Challenges, obstacles and measures regarding achieving and ensuring personality protection in the digitalization era in public administration

Gabriela MANEA

ABSTRACT
In the era of digitization of public administration, an extremely important problem that it faces is the protection of personality, because in this process a large part of citizens' personal data is stored and processed electronically. In this sense, it is essential that public authorities ensure by taking effective measures to protect personal data, but also to respect the right to privacy of citizens. The digitization of public administration comes with an open list of advantages, but also obstacles and challenges, for individuals (citizens), for legal entities, for the private environment, for the business environment, but also for society as a whole. The purpose of this article is to make known the challenges and obstacles that the public administration faces in the digitization process on the one hand, and on the other hand, what measures must be implemented in order to respect and ensure the protection of the personality. Achieving and ensuring the protection of the personality by the public administration in the digital era is essential, both for maintaining the citizen's degree of trust in the state authorities, and for respecting their fundamental rights. In order to achieve and guarantee the protection of the personality, the public administration must ensure that the civil servants who work with the personal data of citizens are adequately trained in data protection, as well as with knowledge and compliance with the legislation in force in the field.

KEYWORDS: *Public administration, digitization, privacy protection, personal data.*

1. Introduction

In the age of digitization, digital technologies present enormous potential for Europe and the member countries of the European Union. To this end the European Commission is committed to "creating a Europe ready for the digital age, ensuring that citizens, businesses and administrations have and use new generations of technologies, a Europe where the digital transformation will benefit everyone."[1] In this sense, the European Commission helps member states to carry out reforms to capitalize on the potential of digital growth, but also to implement innovative solutions for citizens and businesses, as well as to improve the accessibility and efficiency of public services.)

In Romania, the public administration is maximally challenged by the introduction of the latest generation technologies, in order to develop and implement e-government services, for the

[1] Strategies and policies, Digital transition accessed https://reform-support.ec.europa.eu/what-we-do/digital-transition_ro, on 22.07.2024.

improvement and efficiency of the way of interaction of the citizen (natural person) and the legal person with the public administration. The digital transformation of public administration is the way in which the services offered are faster, cheaper and of a clearly superior quality. The quality of the services provided by the public administration is implicitly related to the respect of human rights in the era of digitization and "man's emancipation to know his rights".[2]

E-government leads to improved efficiency but also to increased accessibility and use of services and processed information. It also contributes to the promotion of ethically compliant practices, identifies and reduces risks regarding the phenomenon of corruption. E-governance presents a challenge to administration worldwide as it has encountered some barriers in the implementation of e-government systems such as: Digital Divide, Management Failures and Organizational Inflexibility.[3] For better governance, it is necessary for the public administration to be digitized, to benefit from an adequate administration framework, with an updated regulation, implemented coherently, unitarily and correctly, with a well-defined infrastructure, using information and communication technology, as artificial intelligence would also be newer.

Digitization aims to process information and data, but also analog processes in a digital format, using technology. This brings benefits to the public administration, which have proven to be vital, and here we mention the conversion of documents, data from them and processes into digital format, with the help of which the administration stores and processes the information received from the citizen much more easily, with the help of networks of communications made for this purpose, as well as of computers. In order to respect and protect the privacy rights of citizens, the public administration must respect and correctly implement the norms of European and national legislation regarding the processing of personal data.

In Romanian law, there is no dedicated space for defining the notion of "personality rights"[4]. In a general way there are concerns for the regulation of certain personality rights, such as the right to image, the right to life and the right to integrity. The approach to personality rights in the era of digitization is difficult controversial and under the sign of uncertainty, regarding their identification, correct definition, as well as their scope. The legislator has so far failed to identify the context and regulate the unitary legal framework regarding personality rights, as it is incomplete and lacks the effect of harmonization.

Personality rights are defined "in general, those rights inherent in the quality of human person that belong to any individual by the very fact of being human"[5].The natural person is represented by man, considered individually, as the holder of civil rights and obligations. In the context given by the relations established between the citizen and the public administration, the right to information has a complex content.[6] The era of digitization translates into the rapid trading

[2]I. Zlătescu Moroianu, Human rights – a system of evolution, revised 2nd edition, IRDO Publishing House, Bucharest, 2008, pp. 10 et seq.
[3] Cătălin Vrabie, Bucharest, Romania: Pro Universitaria Publishing House, 2016.
[4] O. Ungureanu, C. Munteanu, Observations regarding the natural person and the legal personality "Romanian Pandectiles", no. 4, 2005, p. 180-190.
[5] B. Selejan-Guțan, L.-M. Crăciunean, Public International Law, Bucharest, Edit. Hamangiu, 2008, p. 99.
[6] P. Kayser, Diffamation et atteinte au droit au respect de la vie privée, „Mélanges Jauffret",Presses Universitaires d'Aix-Marseille, 1974, p. 411 (citat după X. Agostinelli, op. cit., p. 78).

and use of information in the interest of the citizen, but also of the public authorities, but without infringing the rights of personality.

The European Court of Human Rights ruled in relation to the provisions of art. 10 on freedom of expression through a series of decisions with reference to the explanation of the phrase matters of public interest. Thus, the following can be categorized as issues of public interest: the functioning of the judicial administration (in situations where it is appropriate)[7] or the independence of trade union organizations, the illicit character that the wealth acquired by a politician can have [8],, because "A public person, with important positions, must support the publication of photos that represent him"[9]. In order to protect the rights of the personality both at the international level, as well as at the European and national level, the norms and regulations in the field are implemented and put into practice through institutions with competences in this regard.

2. The representative institutions regarding data protection at international and European level

At the international and European level, the following representative institutions with competence regarding the protection of personal data operate: a) United Nations Educational, Scientific and Cultural Organization (UNESCO)[10]- promotes freedom of expression, protection of privacy and combating discretion on the Internet; b) Council of Europe[11] - promotes respect for human rights and data protection at European level.; c) European Commission for Data Protection (ECPD)[12] – the independent body of the E.U. what are to monitor and the application of the

[7] The Constantinescu v. Romania case, in C. -L. Popescu, op. cit., p. 21, accessed at https://legeaz.net/hotarari-cedo/constantinescu-contra-romaniei-33v, on 09.08.2024.

[8]The case of Krone Verlag GmbH & Co. KG v. Austria, in C. -L. Popescu, op. cit., p. 68, accessed at https://legeaz.net/hotarari-cedo/krone-verlag-gmbh-nqy, on 09.08.2024.

[9]Krone Verlag GmbH & Co. KG v. Austria - Freedom of the press. Information of public interest. Politician. accessed at https://legeaz.net/hotarari-cedo/krone-verlag-gmbh-nqy, on 08/09/2024.

[10] The United Nations Educational, Scientific and Cultural Organization (UNESCO) is a specialized agency of the United Nations (UN) that aims to promote world peace and security through international cooperation in education, science and culture. It has 193 member states and 11 associate members, as well as partners from the non-governmental, intergovernmental and private sectors. Based in Paris, France, UNESCO has 53 regional offices and 199 national commissions that facilitate its global mandate, information accessed at https://ro.wikipedia.org/wiki/Organiza%C8%9Bia_Na%C8%9Biunilor_Unite_pentru_Educa%C8%9Bie,_%C8%98tiin%C8%9B%C4%83_%C8%99i_Cultur%C4%83, on 09.08.2024.

