of the specific relations and the rapid development of systems and processing procedures, the codes are imposed against laws as a form of a more dynamic and flexible regulation, easy and quick to change.

A chapter in the context of voluntary regulations necessary from the prospective of protection of personal data realization, are so-called internal regulations or insurance projects on personal data protection. Currently, any structure through competence is an operator of personal data.

Reality shows that in terms of the informational society development, any public or private institution, legal person or an individual can have a personal data operator, having in its attribution tasks of collection, storage, use, processing, dissemination and data transfer. But all these processes require the compliance with certain principles, rules relating to the insurance of data security that rumor, but these rules can be subject of each specific activity.

So, in order to regulate individual activity or operators of a unit or sphere it's necessary to develop rules to ensure safety, materialized in the form of regulations, instructions and security projects. Regulation of operator's activity is a quite complex one and is rooted in regulation norms of informational society. The regulation of data processing activity per unit must start from the following principles:

- Confidentiality - protecting the privacy of unsanctioned uses;

- Integrity - ensuring accuracy and data integrity during sanctioned uses;

- Accessibility – insurance the access to authorized personal data structures;

Development of necessary regulations to guide the data processing unit is already an activity whose necessity is recognized. Thus, this process involves several stages, as follows:

1. The research of access resources, collection, storage, use, processing, distribution, transmission of personal data. This activity consists of:

- Analysis of informational resources;
- Identification of data that is working in each set of information resources;
- Data flow analysis;
- Identification of data protection measures;
- Identification and analysis of data prejudice and their opposing measures security, establishing consistencies or inconsistencies;
- Analysis of the necessity to use the cryptographic security;
- Establishment of patterns of fraud and fraudulent typing;
- Opposing the researched situation to legal existing norms, the detection of asymmetries and inconsistencies;
- Development of the report that must include information and conclusion on each of set out points, followed by identifying the needed steps to be done to ensure data protection in that company;

2. Design and implementation of technical measures established in the research report.

3. Development of the necessary rules followed by operators

within the realization of activities related personal data use.

Technical regulations gain an increasingly connotation in recent years and are increasingly considered as an alternative regulation, being assigned to the category of informal regulations.

In the conditions of advanced technology development, legal norms do not always remain to be competitive with technical ones. Thus, technical regulations often can provide a more increased protection than legal ones. The main technical means that ensure data protection can be listed as follows:

- technical limitation of collection operations;
- implementation of operational processes of data processing without the participation of the human factor;
- ensuring advanced security;

The role of technical regulations is realized in particular by private actors, but at the moment the European Community by proposed reforms, is expressing its clear approval behavior of these forms of regulation. By the proposed reform project of the European data protection system is encouraged the establishment of certification mechanisms for data protection and data protection seals and marks, enabling subjects to evaluate quicker the level of data protection that is provided by operators and mandated persons. [1, p. 74].

However, technical regulations doesn't exclude the legal regulations, contrary, technical regulations often find their origins in the legal ones. Thus, Baldwin, R.D. in his work "Better Regulation in troubled Times" to achieve an advanced protection of personal data, proposes a combination between technical regulation methods and legal ones, adding the necessity to implement in data processing process the following principles: transparency, participation and accountability [3, p.203].

Regulatory coordination and technical standards can improve regulatory efficiency, minimizing the need to resort to more punitive forms. However, we believe that voluntary legal regulation and technical one are some interdependent phenomena and only sharing them can help provide advanced protection of personal data.

But even the use of sophisticated regulatory mechanisms will not achieve the goal, if will not exist an increased interest from carriers and personal data, materialized through advanced civic activism. Thus, state efforts must be directed not only towards the development of regulations, but also to mediation and imposing their recovery.

Bibliography

1. Proposal for Regulation of the European Parliament and of Council on the protection of individuals regarding personal data processing and free movement of such data (General Regulation on data protection), Bruxelles, 25.1.2012, page 73

2. Sârcu Diana, Rusu Valentina. The concept of personal data and personal data categories protected in the Council of Europe, Moldavian Journal of International Law and International Relations, No.3, 2011, page 11

3. Baldwin, R.D. "Better regulation in troubled Times", Health Economics, Policy and Law (1), 2006, p. 203-207