Journal of Systemics, Cybernetics and Informatics (2022) 20(2), 17-22
https://doi.org/10.54808/JSCI.20.02.17

Privacy of Data Against the Challenges of Information Technology from the Perspective of the Normative Regulation of GDPAR; Aspects of Security During the Processing of Personal Data

Yllka RUPA
Department of Civil Law, "Luigj Gurakuqi" Univerisity
Shkoder, Albania

ABSTRACT[1]

Information technology has transformed the economy and social life by influencing the creation of a global order controlled by algorithms. It is the individuals who endanger their privacy precisely by becoming part of the exchanges of personal data for various purposes. Rapid advances in technology and globalization have posed new challenges to personal data protection. But how prepared is the justice system to guarantee the individual for the privacy of the data? GDPAR, and recent developments in the field of personal data security and protection of the individual will be addressed in this article. Among other things, this paper will reflect on a world where the regulatory system of justice is increasingly at stake due to a new order of control, that of digital technology.

Keywords: data privacy and processing, GDPAR, human rights and freedom, data protection

1. INTRODUCTION

Information technology is increasingly seen as a contemporary trend capable of intervening and controlling all walks of life and establishing a global observer order controlled by a certain group of agents. Discussions on the effects of the technological revolution have gone so far as to question the rule of law as the basic instrument for regulating social relations and as the undisputed guarantee of fundamental rights and freedom. Liberal ideas have always placed man at the center of political and social change, for which special importance has been given to human rights and freedom. The assessment of the rights of the person, as an indisputable value of states with liberal tendencies, has made them always in the focus of international and constitutional legal regulations when it comes to special state territories.

Human rights take into account aspects of a person's internal freedom to decide on everything that materializes his or her participation in matters of governance and those of the private spectrum. This is about freedom of expression, organization and participation in organizations of a political, economic and social nature. Moreover, the political rights which engage the individual with his free participation in an electoral process, believe that free will is the truest indicator of the affirmation of a consolidated democracy. When it comes to fundamental rights and individual freedom the first thing that comes to mind are the classic acts of their international regulation.[2] These are the documents that revolutionized the system of human freedom by expanding the regulatory spectrum and also affirming new concepts, which were seen as of fundamental importance not only for the consolidation of the personal status of the individual but also for the affirmation of special categories of rights.

The last century marks an important stage of care to advance in terms of strict regulation in the field of personal rights and freedom. Coping with the latest information technology science that is advancing at an unpredictable pace has brought about the need for a serious focus on so-called *privacy*. This concept will now take on a special significance precisely for the fact of a new trend with threatening tendencies that the intervention of algorithms

[1] I would like to express my deeply felt gratefulness to Professor Thomas Marlowe for his comprehensive and detailed peer-editing of this document

[2] The European Convention on Human Rights, which entered into force on 3 September 1953, is considered to be the most important act for the promotion and protection of human rights. The right to privacy is enshrined in Article 8 of the Convention, which provides for the individual's right to privacy, a right which can be limited only in accordance with law.

can bring.[3] The great challenges of lawmakers are now seen not merely in qualitative adjustments of a defensive nature, but rather in the predictive and preventive abilities of new phenomena which have undertaken to control the world universally and in particular the microcosmos that is found in all of us. Confronting strict legal rules with the galloping developments of information technology and especially artificial intelligence may seem like an abstract confrontation given the completely different methodologies of approach with each of these two categories. Artificial intelligence is the most spectacular product of advancing scientific thought. Being in constant perfection, it has managed to create a centralized observation system, from which even the simplest human activity is difficult to escape. Cyber surveillance tends to enter into important fields of private life, which leads to the individual being discovered in the performance of certain activities that the law considers to be of particular importance mainly in the field of fundamental rights and the application of fundamental freedom.