[11]The European Council brings together EU leaders to set the Union's political priorities and is the highest level of political cooperation between EU countries. The European Council is one of the 7 official institutions of the Union. It exercises its activity within the (usually quarterly) summits of EU leaders, chaired by a permanent president, accessed at https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search -all-eu-institutions-and-bodies/european-council_ro, on 09.08.2024.

[12]European Commission for Data Protection (ECPD) – is the institution responsible for ensuring that the General Data Protection Regulation (GDPR) and the Data Protection Directive in matters of law enforcement are applied consistently in EU countries, as well as in Norway , Liechtenstein and Iceland, accessed at https://european-

legislation on the protection of responsibility at the European level;; d) United States National Association for Data Protection (NADP)[13] –non-governmental organization promoting data protection principles in the United States; e) World Economic Forum [14] – promotes dialogue between governments, companies and civil society to develop a global framework for the protection of personal data in the digital age; f) The National Supervisory Authority for Personal Data Processing (ANSPDCP)[15]– the supervisory authority for the protection of personal data in Romania.. All these institutions play a particularly important role in the era of digitization, in terms of protecting individual rights and in terms of promoting the values of a responsible and fair digital society.

3. The representative institutions regarding data protection in the era of digitization in Romania

At the national level, the representative institutions with powers and responsibilities regarding the protection of personality rights by protecting the processing of personal data are the following: a) National Supervisory Authority for the Processing of Personal Data (ANSPDCP)[16] - this is the regulatory authority in the field of data protection, having the role of ensuring compliance with the legislation in the field and protecting the rights of natural persons with regard to the processing of their personal data. In addition to the ANSPDCP, there are other institutions and organizations that may have roles in data protection, depending on the sector of activity:; b)

union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board -edpb_ro, on 09.0.2024.

[13] National Association for Data Protection of the United States (NADP) - Privacy Shield EU-US (Privacy Shield EU-US), "In August 2016, the Implementing Decision (EU) was published in the Official Journal of the European Union 2016/1250 of the Commission of 12 July 2016 under Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection offered by the EU-US Privacy Shield. According to this decision, the United States guarantees an adequate level of protection of personal data transferred from the European Union to organizations in the United States under the EU-US Privacy Shield, provided that those entities process the personal data in accordance with a strong set of principles and guarantees for the protection of privacy and personal data that are equivalent to those in the European Union." accessed at https://www.dataprotection.ro/?page=Scutul_de_confidentialitate_UE-SUA&lang=ro, on 09.08.2024.

[14] The World Economic Forum is the International Organization for Public-Private Cooperation. It provides a global, impartial and non-profit platform for meaningful connection between stakeholders to establish trust and build initiatives for cooperation and progress, accessed at https://www.weforum.org/about/world-economic-forum /, on 09.08.2024.

[15] The National Supervisory Authority for the Processing of Personal Data, as an autonomous central public authority with general competence in the field of personal data protection, represents the guarantor of respect for the fundamental rights to private life and the protection of personal data, established especially by art. 7 and 8 of the Charter of Fundamental Rights of the European Union, art. 16 of the Treaty on the Functioning of the European Union and of art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, information accessed on 08/09/2024.

[16] *Ibid.*

Ministry of Transport and Infrastructure [17] - which deals with data processing in transports; c) Ministry of Internal Affairs[18] - responsible for aspects related to security and data protection in the field of public order; d) The Court of Appeal and the courts - which can review appeals related to ANSPDCP decisions or other disputes related to data protection; e) The Commission for the Defense of Human Rights, Cults and the Problems of National Minorities - within the Romanian Parliament, which can discuss legislation in the field of data protection; f) Non-governmental organizations - which promote human rights and can take measures in favor of data protection. These authorities and organizations collaborate to ensure the respect of the right to private life, the rights of personality through the protection of personal data in institutions and local public administrations and the central administration in Romania.

4. The regulations regarding the respect of personality rights by protecting the processing of personal data

4.1. Legislation on the protection of personal data processing at European level

The protection of personal data and respect for life are fundamental European rights. According to research carried out at the level of the European Parliament [19] EU legislation with reference to the regulation of data flows makes an annual contribution to the GDP of the European Union [20] of EUR 51.6 billion. From the results of research prepared for the European Parliament's Committee of Inquiry to investigate the use of Pegasus[21] and surveillance spy programs, equivalent

[17] The Ministry of Transport and Infrastructure (MTI) is the specialized body of the central public administration that establishes the policy in the field of transport at national level, elaborates the strategy and specific regulations for the development and harmonization of transport activities. https://www.bing.com/search?q=b)%20Ministerul%20Transportilur%20%C8%99i%20Infrastructurii&pc=0P472&ptag=C999N9998D031521A00ED787AAB&form=PCF463&conlogo=CT3210127, on 09.08.2024.

[18]The Ministry of Internal Affairs is a specialized body of the central public administration that establishes measures for the defense of fundamental human rights and freedoms, as well as public and private property, accessed at https://diaspora.gov.ro/mai, on 09.08. 2024.

[19] The European Parliament is an important forum for political debate and decision-making at EU level. Members of the European Parliament are directly elected by voters in all member states to represent the interests of citizens in the legislative process of the European Union and to ensure that the other EU institutions operate democratically. The Parliament exercises the role of co-legislator, having, together with the Council, the power to adopt and amend legislative proposals and to adopt the Union budget. He also supervises the work of the Commission and the other European bodies and cooperates with the national parliaments of the EU countries, which also contribute. Find out how the whole system works, accessed at https://www.europarl.europa.eu/about-parliament/ro, on 01.08.2024.

[20]The GDP of the European Union - The European Union is the first world economic power that combines the economies of the 27 member states, having a gross domestic product (GDP) of 16,748 billion dollars, in nominal parity.. Twenty member states have adopted a common currency, Euro, regulated by the European Central Bank. The EU economy represents a single market and the EU is represented as a single entity within the WTO (World Trade Organization), accessed at https://ro.wikipedia.org/wiki/Economia_Uniunii_Europene, on 12.08.2024.

[21] Pegasus and surveillance spyware, IN-DEPTH ANALYSIS for the PEGASUS committee, European Parliamnet, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf, as of 10.08.2024.

to the PEGA Commission[22], come to confirm the importance of data processing for the defense of individual freedoms and for the defense of democracy in the EU. As a result, the EU has the obligation to ensure the consistent application of the fundamental right to data protection, a right enshrined in the Charter of Fundamental Rights[23] of the EU.

At the European level, the main regulation regarding the protection of personal data is represented by the General Data Protection Regulation (GDPR)[24], adopted in 2016 and applicable from 2018, which establishes the strict rules regarding the processing of personal data for all member states of the European Union. GDPR. gives people extended rights regarding the processing of personal data, such as: the right to access data, the right to rectify or delete inaccurate or inappropriate data, the right to data portability, the right to restrict data processing, and the right to oppose data processing.

In addition to the GDPR, there are other laws and directives that protect the right to privacy and data protection at the European level, such as the e-Privacy Directive[25] and the Council of Europe Convention for the Protection of Individuals with regard to Automated Processing of Personal Data[26].

The provisions of art. 8 of the European Convention of Human Rights and Fundamental Freedoms of November 4, 1950, (ECHR), establishes the right to respect for private and family life, home and correspondence of all persons.

