AI Ethics and Data Privacy compliance

1st Doina BANCIU
Academy of Romanian Scientists
(of Affiliation)
Bucharest, Romania
doina.banciu@aosr.ro

2nd Carmen Elena CÎRNU
National Institute for Research &
Development in Informatics
Bucharest, Romania
carmen.cirnu@ici.ro

Abstract— **Throughout history, technological evolution has generated less desired side effects with impact on society. In the field of IT&C, there are ongoing discussions about the role of robots within economy, but also about their impact on the labour market. In the case of digital media systems, we talk about misinformation, manipulation, fake news, etc. Issues related to the protection of the citizen's life in the face of technology began more than 25 years ago; In addition to the many messages such as "the citizen is at the center of concern" or „privacy must be respected", transmitted through various channels of different entities or companies in the field of ICT, the EU has promoted a number of legislative and normative documents to protect citizens' rights and freedoms.**

Keywords— Artificial Intelligence, GDPR, ethics, non-ethics

I. INTRODUCTION

Throughout history, technological evolution has generated less desired side effects with impact on society. In the field of IT&C, there are ongoing discussions about the role of robots within economy, but also about their impact on the labour market. In the case of digital media systems, we talk about misinformation, manipulation, fake news, etc. Issues related to the protection of the citizen's life in the face of technology began more than 25 years ago; In addition to the many messages such as "the citizen is at the center of concern" or „privacy must be respected", transmitted through various channels of different entities or companies in the field of ICT, the EU has promoted a number of legislative and normative documents to protect citizens' rights and freedoms.

The development of social networks and the implementation of e-government systems has led to storing data about citizens in digital environments or identifying it according to criteria which stakeholders could hide in high-performance software systems. To counterbalance, the EU has tried to limit the use of personal data for other purposes than those declared, by imposing on Member States the General Data Protection Regulation (known as the "GDPR"), which has become mandatory in all states. A legislative framework for artificial intelligence (AI) will probably be developed in the future, but at the moment there is no general consensus in the field of artificial intelligence.

Artificial intelligence (AI) is a booming development process. AI has created a vast suite of applications with transformative effect not only on the economy, but also on society as a whole. Although Artificial general intelligence still has a long way to go, AI - in today's form - is already becoming a part of the decision-making process.

It is well known that every new generation of technology, especially with transformative impact, generates ethical and impact governance issues. The applicability of AI in areas as diverse as health services, education, transportation, e-commerce or defense requires addressing new issues, ethics, safety and human control over this new technology and, of course, regulatory elements.

The risk of ignoring these issues and others such as vulnerabilities and threats or the erosion of the legitimacy of systems and, in particular, the impact on citizens' privacy - can lead to major imbalances in society.

These elements are analysed in various formulas, in different entities or countries, depending on the specific historical development of IT&C, the concepts underlying the company, as well as legislation and regulations.

II. HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE INITIATIVES

In Europe, there is a strategic advantage over AI ethics that lies in its power to regulate, to set rules and standards. It is becoming part of the concept of strategic autonomy and sovereignty in the area of disruptive technologies.

EU technological sovereignty is based on the European values and culture that emphasize human autonomy through concepts of sovereignty in relation to its own data and interaction with AI.

The new European strategy, which traces the steps towards digital transformation, contains elements that call into question the ethics of AI (Europe fit for the digital age, European Digital Strategy, the European Data Strategy, the Digital Services Act, the Digital Markets Act - impact on AI).

The European Commission has established a new AI regulatory framework through the adopted documents: European Commission (2021) COM / 2021/206 (final), Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Law on Artificial Intelligence), Coordinated Plan on Artificial Intelligence 2021.

As stated in the European documents, EU must become a "global leader in the development of safe, reliable and ethical AI". Only "joint action at European level can protect the EU's digital sovereignty and put to good use regulatory tools and power in order to elaborate global rules and standards."

The US has developed a strong AI industry, with a focus on governance, including ethics, justified trust in AI systems, support for democratic values: privacy, freedom, civil rights in the use of AI for national security, and fighting against malicious security operations of information led by AI.

There are numerous documents dealing with the subject of AI ethics: National Artificial Intelligence Initiative, Final

Report - National Security Commission on Artificial Intelligence, AI Partnership for Defense, to name a few.

The US has developed a strong AI industry, with focus on governance, including ethics, justified trust in AI systems, support for democratic values: privacy, freedom, civil rights in the use of AI for national security, and the fight against malicious security operations of information led by AI.