2. IS THE JUSTICE SYSTEM PREPARED TO FACE THE CHALLENGES OF TECHNOLOGY?

What is more important than the answer to this question has to do with the phrase, regulatory authority. In the hierarchy of regulatory instruments of a global nature, will it again be the human right, the decisive authority, and what constraints will it be able to set so that technological progress, no matter how fast, does not control the spaces which have to do will the feelings of the citizen. Democracy assumes that human feelings reflect a deep and mysterious "free will" and that this "free will" is the fundamental source of authority, although some people are many times more intelligent than others, all human beings are equally free. (Hanari, 46)Tendencies to intervene in the private spaces of the senses/feelings and to control the rationality of thought are likely to change the trajectory of historical legal development which has always promoted the crucial role of law in the context of social discipline.

The technological reality of algorithms, the presence of which goes no further than a click on a web, where the person is looking for something that they need, or the telephone connection with a friend who gives his locality in real time, is likely to turn human rights to a second-hand instrument. Furthermore, we can justify in what balances the procedural aspects of both of these orders already. Informatization of all communication processes, files with the content of citizen data, including those of sensitive[4] character do not require any lengthy procedure as it is enough to know a simple computer program, perhaps the simplest. On the other hand, the procedures of legal regulation, whether normal or accelerated, national or international, related to different areas of human life, or special situations, have remained just as strict and unchanged, which is why most emergencies may not be able to be realized in real time. This unbalanced confrontation is another indicator of the indisputable power and superiority of information technology over the authoritarian rule of law. Is it possible for legal arrangements in the area of personal data and privacy to run at the same pace as those of artificial intelligence? Undoubtedly, the answer must be the product of a profound reform of the material and procedural aspects of law. If the law achieves the ultimate goal of guaranteeing the individual, in the realm of privacy, an effective protection against cyber-attacks, the idea of an unquestionable control of the world by algorithms will seem unrealistic. On the contrary, views on the systematization and protection of the global order, mainly in the field of fundamental rights and freedoms, as the basis of democracy and the integrity of the individual, will be questioned. Such submissions have been of constant concern, and at the beginning of this millennium have been presented as global challenges. These have led to profound regulatory and operational arrangements in the area of fundamental rights in general and personal data in particular. A clear expression is the product brought by the EU Regulation in the field of personal data, mainly in the field of security of processing and data transfer.

3. WHAT GURANTEES WILL THIS WIDE-RANGING INTERNATIONAL ACT PROVIDE TO DATA PROTECTION?

Are these guarantees related to the aspect of recognizing and making public this act and should this aspect be seen as one of the most basic to make as concrete as possible the effectiveness of the protection of personal data? The challenges in confronting law and technology are not limited to GDPR inputs alone, they must be seen in coordination with other complementary platforms that can “refrain” uncontrolled algorithmic intrusions into the privacy plan for the individual.

[3] Algorithm is the basic concept of information technology. This concept was first developed as a mathematical concept. Euclid's algorithm for finding the greatest common divisor of two positive numbers is well known. The evolution of algorithms and their instrumentalization in technology paved the way for computer science.

[4] Law No. 9887, dated 10.03.2008 "On the protection of personal data", Article 3 provides the following definition for sensitive data: - In the category of sensitive data is included any information about the person that has to do with its origin racial or ethnic views, political views, trade union membership, religious or philosophical beliefs, criminal convictions, as well as data on health and sexual life.