[22] PEGA – Committee of the European Parliament to investigate the use of Pegasus surveillance spyware, Committee to investigate the use of Pegasus surveillance spyware, Multimedia CentreEuropean Parliament, accessed at https://multimedia.europarl.europa.eu/en/topic/pega-committee-to-investigate-use-of-pegasus-surveillance-spyware_22903, on 10.08.2024.

[23] Charter of Fundamental Rights of the European Union (2010/C 83/02), 30.3.2010 Official Journal of the European Union C 83/389.

[24] GDPR - General Data Protection Regulation (GDPR) - regulation (EU) of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing the Directive 95/46/CE (General Data Protection Regulation), applicable in 2018, accessed at https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html, on 09.08.2024.

[25] e-Privancy Directorate - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of confidentiality in the public communications sector (Directive on privacy and electronic communications), in force, amended, current consolidated version 19 /12/2009, accessed at http://data.europa.eu/eli/dir/2002/58/oj, on 09.08.2024.

[26] Convention 108 of January 28, 1981 of the Council of Europe for the protection of individuals with regard to automated processing of personal data was the first international instrument with binding legal force adopted in the field of data protection. Its purpose is to guarantee to all natural persons the respect of their fundamental rights and freedoms, and in particular the right to private life, in relation to the automated processing of personal data, accessed at https://www.europarl.europa. eu/factsheets/ro/sheet/157/protectia-datalar-cu-caracter personal#:~:text=Conven%C8%9Bia%C8%9Bia%C8%9Bia%C8%9Bia%C8%9Bia%2028%20januarie%201981%20a%20Consiliului%C4%83%20legal%C4%83%20mandatory%20adopted%20%C3%AIn%20the%20area%20protect%C8%9Biei%20data., on 09.08.2024.

The Universal Declaration of Human Rights[27], by the provisions of art. 12 regulates the right to the protection of the law against arbitrary interferences in his personal life, in his family, in his domicile or in his correspondence, his honor and reputation cannot be affected.

By the provisions of art. 7 and art. 8 of the Charter of Fundamental Rights of the European[28] Union, the rights regarding respect for private life and the protection of personal data are recognized, which are closely related but separate fundamental rights.

Data Protection Directive in the field of law enforcement[29] protects the fundamental right of citizens for data protection in all situations where public authorities, in law enforcement, use personal data. The Directive also guarantees that the personal data of victims, witnesses and suspects is properly protected and facilitates cross-border cooperation in the fight against crime and terrorism.

Directive on privacy and electronic communications[30] comes to regulate the conditions of data retention and which states that EU law opposes the general and undifferentiated retention of transfer and location data. This Directive has been repeatedly brought before the Court of Justice of the EU (CJEU), which has materialized in a series of decisions, the most recent case being in 2020[31].

In addition to the main legislative acts on the protection of personal data, specific provisions are also established by sectoral legislative acts, such as:

a) The provisions of art. 13 (relating to the protection of personal data) of Directive (EU) 2016/681 of the European Parliament and of the Council of April 27, 2016 regarding

[27] Art. 12 of the Universal Declaration of Human Rights of December 10, 1948, issued by the United Nations, published in the Brochure of December 10, 1948, accessed at https://legislatie.just.ro/Public/DetaliiDocumentAfis/22751, on 09.08. 2024.

[28] Charter of Fundamental Rights of the European Union (2010/C 83/02), 30.3.2010 Official Journal of the European Union C 83/389, accessed at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= OJ:C:2010:083:0389:0403:ro:PDF, on 16.08.2024.

[29]Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating or prosecuting crimes or executing penalties and regarding the free movement of this data and repealing Council Framework Decision 2008/977/JHA became applicable in May 2018, accessed at https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/ ro/FTU_4.2.8.pdf, on 09.08.2024.

[30] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of confidentiality in the public communications sector (Directive on privacy and electronic communications) was amended by Directive 2009/136/EC of 25 November 2009, accessed at https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX:32002L0058, http://data.europa.eu/eli/dir/2002/58/oj, http ://data.europa.eu/eli/dir/2009/136/oj, on 09.08.2024.

[31] Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others, Court of Justice of the European Union PRESS RELEASE No 123/20 Luxembourg, 6 October 2020, accessed at https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf#:~:text=By%20two%20Grand%20Chamber%20judgments,processing%20operations%2C%20such%20as%20its, on 09.08.2024.

the use of data from the passenger name register (PNR) for the prevention, detection, investigation and prosecution of terrorist offenses and serious crimes.

b) The provisions of art. 6 (on data processing) of Council Directive 2004/82/EC of 29 April 2004 on the obligation of transport operators to communicate passenger data (API), repealed by 2 Regulations[32]-[33] which were voted on April 24, 2024 in the plenary session of the Parliament.

c) Provisions relating to data protection guarantees, provided for in Chapter IV of Regulation (EU) 2016/794[34] of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol).

d) The provisions of Regulation (EU) 2017/1939[35]of the Council of 12 October 2017 from Chapter VIII, regarding the implementation of a form of consolidated cooperation regarding the establishment of the European Public Prosecutor's Office (EPPO).

4.2. Legislation regarding the observance of the right of personality through the processing of personal data at the national level

National privacy legislation may vary from country to country, but generally includes provisions on the protection of personal data, the right to image and privacy, protection against harassment and discrimination, as well as rules on the confidentiality of personal information. In Romania, the laws that regulate the protection of personality rights through the processing of personal data are:

a) Law no. 677/2001[36] regarding the protection of individuals regarding the processing of personal data and the free movement of such data;

b) The Civil Code[37], which regulates the right to privacy and image;

[32] Regulation 2022/0424(COD) on the collection and transfer of prior passenger information in order to improve and facilitate controls at external borders, accessed at https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0424(COD)&l=en, on 10.08.2024.

[33] Regulation 2022/0425(COD) on the collection and transfer of prior passenger information for the purposes of the prevention, detection, investigation and prosecution of terrorist offenses and serious crimes, accessed at https://oeil.secure.europarl.europa. eu/oeil/popups/ficheprocedure.do?reference=2022/0425(COD)&l=en, on 10.08.2024.

[34]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 and repealing Directive 95/46/EC (General Regulation on data protection), 4.5.2016 RO Official Journal of the European Union L 119/1, accessed at https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679, on 10.08.2024.

[35] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing a form of consolidated cooperation with regard to the establishment of the European Public Prosecutor's Office (EPPO), in force, amended, consolidated form on 10/01/2021, accessed at http://data.europa.eu/eli/reg/2017/1939/oj, on 10.08.2024.

[36] Law no. 677 of November 21, 2001 for the protection of individuals regarding the processing of personal data and the free movement of such data, published in M. Of. no. 790 of December 12, 2001, accessed at https://legislatie.just.ro/Public/DetaliiDocument/32733, on August 12, 2024.