There are numerous documents dealing with the subject of AI ethics: National Artificial Intelligence Initiative, Final Report - National Security Commission on Artificial Intelligence. AI Partnership for Defense.

There is a common concern for Trans-Atlantic cooperation in AI ethics. Within the EU-US Trade and Technology Cooperation Council, one of the ten working groups is focused on AI and on issues related to its ethics and implementation values. On the other hand, the OECD pays close attention to many aspects of AI development.

We recall the AI principles promoted by the OECD and the recommendations for policy makers, which are mainly limited to investments in R&D:

III. VALUES-BASED PRINCIPLES

- Inclusive growth, sustainable development and well-being

- Human-centred values and fairness

- Transparency and explainability

- Robustness, security and safety

- Accountability

Recommendations for policy makers

- Investing in AI R&D

- Fostering a digital ecosystem for AI

- Providing an enabling policy environment for AI

- Building human capacity and preparing for labor market transition

- International co-operation for trustworthy AI

If we look at large information and communication systems and analyse the general characteristics of AI in terms of data privacy and human rights, we can see that:

- AI is not focused on people and their rights in the case of large information and communication systems (Google, Twitter, other social media channels, etc.);

- Search engine-induced AI can have profound consequences for private human rights, they can identify data and preferences about users and transfer the information to interested business companies;

- Insufficiently tested algorithms can introduce regrettable or even fatal errors for human existence (eg. misidentification of a person).

The above findings have led international and national bodies to analyse human rights issues and develop documents and recommendations for the development of AI systems:

• The UNESCO General Conference (November 2021) launched a set of ethical recommendations on AI.

• The EU Agency for Fundamental Rights has raised a number of issues regarding respect for human rights in the context of the development of AI ("Getting the Future Right - Artificial Intelligence and Fundamental Rights").

IV. THE CONCEPT OF GDPR - GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (hereinafter "GDPR" or "GDPR Regulation") is a set of rules that applies to all organizations that collect and retain personal data from anyone in the European Union. "GDPR" became law in Romania starting with May 25, 2018.

The purpose of GDPR is to create a standardized framework on data privacy so that individual human rights are protected. This is essential within an economy that is increasingly based on the use of personal data in many areas of activity.

In the context of digital transformation, the protection of personal data is an issue that is relevant in any company and is in the focus of government structures.

As mentioned in (https://gdprcomplet.ro/consultanta-gdpr-firme-it/) the concepts underlying GDPR compliance are:

- Legality, fairness and transparency towards the data subject.

- Limitation of purpose - use of data exclusively in the manner presented to the individual;

- Data minimization - processing the necessary data only;

- Accuracy – updates when necessary;

- Integrity and confidentiality - data protection through appropriate measures;

- Responsibility - the ability to demonstrate respect for principles;

- Storage limitations.

The following table compares the rights of users in the light of GDPR and AI, respectively

	User's rights	GDPR	IA / Citizen's rights
1	- to information	Data is processed, noting why, for what purposes, to whom it is transmitted and what rights it has	There are no restrictions on the use of personal data. Data is retrieved from

			anywhere and published. Access is free and unrestricted.
2	- to access	Access to processed personal information	Free access to information about the citizen, but only to the public ones
3	- to correct	Correcting personal data and incomplete/inaccurate information concerning it	Difficult procedures, often impossible to implement
4	- to delete	Deleting data concerning the user	Difficult procedures, often impossible to implement
5	- to restrict processing	Restriction on processing of the application with the necessary arguments	There is no possibility of restriction
6	- to portability	It may be required to carry data from one operator to another	Not applicable due to lack of information
7	- to object	End processing, with documents and arguments	It is not regulated procedurally and legally
8	- not to be subject to an automatic decision, including profiling	Interventions in the case of important decisions concerning the user personally	There are no restrictions
9	- to lodge a complaint with the Supervisory Authority	Complaint forms against non-compliant processing	There is no institutional form
10	- to apply to the court	To obtain pecuniary and / or non-pecuniary damage if damage has resulted	It is not legally regulated

Structurally, there are major differences between AI and GDPR in terms of "data privacy"

• GDPR protects the person	AI discloses personal information with / without consent
• GDPR regulates the use of data	AI works according to its own rules
• GDPR allows for individual protection actions	AI does not facilitate individual protection actions
• GDPR imposes concrete pecuniary sanctions	AI does not have a sanctioning mechanism

The users can't influence the balance between ethics and non-ethics, because the non-ethics aspects are hided in the software, especially in the AI components.

If we analyze the main objectives of the information and documentation systems, we will identify some common issues:

• Democratic access to the cultural information storages in national and international digital collections (any discrimination).