4. PROTECTION OF INDIVIDUALS IN CONNECTION WITH THE PROCESSING OF PERSONAL DATA AS A FONDAMENTAL RIGHT

In terms of interpersonal relationships, the processing of personal data and their filing is a process that accompanies every relationship that we as individuals build with other people. From the beginning of the life, we are listed in folders which contain the most sensitive elements of identification of our being. During the subsequent stages, the disclosure of data is an inevitable action that goes along with education, employment contract, business connections, performance of various services, etc. This continuation of the presentation of personal data, as a process aimed at identifying the person in relation to third parties, builds the trajectory of our actions which can easily identify the picture of events that have marked our journey in life. Precisely by considering data privacy as a fundamental right, the protection of the individual has been placed at the center of normative arrangements. Data processing and transfer actions can seriously jeopardize the privacy aspects so much so that the person himself or herself may lose control of the ability to ascertain and intervene personally. Such a possibility has already faded as much as it seems impossible. Rather than a declaration of data (a fact related to the realization of some services, or some goods, in most cases mandatory), this process resembles a submission of them to other entities. It is these entities that process and control the data of the person, which in the function of the activity for which they are created complete the so-called *profiling* of the person.[5] These companies are in a way data possessors and the power of regulatory norms is seen precisely in the perspective of establishing mechanisms for discrete possession and in accordance with the free will of the person himself/herself. How well the person is able to control the progress of the processing and in certain cases of data transfer is not possible to determine accurately, despite the fact that the GDPR provided the standard of control of the person over his/her data.[6]

The importance of legal right as a regulatory instrument is clearly seen even if we refer to the specifics of the processing entities. When it comes to processing entities, we cannot say that all have the same levels of security, able to fully protect the privacy of data. Nevertheless, they have the obligation to enforce safety rules. GDPAR, affirms a level of protection taking into account the state of technology.[7] Thus, their challenge as a data controller and processor is to set up a system that guarantees the level of technology applied in accordance with the standard that achieves the security of data privacy. For all these reasons, the principles and rules of data processing affirmed by Regulation (EU) 2016 \ 679 of the European Parliament and Council have set the standard for a security zone in which personal data navigate. GDPR is already identified with privacy so much so that at all stages of data processing, processing entities represent the standard, rather than the security of its implementation.

The protection of individuals in connection with the processing of personal data is a fundamental right. Within the EU, this perception is enshrined in the Charter of Rights of the European Union[8] (European Convention on Human Rights, Article 8) and in the Treaty on the Functioning of the European Union, which also provides that everyone has the right to the protection of personal data. These two acts can be considered constitutional in the role they later played in creating a complete normative corpus for the protection of personal data. Directive 95/46 / EU of the European Parliament and Council was the most comprehensive normative act aimed at harmonizing the protection of the fundamental rights and freedoms of individuals with regard to the processing of personal data. From 1995, this act would play a regulatory role in the context of personal data processing.

The right to protection of personal data is a fundamental right but not an absolute right. Relying on the principle of relativism of rights and not their absoluteness, legal protection creates a balance between them taking into account the function they have. Personal data as a separate category, are protected in relation to the function they perform in a society. In a society where human relations are dominant and nothing can be completely absolute, it is important to define a sphere in which one can intervene only in cases of special importance. It was GDPAR that emerged as a result of such an activity of exchanging human relations through rapid technological developments. The need for communication through personal data has increased significantly between private and public legal entities. To fulfill their functions and purpose, private companies own and exchange a vast network of personal data in real time, an opportunity which has been made possible through new technological communication opportunities. In these circumstances the GDPR was seen as a strong and coherent framework for data protection in the context of the European Union, and

[5] The President of Microsoft, invited to Albania at the 41st session of the summit on personal data protection, October 23, 2019, stated that the entry into force of the GDPR marked a profound reform to protect privacy in EU countries and beyond. It was the GDPR that influenced the state of California through the referendum, gave their positive opinion on the protection through law, of personal data. Over 82% of citizens voted in favor of the law on personal data protection and today the CCPA (California Consumer Privacy Act) is the strongest normative act in the US for data protection.

[6] GDPAR, has set the standard of personal control over data.

[7] Consolidated Version of the Treaties of the European Union and the Charter of Fundamental Rights of the European Union, published by the Ministry of European Integration, Tirana 2010.

a robust execution platform on the other hand. At its core, this act seeks to build trust in the person himself/herself in relation to his legal guarantees in the context of privacy, but on the other hand, it also builds confidence that the new global order controlled by information technology will be able to strengthen technical capacity to guarantee data privacy.