[37] Noul Cod Civil (Legea nr. 287/2009, publicată în M. Of. nr. 55 din 15 iulie 2011), republicat, actualizat la zi și consolidat, accesat la https://legeaz.net/noul-cod-civil/, la data de 12.08.2024.

c) The Criminal Code[38], which protects people against harassment, crimes against privacy and other attacks on the person;

d) Law no. 190/18.07.2018[39] regarding the activity of monitoring employees. According to the provisions of article 5 of this law, employers are allowed to video monitor their employees or monitor their conversations, but only under certain conditions, as indicated by the normative act: "in order to achieve the legitimate interests pursued by the employer, it is allowed only if: a) the legitimate interests pursued by the employer are thoroughly justified and prevail over the interests or rights and freedoms of the persons concerned; b) the employer provided the mandatory, complete and explicit prior information to the employees; c) the employer consulted the union or, as the case may be, the representatives of the employees before the introduction of the monitoring systems; d) other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proven their effectiveness; and e) the duration of storage of personal data is proportional to the purpose of the processing, but no longer than 30 days, except for situations expressly regulated by law or thoroughly justified cases".[40]

Also, in the European Union, the General Data Protection Regulation (GDPR)[41], which entered into force in 2018, and which regulates in detail the protection of personal data of European citizens. This regulation applies to all member states, including Romania, and imposes strict rules on the processing and protection of personal data.

This Regulation (RGPD) comes "to protect natural persons when their data is processed by the private sector and most of the public sector, allows natural persons to have better control over their personal data, modernizes and unifies the rules, establishes a system of fully independent supervisory authorities"[42] Also, the provisions (RGPD) come to strengthen the existing rights of natural persons, provide new rights and grant natural persons increased control over their personal data. These provisions include: a) easier access to a physical entity's own data by providing information on how data is processed and ensuring the availability of information, in an intelligible and clear form; b) a new right to data portability, thus facilitating the transmission of personal data from the service provider to another provider; c) a clearer right to erasure (the right to be forgotten

[38] The new updated Penal Code 2024 – (Law no. 286/2009, published in M. Of. no. 510 of July 24, 2009), updated and consolidated, accessed at https://legeaz.net/noul-cod-penal/, on 12.08.2024.

[39] LAW no. 190 of July 18, 2018 on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/CE (General Data Protection Regulation), Published in M. Of. no. 651 of July 26, 2018, accessed at https://legislatie.just.ro/Public/DetaliiDocument/203151, on August 10, 2024.

[40] Art. 5 of Law no. 190 of July 18, 2018, published in M. Of. no. 651 of July 26, 2018, which will be revised according to the European Commission's Report on the evaluation and revision of the regulation from June 2020, with its new evaluation scheduled for 2024.

[41]Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the institutions, bodies, offices and agencies of the Union and on the free movement of such data and repealing of Regulation (EC) no. 45/2001 and Decision no. 1247/2002/CE, 21.11.2018, RO, Official Journal of the European Union L 295/39, in force, accessed at https://eur-lex.europa.eu/eli/reg/2018/1725/oj, http ://data.europa.eu/eli/reg/2018/1725/oj, on 10.08.2024.

[42] https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html, on 11.08.2024.

on the Internet)[43] and d) the right to know when their personal data has been breached, according to which companies and organizations must notify the competent data protection supervisory authority and, in cases of serious data breaches, also individuals.[44]

According to the provisions of the GDPR, the public administration has a series of obligations regarding the collection, processing and storage of personal data, obligations that must be carried out according to the provisions of the principles of respect for the right of personality in the public administration, respecting the conditions for processing personal data.

5. Respecting the right to privacy by respecting the principles regarding the processing of personal data in the public administration

When a public administration processes personal data relating to a natural person, it is subject to GDPR rules. The processing of personal data by public administrations is carried out "on the basis of a legal obligation or to the extent that this is necessary for the fulfillment of some public interest attributions or in the exercise of the public authority with which it is vested.".[45]

[43] See Judgment of the Court (Grand Chamber) of 13 May 2014 – Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, " It argued that the proceedings had been settled for several years and that reference to them had become irrelevant.
The Court found that an operator of an Internet search engine is responsible for the processing of personal data appearing on web pages published by other sources and must comply with legislation protecting natural persons in this regard (Directive 95/46/EC).
The Court ruled that the search engine operator could, in certain circumstances, be required to remove links to certain web pages from the list of results that appear when a search is made for a particular name (this right is known as the right to be forgotten or the right to "de-indexing"), if the information is considered inaccurate, inadequate, irrelevant, no longer relevant or excessive for the purpose of data processing, but not only because it is inconvenient for the data subject. Google LLC v Commission nationale de l'informatique et des libertés (CNIL) (2019). In the action brought by Google against the French data protection authority, the CJEU was called upon to rule on the geographical scope of the right to be forgotten. In 2016, the French regulator fined Google €100,000 for refusing to enforce the right to be forgotten worldwide. It also required the company to apply the right to be forgotten to all Google domain names, including google.com. In response, Google argued that the French data protection authority only had the power to order that it apply to the French domain google.fr.
In its ruling, the Court ruled that the right to be forgotten does not apply to links displayed on all versions of a search engine worldwide, but applies to search engines with domain names associated with EU member states, i.e. not just google .fr, but also google.it, google.de, google.nl, etc. Search engine operators are also required to apply, if necessary, measures that "effectively prevent or at least seriously discourage" internet users from accessing de-indexed material when searching by name in - a member state.", accessed at https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A62012CJ0131, on 11.08.2024 and "The right to be forgotten (GDPR.eu).

[44] Summary on and d) the right to know when their personal data has been breached, according to which companies and organizations must notify the competent data protection supervisory authority and, in cases of serious data breaches, individuals too, accessed at https ://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html, on 11.08.2024.

[45]https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_ro, accessed on 09.08.2024.

In the era of digitization, the activity of the public administration with reference to the protection of personal data must be carried out in accordance with the provisions of some key principles in accordance with the provisions of art. 5, para. (1) and para. (2) of the GDPR these principles are as follows:

a) "the principle of fair, legal processing; and transparent to the person(s) concerned;
b) the principle regarding the limitation of the purpose by collecting for determined, explicit and legitimate purposes and they are not subsequently processed in a way incompatible with these purposes;
c) the principle of reducing processed data to a minimum and keeping them, by keeping and processing adequate and relevant data;
d) the principle according to which accurate data must be processed and, in the situations in which it is required, updated, and for inaccurate data, the necessary measures must be taken to delete or rectify it without delay;
e) the principle of keeping in a form that allows the identification of the data subjects for a period that does not exceed the period necessary to fulfill the purposes for which the data are processed. In accordance with the provisions of art. 89 paragraph (1), personal data can be stored for longer periods to the extent that they will be processed exclusively for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, but subject to the in application of the appropriate technical and organizational measures, provided for in the regulation in order to guarantee the rights and freedoms of the data subject;
f) the principle regarding processing in conditions of respect for integrity and confidentiality, which means processing in a way in which adequate security of personal data is ensured, including protection against unauthorized or illegal processing, or against loss, destruction or accidental damage, by taking appropriate technical and organizational measures;
g) the principle according to which the responsibility for compliance with the requirements provided for in paragraph (1) of art. 5, rests entirely with the operator, who can demonstrate this compliance, responsibility.".[46]

In the case of data processing based on the law, the law must ensure the conditions for compliance with these principles. For example, we have: the types of data processed, the period in which they are stored and the corresponding protection measures. In addition to these key principles, the public administration in the process of processing personal data, in order to respect the individual's personality right, must also respect other principles, among which we mention:

[46] See the provisions of art. 5, para. (1) of the GDPR – Regulation (EU) no. 679 of April 27, 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with relevance for the EEA), International Act, published in J. Of. L, no. 119 of May 4, 1996, accessed at https://legislatie.just.ro/Public/DetaliiDocumentAfis/201834, on 12.0.2024.

a) the principle of respecting the confidentiality of personal data, according to which the use of digital technologies must be done in accordance with the standards of personal data protection and ensure the confidentiality of personal information of citizens;
b) the principle of respect for transparency and responsibility, according to which the public administration must offer easy services, accessibility to information about how personal data is used and processed, and also about the administrative processes that take place in the digital environment;
c) the principle of obtaining informed consent according to which citizens must be transparently and clearly informed about how their personal data is collected, stored and used, and also be given the opportunity to express their informed consent cause;
d) the principle of the right to informational self-determination. According to this principle, citizens must have control over the personal data they provide to public authorities, including the right to request deletion or updating of this data;
e) the principle of non-discrimination, according to which digital technologies must be used without discriminating on the basis of sex, age, race or any other criterion protected by the legislation in force;
f) the principle of information security and confidentiality, according to which the public administration is obliged to ensure the security of the personal data it holds against unauthorized access, and to adopt measures in this regard to prevent possible security breaches;
g) the principle of accessibility, according to which digital technologies used in public administration must be accessible to all citizens, including persons with disabilities, in order to ensure equal participation in administrative processes;
a) the principle of respect for individual rights, so that the public administration respects the individual rights of citizens in administrative processes, which take place in the digital environment, including the right to information, the right to consultation and the right to challenge [47].

Cumulatively respecting all these principles, the public administration can fulfill its obligations and tasks according to the legal provisions in the field, offering citizens quality services and maximum security, without prejudice to their rights regarding the protection of personality.

[47]Regulation (EU) 2016/679 of the European Parliament and 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 and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), consolidated version of 04/05/2016, accessed at https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32016R0679, accessed on 12.08.2024.

6. Responsibilities and obligations of the operator (public authority) vis-à-vis the rights of the data subject (citizen)

According to the provisions of art. 12, para. (1), para. (2), para. (3), para. (4) and para. (5) of the Regulation[48], in order to ensure the protection of personal data, a series of responsibilities and obligations are provided for the public administration (the operator) in relation to the natural person whose personal data have been processed. Among these responsibilities, we mention:

a) taking appropriate measures to provide the data subject with any communications related to the processing, in a concise, transparent, intelligible and easily accessible form, using clear and simple language, in particular for any information specifically addressed to a child (in writing or by any other means, including, when appropriate, in electronic format), and at the request of the data subject, the information can be provided verbally, provided that the identity of the data subject is proven;
b) facilitating the exercise of the rights of the data subject, as a rule, the exception being the case where the operator proves that he is unable to identify the data subject;
c) providing the data subject with information on the actions taken following a request pursuant to articles (15) - (22) of the regulation, without undue delay, within one month at most from the receipt of the request, which may be extended up to 2 months when the volume of activity is justified;
d) in the situation where the operator has not taken measures regarding the request of the data subject, it must inform the data subject, without delay, within one month of receiving the request, giving reasons for the measures that were not taken and the possibility of lodge a complaint with a supervisory authority, and file a judicial appeal.

In the relationship with the citizen, it is very important to comply with the provisions regarding the processing of personal data, and in this equation, obtaining consent is the basis of any procedure in which the entity is represented by the natural person, by the citizen.

7. Consent of the user (citizen)

The consent of the user is particularly important in the relations established between the public administration and the citizen. It emphasizes the importance of obtaining the explicit and informed consent of users regarding the processing of personal data. In this sense, the public administration has a clear task, according to which it must properly inform users about how their data is processed and how they can exercise their rights provided by the DGPR.

According to the provisions of para. (42) of the Regulation, in the situation "where the processing is based on the consent of the data subject, the operator should be able to demonstrate

[48]Regulation (EU) 2016/679 of the European Parliament and 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 and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), consolidated version of 04/05/2016, accessed at https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32016R0679, accessed on 12.08.2024.

that the data subject has given his consent for the processing operation. In particular, in the context of a written statement on another matter, safeguards should ensure that the data subject is aware that he has given his consent and to what extent he has done so. In accordance with Council Directive 93/13/EEC, a declaration of consent made in advance by the operator should be provided in an intelligible and easily accessible form, using clear and plain language, and this declaration should not contain abusive clauses.

In order for the granting of consent to be informed, the data subject should at least be aware of the identity of the operator and the purposes of the processing for which the personal data are intended. Consent should not be considered freely given if the data subject does not genuinely have free choice or is unable to refuse or withdraw consent without prejudice. In particular, in the context of a written statement on another matter, safeguards should ensure that the data subject is aware that he has given his consent and to what extent he has done so. In accordance with Council Directive 93/13/EEC, a declaration of consent made in advance by the operator should be provided in an intelligible and easily accessible form, using clear and plain language, and this declaration should not contain abusive clauses."[49]

Enshrined legislatively, in some legal systems, or released and confirmed through jurisprudence or doctrine, the principle of consent is unanimously accepted as a condition for the disclosure or exposure of personality rights.[50] The person's right to his own image is one of the personality rights that, in relation to the demands of consent, raises serious and difficult issues. "Like the name, the person's image finds protection as an identifying element of the person. It being a representation of the person's physical features, when taken without the person's consent constitutes a violation of the right to the image."[51]

Regarding the regulations at the national level, the Law on free access to information of public interest no. 544/2001[52] is the one that regulates and ensures access to information of public interest. This information is that which concerns public authorities or public institutions, or if the information results from their activity, regardless of the way in which that information is expressed. Information of public interest has a much wider area, including information concerning the general interests of society.[53]

---

[49] The provisions of para. (42) of 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 and repealing Directive 95/46/ EC (General Data Protection Regulation) (Text with EEA relevance), accessed at https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32016R0679, accessed on 12.08 .2024.

[50] Calina Jugastru. "CONSENT IN THE CONTEXT OF PERSONALITY RIGHTS". Yearbook of the "George Baritiu" History Institute from Cluj-Napoca - HUMANISTICA Series 7:317-334, accessed at https://www.ceeol.com/search/article-detail?id=59059. The Central and Eastern European Online Library, The joined archive of hundreds of Central-, East- and South-East-European publishers, research institutes, and various content provider, pp. 9-19, O. Ungureanu, The right to honor and the right to dignity..., p. 4-5.

[51]Ovidiu Ungureanu, Cornelia Munteanu, The right to one's own image in the new Civil Code, accessed at https://legeaz.net/noutati-legislative/dreptul-la-proprie-image-in-noul-cod-civil, on 20.08. 2024.

[52] Law no. 544/2001 regarding free access to information of public interest, published in M. Of. of Romania", Part I, no. 663/23.10.2001.

[53] C. M. Cercelescu, The legal regime of the press. The rights and obligations of journalists, Bucharest, Edit. Teora, 2002, p. 98.

The problems related to personal information are currently subject to the provisions of Law no. 677/2001[54](repealed and replaced by the GDPR, but it is mentioned for historical context), which regulates the principles, the procedures themselves, but also the conditions under which personal data must be processed, and for the field of electronic communications the provisions of Law no. 506/2004[55] come to regulate this area regarding the collection and processing of personal information. These two laws come together, as an instrument that helps transpose the requirements of Community law in the matter, and which pays special attention to the protection of the right to private life.