4.1 To what extent is the right of personal data protection able to change our perception of data security?

The question that arises must be seen from the point of view of the purpose of the legislative initiative itself. The need to intervene in the realm of data privacy was also seen as a barrier to the creative imagination of algorithms. (Fuga, 594) The impression that nothing can escape the control of artificial intelligence, except the negative impact on the perception of personal security, created a lack of credibility in the field of economic and commercial communication. Large trading companies, which are also the largest processors and exchangers of personal data, are facing new challenges in terms of security they offer to their partners, mainly related to data security, regardless of the importance it has for the person. Currently on the basis of systems created by artificial intelligence, robots have been created, which are not only programmed to find *big data* on the Web, but also to classify this data, put it in a certain order, while interpreting them to some extent.[9]

Despite the importance it attaches to the individual, GDPAR has a special significance for other public and private actors who are already establishing some credibility in their relations, seeing the executive power of GDPAR as the optimal solution to data protection. If during a common click we make for an equally common reason, the algorithm immediately presents us with the phrase protection by GDPR. This immediately increases our credibility on the page where we clicked. However, we can be completely indifferent, especially when in real time we are presented with dozens of such. The possibility of the individual himself controlling the data that he has presented to third parties, is an obligation that GDPAR imposes on the controlling companies. This visual presentation is valid for the business entity and the individual at the same time. The credibility relationship that is created in this case should not put us in a completely uncontrolled security situation, due to the fact that at this moment we have submitted our data and if the trust platform GDPR ensures us data, it is inevitable to "disturb" our privacy every time we surf the internet. We have noticed that companies that market their products through computer and social networks have their target group, and it is precisely the people who can click at a certain moment to get a simple information. Convinced and perhaps even "manipulated" by the secure GDPAR algorithm, this target suffers from the daily concerns of the operators who manage the advertising aspects of various companies, which act for the profiling of individuals based on their clicks in their web.

The question that arises is related to the possibility that individuals have to present their objection in such cases and what may be the sanctions against concrete abuses. So is consent enough to be concretized with just one click, and it is possible to clearly define the object of consent given with just one click. If we look at the relationship of interest between the data management company and the person him/herself, we are in a state of imbalance, which makes us think of a clear abuse or misuse of data. We can say that although GDPAR is considered an act that guarantees a uniform level of protection of personal data for individuals in all countries of the Union, we cannot say that its executive level is or can be as progressive as the advancement of technology. Individuals are free to present personal data when they have received the necessary guarantees and have been acquainted with them before, but security platforms are more burdensome as obligations of processing entities. How powerful these entities are in assuming executive responsibilities related to data protection is impossible for individuals to fully disclose.

5. GDPAR INNOVATIONS RELATED TO SECURITY CONDITIONS

The security elements during data processing are directly related to the storage standard and the level of guaranteeing the security of the person. Processing structures link the trust they need to build to third parties precisely with the level that processing guarantees. Individuals are also interested in knowing what are the levels accepted by data processing entities regarding the execution of security standards. GDPAR has advanced on the legal regulation of this criterion, affirming rules that can compete with current safety standards. Companies that process personal data were thus placed before the strict legal requirements that compel them to raise security standards. In line with GDPAR requirements, processing actors undertake their actions to invest in information technology and mainly to adopt servers that store data and increase confidence in a transparent activity.[10] Companies now face the great challenge of putting artificial intelligence in such a situation where the individual's

[9] GDPAR aims to protect individuals in relation to the processing of personal data and considers data privacy as a fundamental right.

[10] The President of Microsoft, stated at the Conference of Data Protection and privacy Commissioners 2019, Tirana Albania, that new technologies must be accompanied by new laws, as the world will enter 2020 with 25 times more digital data than we have had in 2010, and this is just the beginning of the decade

access to knowledge of all data processing activity is a legal obligation.