8. Obstacles encountered by the public administration regarding the protection of personality in the process of processing personal data

In the processes of applying the provisions of the legislation in force, in order to protect the personality, the public administration faces certain obstacles, of a different and diverse nature, related to the structures and services offered by it. Thus, we can list some of the most important ones:a) limited financial resources - the implementation of high-performance digital solutions to protect personal information requires expensive investments, and many public institutions face limited financial resources; b) lack of technical expertise – institutions are faced with a lack of qualified staff to be able to implement and manage the digital solutions necessary to protect personal data; c) the complexity and uneven implementation of the regulations regarding the protection of personal data are in continuous change and evolution, thus creating confusion and many uncertainties, and many difficulties in their implementation; d) resistance to change is another obstacle, which is why certain public institutions are reluctant to adopt digital solutions, since technological changes may require substantial changes in existing processes and procedures; e) the vulnerability to cyber attacks is increasing, and with the increase in dependence on technology, public institutions are becoming more and more vulnerable to cyber threats, thus endangering the confidentiality of personal data; f) the implementation of legislative reforms is also an obstacle with a major impact, because the public administration may encounter difficulties in implementing the necessary legislative reforms to ensure personal data protection measures in accordance with European and international standards; g) also, the lack of logistical and informational support, of the software, implemented and used at the national level, in a unitary manner, represents one of the major obstacles for the public administration, regarding the processing of personal data and respect for the right of personality; h) the lack of automated data recording systems and the possibility of processing restrictions, in principle, to be ensured by technical means, so that personal data are not subject to other subsequent processing operations, and cannot be changed; i) the large volume of stored, managed and processed personal data

[54] Law no. 677 of November 21, 2001, for the protection of individuals regarding the processing of personal data and the free movement of such data, published in M. Of. no. 790 of December 12, 2024, repealed, accessed at https://legislatie.just.ro/Public/DetaliiDocumentAfis/32733, on August 12, 2024.
[55] Law no. 506/2004 regarding the processing of personal data and the protection of private life in the electronic communications sector, published in M. Of. of Romania, Part I, no. 1101/25.11.2004.

prevents the operator from transferring the stored data to another operator, authority, based on the request of the data subject.

Also, a series of problems regarding the protection of personality can be created by public officials and here we list: a) violation of confidentiality - public officials should respect the confidentiality of citizens' personal information and not disclose it without their consent ; b) abuse of authority - there is a risk that public officials use citizens' personal information for improper purposes or to pursue their own interests; c) violation of the right to privacy - civil servants should respect the right to privacy of citizens and not intervene in their private life without a justified reason; d) excessive surveillance - there is a risk that civil servants supervise or excessively monitor the activities and communications of citizens, thus affecting the right to confidentiality and privacy; e) unauthorized access to personal information - civil servants should have access only to the personal information strictly necessary for the performance of their duties and to comply with the rules of confidentiality and data security; f) discrimination - civil servants should be impartial and not discriminate based on race, religion, sexual orientation or other personal characteristics when making decisions or acting on behalf of the state.

9. Measures regarding the respect of personality rights by protecting personal data processed by the public administration

The public administration in fulfilling the tasks and obligations regarding the implementation of the procedures for the protection of the personality is forced to take a series of measures, according to the provisions of Regulation (EU) 2016/679. The public administration in order to comply with the measures regarding the protection of personality by complying with the protection of the processing of personal data, must implement a series of security measures to protect personal data against unauthorized access, loss or destruction. These measures may include data encryption, two-factor authentication, or backups.

Also, the public administration must implement a series of measures to protect personal data and access to them, among which we mention the most representative ones:

a) appointment of a data protection officer (DPO), either internally or by outsourcing this activity to an external DPO;
b) to ensure that he has put in place the appropriate technical and organizational measures in order to secure personal data: "(1) updating the operations/work in the sense of establishing and implementing measures to ensure the security of electronic data against unauthorized access (both from outside the institution and inside it) to signal unauthorized access, to ensure the correct preservation and archiving of files containing personal data; (2) updating/elaborating operational/work procedures or elaborating specific procedures to address the management of personal data: how this is done, who and under what conditions is authorized to collect and process personal data; and (3) establish the inclusion of confidentiality clauses in individual employment contracts for persons authorized to collect and process personal data regardless of whether they belong to their own employees or to different categories of beneficiaries of public

services. In the case of staff made up of civil servants, to analyze the opportunity to conclude confidentiality agreements regarding the management of personal data. " [56]

c) in the case of the outsourcing of part of the processing to an external organization ("person authorized by the operator"), it is mandatory to conclude a contract or another legal act guaranteeing "the fact that the person authorized by the operator offers sufficient guarantees for putting in application of appropriate technical and organizational measures that meet GDPR standards."[57]
d) informing in real time and ensuring that employees are aware of the legal provisions regarding the protection of personal data and the confidentiality of information;
e) the implementation of continuous training programs for officials, which he must coordinate and help them understand the importance of complying with personal data protection procedures;
f) develop and implement clear policies and procedures with reference to the collection, storage and processing of personal data;
g) to ensure the creation of a responsible design regarding the protection of personal data;
h) implement technical and organizational measures to protect personal data against unauthorized access, destruction or disclosure;
i) measures regarding the periodic verification of compliance with personal data protection procedures and the implementation of the necessary corrections when deficiencies are identified;
j) the implementation of measures regarding collaboration relationships with the supervisory authorities of personal data protection to ensure compliance with the provisions of the legislation in force.
k) collaboration with the competent authorities in the field of personal data protection and we are talking about ANSPDCP [58] to ensure compliance with the legislation in force and to prevent and manage possible breaches thereof..
l) regular auditing of the systems, processes and procedures used to manage personal data, in order to identify potential vulnerabilities and implement apropriate corrective measuresde măsuri corective corespunzătoare.

[56]Application of the provisions of the Data Protection Regulation (GDPR) in Public Institutions, accessed at https://www.portalinstitutiipublice.ro/aplicarea-prevederilor-regulamentului-pentru-protectia-datelor-gdpr-in-institutiile-publice-4383.htm, at dated 11.08.2024.

[57]https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general- data-protection-regulation-gdpr-public-administration-should-be-aware_ro, accessed on 09.08.2024.

[58] ANSPDCP – the National Agency for the Supervision of the Protection of Personal Data, as an autonomous central public authority with general competence in the field of personal data protection, represents the guarantor of respect for the fundamental rights to private life and the protection of personal data, established especially by art. 7 and 8 of the Charter of Fundamental Rights of the European Union, art. 16 of the Treaty on the Functioning of the European Union and of art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, information accessed at https://www.dataprotection.ro/, on 11.08.2024.

All these measures are more than necessary to protect the personal data of employees and natural persons with whom public authorities interact, in order to avoid the creation of security incidents, which would harm the image, reputation and credibility of the institutions, but also the personality rights of individuals, whose personal data are processed. The measures that the public administration can take must be related to analyzes and audits done in advance precisely in order to be able to find the correct and effective solutions in accordance with the nature and place of the problems identified. Establishing the degree of violation of personality rights in the public administration, by not complying with the legal provisions regarding the processing of personal data could be measured, by means of research carried out in relation to a series of predetermined indicators.