The security conditions imposed by the GDPAR oblige the processing entities to establish such a relationship with the individual where the latter is the determining contractor for the initiation of the processing process. Obtaining consent is a legal condition and relates to the obligation that the processing entity must implement before starting the process. Continuing with the idea of preventing the serious risk of data misuse, GDPAR sets the standard for their automatic processing, and the inclusion of programs that enable basic security concepts to be classified as new GDPAR feeds. The regulation bases the security technique on some important elements that form the core of data privacy. Pseudonymization, anonymity, confidentiality, etc., are strict procedures that accompany the processing of personal data. Implementing pseudonymization for personal data can reduce the risk of data damage or control of interested entities. Controlling and processing entities now have the obligation to pseudonymize the data, thus fulfilling their legal obligation. The regulation explicitly mentions the anonymization of personal data as a basic criterion for privacy. The anonymization of data has to do with their destination only in function of the purpose for which they were processed and access to them only by authorized individuals. Perhaps seemingly very simple, the data anonymization procedure puts the controlling and the processing entity in front of a new challenge that has to do with setting up such a technical network that does not allow anyone to interfere in the files where the individual saves his/her data, otherwise the network itself finds traces of interference.

Anonymity preservation techniques also presuppose a quick response in cases where someone interferes outside of their competencies and abusively in data storage systems. The European Court of Human Rights argues that data processing and retention institutions should have adopted such techniques that leave traces and detect any unauthorized interference.[11] Anonymization allows the general analysis of data of individuals by specific entities who carry out the process by swearing to maintain confidentiality. The technical and organizational measures necessary to anonymize the data as well as the authorized individuals must be indicated by the controlling entity. Processing entities undertake the presentation of data processing techniques in accordance with the security rules set out in the GDPAR. These are entities that contract with data controllers and present their superiority in terms of the technology they possess and the belief in a high standard of data processing. In most cases, the controllers and data processors are different entities that contract to carry out the processing in compliance with the legal requirements of GDPAR. The obligation to enforce security also rests with those public authorities to whom personal data are disclosed in fulfillment of a legal obligation to carry out their official mission. As such we can mention taxation and social security authorities, customs and public entities, courts and universities, independent administration authorities, financial market authorities. The processing of data by these authorities presents special specifics which require professional legal interpretation. Often the disclosure of data to these authorities is linked to the receiving of a direct public service to the citizen, which calls into question the freedom to give consent.

In the sense that this consent is conditioned on the receiving of a product, the individual is put in the position of dilemma and necessarily accepts the condition of disclosure of data. The ideal execution of the conditions of legality provided by GDPAR, is difficult to achieve in its absolute, in the case of the activities of the above-mentioned authorities. However, the relative character already accepted for the privacy of the data, it legalizes the public activity of these entities. This aspect does not question the legal processing of the data. There are countries that have not yet reached the stage of such a development of working conditions and safety techniques to effectively implement GDPAR safety standards, otherwise there would not be so many court rulings declaring violations of the data during their processing. Given that in most cases (even the regulation extends to the aspects of automatic data processing) data processing is carried out through automatic technologies as well as automatic decision-making regarding the processing or profiling of data with the standard that they have adopted. This allows the aforementioned authorities to contract with reliable processors (accepting co-operation costs) that set high safety standards for the processing activity. Safety standards are linked to the provisions of Article 32 of the GDPAR.

On May 25, 2018, let us not forget that we had a historic moment in the protection of privacy and this is the day when the GDPAR enters into force. The new regulations have been described as a second wave (after the order established by the directive) of regulating data privacy issues. In terms of privacy, new stages are being marked which will later serve as the legal basis of all initiatives to cope with the management of the increased flow of data exchange. Data processing companies are faced with new responsibilities related to technology upgrades and appropriate technical and organizational measures. The ultimate goal is to provide a level of security appropriate to the risk. To what extent does data processing aggravate the rights and freedoms of persons and what are the measures to ensure that the trajectory of the data control process is guaranteed? Indeed the four elements of security processing are related to the ability of systems to implement the data control process automatically. Data automation and encryption, the ability to ensure confidentiality and integrity, the availability and stability of processing systems and services, are innovations that

[11] Court verdict

GDPAR has brought in terms of security. Individuals will now have access and control over data processing procedures. But how much is possible to factualize the security aspects, if we take into account the speed of data circulation, the lack of barriers to their transfer from one company to another regardless of their location? It will be the technological challenges that will have the final say on the principles of security and the concretization of the GDPAR standard.

Recent debates at data privacy summits emphasize the coordination of the field of law with that of technology, competition and e-commerce. It is about telecommunications jurisprudence where privacy data occupies an important place. Thus, the sphere of privacy despite the special normative autonomy will be perfected only because of common and harmonized rules that discipline the common aspects of the meeting between them. Article 32 itself explicitly discusses the state of the technique, implementation costs and nature, as determining conditions for the implementation of security measures. (Regulation (EU) 2016/679) It is the tech giants who have rushed to implement security measures in their information technologies. Many of them have offered new technology standards similar to the new legal regulations. If we look at the amazing developments in information technology, we must also anticipate the possibilities of equally rapid developments in legislation. We need to understand that GDPAR has a certain territorial scope in the context of the European Union, and despite the fact that this regulation serves as an indisputable standard to refer to, a global normative pact is needed to universally establish the security for data privacy. Perhaps artificial intelligence futurist companies will be able to spread their influence throughout the world in which they operate. By anticipating the growing need for data protection as a result of their increasing influx in the world of automated technology, and forced by legal criteria, these companies will establish a special security order that if it does not stay at a level higher than that legal, it is likely to surpass it.

6. CONCLUSIONS

Data processing is linked to important interests that determine the activity of public, private, commercial and business authorities. It is precisely the results of the elaboration that play a decisive role in the innovative solutions of issues of global importance belonging to various fields of science. That alone is enough to understand that global activity in the field of personal data control is unstoppable.

Moreover, there is no doubt that the process of control over data, and thus over the human community, risks seriously undermining security standards for fundamental rights and freedom.

GDPAR has already gained the authority of the normative act responsible for the protection of the individual during the processing of personal data. This act has increased the guarantee and trust of individuals in relations with data control entities. By crossing EU borders, GDPAR has extended its influence to other continents, thus providing a good premise for the creation of a global pact to protect data privacy.

Furthermore, data privacy is at a critical juncture given the ever-increasing flow of data. In this view, the function of law, except in terms of current normative regulation, must be extended to its ability to anticipate and resolve situations that may be the product of new technological developments.

Lastly, harmonization and coordination of privacy norms related to the processing of personal data is a necessity in the conditions of their fast and barrier-free circulation. Thus, a reformulation of normative acts at national and international levels is necessary to build a global coordinating order that ensures the privacy of the individuals. The greater the importance of data processing, the greater the risk of their aggravation. It is the duty of law to set the boundaries of data management for all entities that control and process them.

7. REFERENCES

Baraku, Irma, The Right to Information, Tirana, 2020

Consolidated Version of the Treaties of the European Union and the Charter of Fundamental Rights of the European Union, published by the Ministry of European Integration

Directive 95/45 / EU of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data.

European Convention on Human Rights

Fuga, Artan, Mediamorphose and Metacommunication, Tirana: Papyrus, 2017

Harari, Y.N, Lectures for the 21st Century, Tirana, 2019

Law No.9887, dated 10.03.2008 "On the protection of personal data"

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data"

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of the individual with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data.

Treaty on the Functioning of the European Union

Zaganjori, Xh, Inter Gentes, International Protection of Human Rights, Tirana, 2021