The degree of violation of the right of personality in the public administration can be assessed through a series of indicators that reflect the respect for individual rights and the quality of administrative activities. Among the more relevant indicators, we mention: (1) The number of complaints and appeals by recording and analyzing the number of complaints made by citizens regarding the violation of their rights in interactions with the public administration; (2) Institutions' response, measuring the efficiency and promptness with which public institutions respond to citizens' complaints and notifications regarding possible abuses of personality rights; (3) Statistics on abuses taking into account the number of confirmed cases of abuses or violations of the right of personality (for example, unauthorized disclosure of personal information); (4) Accessibility of information by evaluating how information about citizens' rights and how to challenge abuses is made accessible to the public; (5) Informing citizens by analyzing the degree to which citizens are informed about their rights and legal procedures available to protect these rights; (6) Transparency of administrative activities by evaluating the transparency of decision-making processes and the way in which personal data is managed and protected within the public administration; (7) Compliance with legislation by measuring the percentage of compliance of public institutions with national and international regulations regarding the protection of personal data and individual rights; (8). Professional training of employees by measuring the percentage of public administration employees who have been trained in personal rights and data protection; (9) Collaboration with non-governmental organizations by measuring the number of partnerships between public administration and organizations that defend human rights can indicate a commitment to the protection of personality rights and (10). Feedback from citizens by carrying out surveys and studies on the perception of citizens on the respect of their rights by the public administration.

These indicators can be used to create an overview of the degree of respect for personality rights in public administration and to identify areas within public administration that require improvement. Artificial Intelligence could be a viable solution in terms of identifying the rights violated for the persons concerned following the processing of personal data in the public administration, regarding the measurement of the degree of violation of these rights, but also regarding the implementation of a set of measures regarding the prevention

10. Positive aspects of the use (AI) in public administration and the protection of personality rights

Artificial Intelligence (AI) could be a solution in terms of the protection of personality rights, when we relate to local public authorities and citizen requests in several ways. Thus: a) by monitoring personal data – (AI) can monitor and detect violations of the confidentiality of users' personal data, so that protective measures can be taken against them; b) by identifying and preventing fraud – (AI) can be used to identify fraudulent activity and to prevent identity theft or other forms of fraud, through which the protection of a person's personality can be affected; c) by protection against cyber-attacks; d) by customizing the user experience; and e) through education and awareness. But, in the desire to build an efficient and effective public administration, de-bureaucratized and digitized, transparent and accessible, there is an imminent risk that through the implementation of (AI), precisely to achieve these standards of modern civilization, (AI) will overlap in finally to man and institutions, subsequently being forced to find the tools with which to defend ourselves, from what we have created.

11. Measures to prevent actions (AI) in view of the overlap of man and institutions, with regard to the processing of personal data and implicitly violation of personality rights.

There are several ways in which we can prevent Artificial Intelligence (AI) from overlapping human actions and institutions, these include the implementation of measures such as: a) Implementation of clear ethical rules and principles in the development and use (AI). These rules should guarantee respect for human dignity, protect privacy and prevent discrimination and misuse (AI). b). Creating mechanisms of strict supervision and control over (AI), to avoid abuses and to guarantee that the decisions made by (AI) are justified and in line with human values. c) Integrating (AI) into a clear legal and regulatory framework that establishes the responsibilities of developers and users (AI) and provides for sanctions for violations of these rules. d) Promoting transparency and accountability in (AI) development and use, by providing clear and accessible information about how (AI) works and how decisions are made. E) Encouraging dialogue and collaboration between humans and (AI), to ensure that the use of (AI) is for the benefit of humanity and that (AI) is used in a sustainable manner and in accordance with society's values and desires. By applying these precautions, we can avoid the risk of (AI) overlapping humans and institutions in an undesirable or dangerous way.

12. Possible benefits of using (AI) in the processing of personal data in the public administration, respectively in respecting the rights of the personality.

Artificial intelligence (AI) can be an important solution for efficient public administration, but it is not the only solution. Using (AI) can help automate repetitive processes, improve data analysis and make more informed decisions. By implementing (AI) public administration can reduce costs, increase efficiency and provide better and faster services to citizens. For example,

the use of artificial intelligence (AI) in procedural decision-making can lead to better planning of resources and better management of activities. However, there are also certain challenges related to the use of (AI) in public administration, such as data confidentiality, the transparency of decisions made by algorithms or the need to ensure the accessibility of services for all citizens. That is why it is important that the implementation (AI) is done responsibly and transparently taking into account all these aspects. Artificial Intelligence (AI) can play a particularly significant role in protecting users' privacy against various online threats, coming up with effective solutions and tools to prevent privacy breaches and ensure a safe and secure online experience.

13. The risks of involvement (AI) in the processing of personal data in the public administration

By involving (AI) in the processing of personal data in the public administration, in addition to the known and still unknown benefits, there are also a number of more or less predictable and identifiable risks. Among the known and possibly identifiable ones, we list::a) breach of confidentiality, as there is a risk that personal data will be accessed by unauthorized persons or used for purposes other than those for which they were collected; b) discrimination and bias that (AI) algorithms may be prone to, which may lead to incorrect or unfair decisions in public administration, affecting certain groups of people; c) human error, because (AI) can be programmed or trained incorrectly, which can lead to errors in the processing of personal data and wrong decisions taken by public authorities; d) excessive dependence on technology, can make public administration too dependent on (AI), which could lead to a decrease in the quality of public services and the inability to solve the problems facing society; e) as a result of the use of (AI) in the public administration, it can lead to a lack of transparency in the decision-making process and the lack of responsibility, the possibility of establishing it, and as a result, citizens could be negatively affected by the decisions taken by (AI), without understand how these decisions were made or how they can be challenged and f) vulnerability to cyber-attacks, by the fact that (AI) systems used in public administration can be vulnerable to cyber-attacks, which could lead to the compromise of personal data and the violation of citizens' rights and the loss of their trust in state institutions.

14. Conclusions

In the area covered by the right to information from the sphere of public administration, public issues are taken into account on the one hand, and on the other hand, issues related to the person (citizen). In accordance with the provisions of the law, informing the citizen about public information is a task of the public authority, for each field of activity separately and in accordance with its powers. Respecting personality rights means protecting rights against certain encroachments coming from private individuals, based on a horizontal relationship, established between individuals, or vertically between the individual and the state authority. Personality rights can be seen as rights of control because they allow the person to exercise control over aspects of

their personality. Therefore, mastery can be manifested through an abstention, through a disclosure or through a request for clarification or rectification. Being non-patrimonial rights, inalienable, inalienable, imprescriptible acquisitively and exhaustively, strictly personal, they are subject to the provisions of the legislation in force at the time of their exercise, and the infringements of these rights are subject to the provisions of the legislation in force at the time of their execution.

However, in order to protect the rights of the personality, the public administration must create a real long-term strategy, implement the provided measures correctly, coherently and in a unitary manner, continuously improve its civil servants in order to comply with the provisions of the regulations in force, regarding the processing of personal data, both in the reports established at the internal level, and in the level of the reports established at the external level. It is urgently necessary to carry out studies on the identification and measurement of the degree of violation of personality rights through the processing of personal data, to find the correct, preventive and sustainable solutions, using Artificial Intelligence (AI) in this sense.

REFERENCES:

1. Charter of Fundamental Rights of the European Union (2010/C 83/02), 30.3.2010 Official Journal of the European Union C 83/389.
2. The Constantinescu v. Romania case, in C. -L. Popescu, op. cit., p. 21.
3. The case of Krone Verlag GmbH & Co. KG v. Austria, in C. -L. Popescu, op. cit., p. 68.
4. Krone Verlag GmbH & Co. KG v. Austria - Freedom of the press. Information of public interest. Politician, accessed at https://legeaz.net/hotarari-cedo/krone-verlag-gmbh-nqy.
5. Cercelescu C. M., The legal regime of the press. The rights and obligations of journalists, Bucharest, Edit. Teora, 2002, p. 98.
6. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms of 04.11.1950*, integral part of Law no. 30/1994, text published in Part I no. 135 of May 31, 1994.
7. Convention 108 of January 28, 1981 of the Council of Europe for the protection of individuals against automated processing of personal data was the first international instrument with binding legal force adopted in the field of data protection.
8. The Universal Declaration of Human Rights of December 10, 1948, issued by the United Nations, published in the Booklet of December 10, 1948.
9. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of confidentiality in the public communications sector (Directive on privacy and electronic communications), in force, amended, current consolidated version 19/12/ 2009.
10. Directive (EU) 2016/680 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 by the competent authorities for the purpose of preventing, detecting, investigating or prosecuting crimes or executing sentences and on the free movement of this data and repealing the Council's Framework Decision 2008/977/JHA became applicable in May 2018.
11. GDPR - General Data Protection Regulation (GDPR) - regulation (EU) 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 and its repeal of Directive 95/46/CE (General Data Protection Regulation), applicable in 2018.
12. Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophones and Others, Court of Justice of the European Union PRESS RELEASE No 123/20 Luxembourg, 6 October 2020.
13. Jugastru C.. Consent in the context of personality rights". Yearbook of the Institute of History »George Baritiu« from Cluj-Napoca - HUMANISTICA Series 7:317-334.
14. Kayser P., Diffamation et atteinte au droit au respect de la vie privée, " Mélanges Jauffret", Presses Universitaires d'Aix-Marseille, 1974, p. 411 (cited after X. Agostinelli, op. cit., p. 78).
15. Law no. 677 of November 21, 2001 for the protection of individuals regarding the processing of personal data and the free movement of such data, published in M. Of. no. 790 of December 12, 2001.
16. Law no. 190 of July 18, 2018 on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/CE (General Data Protection Regulation), Published in M. Of. no. 651 of July 26, 2018.
17. Law no. 190 of July 18, 2018, published in M. Of. no. 651 of July 26, 2018, which will be revised according to the European Commission's Report on the evaluation and revision of the regulation from June 2020, with its new evaluation scheduled for 2024.
18. Law no. 544/2001 regarding free access to information of public interest, published in M..Of. of Romania", Part I, no. 663/23.10.2001.
19. Law no. 506/2004 regarding the processing of personal data and the protection of private life in the electronic communications sector, published in M. Of. of Romania, Part I, no. 1101/25.11.2004.
20. The new Civil Code (Law no. 287/2009, published in M. Of. no. 55 of July 15, 2011), republished, updated and consolidated.
21. The new updated Criminal Code 2024 – (Law no. 286/2009, published in M. Of. no. 510 of July 24, 2009), updated and consolidated.
22. Regulation 2022/0424(COD) on the collection and transfer of prior information on passengers in order to improve and facilitate controls at external borders.
23. Regulation 2022/0425(COD) regarding the collection and transfer of prior information on passengers for the purpose of preventing, detecting, investigating and prosecuting terrorist offenses and serious crimes.
24. 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 and repealing Directive 95/46/EC (General regulation on data protection), 4.5.2016 RO Official Journal of the European Union L 119/1.
25. Council Regulation (EU) 2017/1939 of 12 October 2017 implementing a form of consolidated cooperation with regard to the establishment of the European Public Prosecutor's Office (EPPO), in force, amended, consolidated form on 10/01/2021.
26. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the institutions, bodies, offices and agencies of the Union and on the free movement of such data and repealing Regulation (EC) no. 45/2001 and Decision no. 1247/2002/CE, 21.11.2018, RO, Official Journal of the European Union L 295/39, in force.

27. Selejan-Guţan B, Crăciunean L. M., Public International Law, Bucharest, Edit. Hamangiu, 2008, p. 99.
28. The Central and Eastern European Online Library, The joined archive of hundreds of Central-, East- and South-East-European publishers, research institutes, and various content providers, pp. 9-19.
29. Treaty on the Functioning of the European Union (consolidated version), Official Journal of the European Union, RO, C 326/47, dated 26.10.2012.
30. Ungureanu O., Munteanu C., Observations regarding the natural person and legal personality "Romanian Pandectele", no. 4, 2005, p. 180-190.
31. Ungureanu O., Munteanu C., The right to one's own image in the new Civil Code. https://legeaz.net/noutati-legislative/dreptul-la-proprie-image-in-noul-cod-civil.
32. Vrabie C., Bucharest, Romania: Pro Universitaria Publishing House, 2016.
33. Zlătescu Moroianu Irina, Human rights – a system of evolution, 2nd revised edition, IRDO Publishing House, Bucharest, 2008, pp. 10 et seq.

Webliografie:

1. https://reform-support.ec.europa.eu/
2. https://european-union.europa.eu/ institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-council_ro.
3. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_ro,
4. https://www.dataprotection.ro/?page=Scutul_de_confidentialitate_UE-SUA&lang=ro
5. https://www.weforum.org/about/world-economic-forum/
6. https://www.bing.com/search?q=b)%20Ministerul%20Transporturilor%20%C8%99i%20Infrastructurii&pc=0P472&ptag=C999N9998D031521A00ED787AAB&form=PCF463&conlogo=CT3210127
7. https://diaspora.gov.ro/mai
8. https://www.europarl.europa.eu/about-parliament/ro,
9. https://ro.wikipedia.org/wiki/Economia_Uniunii_Europene
10. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf,
11. https://multimedia.europarl.europa.eu/en/topic/pega-committee-to-investigate-use-of-pegasus-surveillance-spyware_22903
12. https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html,
13. http://data.europa.eu/eli/dir/2002/58/oj
14. https://www.europarl.europa.eu/
15. https://legislatie.just.ro/Public/DetaliiDocumentAfis/22751
16. https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:ro:PDF
17. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf#:~:text=By%20two%20Grand%20Chamber%20judgments,processing%20operations%2C%20such%20as%20its
18. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0424(COD)&l=en

19. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679
20. https://legislatie.just.ro/Public/DetaliiDocument/32733
21. https://legeaz.net/noul-cod-civil/
22. https://legeaz.net/noul-cod-penal/
23. https://eur-lex.europa.eu/eli/reg/2018/1725/oj.
24. http://data.europa.eu/eli/reg/2018/1725/oj.
25. https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html.
26. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A62012CJ0131,
27. https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html
28. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_ro.
29. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32016R0679.
30. 30.https://legeaz.net/noutati-legislative/dreptul-la-proprie-imagine-in-noul-cod-civil
31. https://www.portalinstitutiipublice.ro/aplicarea-prevederilor-regulamentului-pentru-protectia-datelor-gdpr-in-institutiile-publice-4383.htm.
32. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_ro
33. https://www.dataprotection.ro/.
34. https://legeaz.net/hotarari-cedo/constantinescu-contra-romaniei-33v,
35. https://legeaz.net/hotarari-cedo/krone-verlag-gmbh-nqy.
36. https://legeaz.net/hotarari-cedo/krone-verlag-gmbh-nqy
37. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_2&format=PDF

ABOUT THE AUTHOR

Gabriela MANEA, Adviser within the Structure of the Chief Architect from the City Hall Sector 1 of the Municipality of Bucharest, Romania.
E-mail: gabrielamanea1970@gmail.com