• Dissemination of information through traditional and digital tools.

• Contribute to development positively of behavior and attitude.

Even if the objectives are clearly defined, the contradiction between ethics and non-ethics can be hided under AI software.

ETHICS	NON-ETHICS
Dissemination of any kind of information	Dissemination of fake news
Business development facilitating through access to information	Transfer of business information on interest profiles upon request to non-interested entities
Transparency facilitating	Generating flows for the dissemination of special information (defamation, misleading, influencing behavior, etc.)
Facilitates access to the information desired by the user	Access to preferential information based on special interests or orders
Facilitates different information and documentation on topics	Facilitates information and "*serendipity*" (with possible "noise" and "lost" effects) - the risk of providing harmful socio-political-economic information

The barrier between ethics and non-ethics is very "fuzzy".
Any legal framework can be adapted if the barriers are not

clearly separated. The information system tries to achieve their goals as well as they can, but often unethical aspects are invisible even if they exist.

Figure 1 shows the contradiction between ethical and unethical in the case of human rights and what research and retrieval software systems can do.
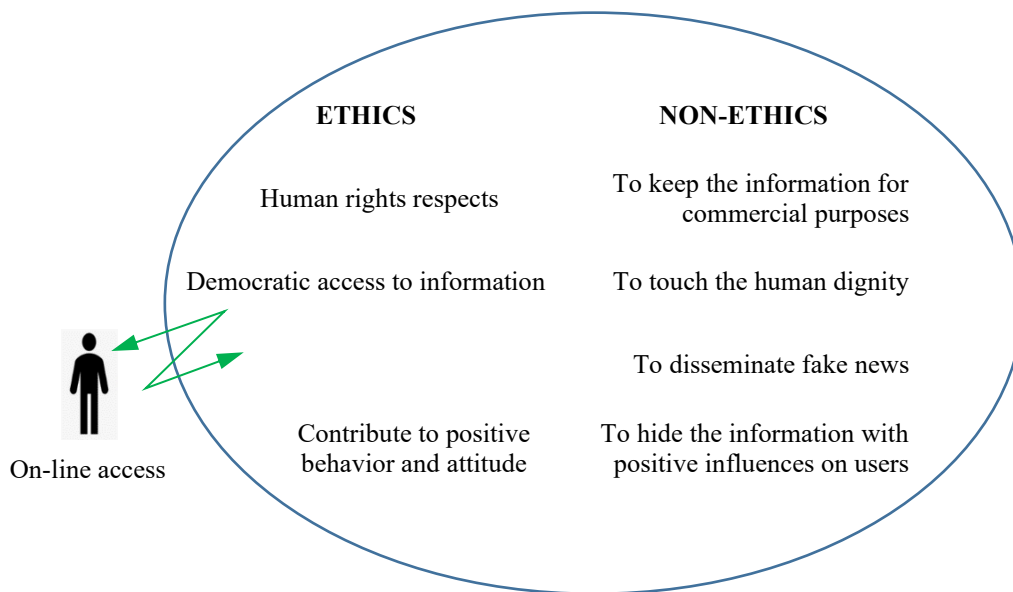

Fig. 1. Contradictions between ethic and non-ethic in information and documentation systems.

Neither system management nor users can control this phenomenon. Often, managers have no knowledge of software systems and it is difficult for users to understand how software requirements or research results have been performed. These aspects allow software developers to create a software system as they wish or as their needs dictate.

On the other hand, the undeniable benefits of AI development cannot prevent companies from developing AI-based software and services. Here are some examples of the direct benefits of AI in Internet-based information systems and networks:

- AI facilitates the dissemination of information of any kind;
- AI facilitates the development of business actions;
- AI facilitates "transparency";
- AI facilitates information and "serendipity".

V. Conclusions

The study on GDPR and AI, from the point of view of human rights, has highlighted several conclusions:

- GDPR regulates the use of personal data and it is mandatory in Europe - the business and public administration comply with the regulation;
- It is obvious that there are still many steps to be taken with regard to AI;
- AI developers have an ethical obligation to make the structure and pathways transparent if algorithms can infringe on human rights;

- AI developers need to explain / argue whether the developed algorithms can identify the occurrence of ethical issues in use and make them known;
- Expanding AI developer communities to improve model quality and reduce bias (the Harvard example has such an initiative, but the effect is limited);
- The legal framework is not yet adapted to AI applications, and large companies need to play a key role in regulation, along with universities and research institutions;
- Cooperation and collaboration in order to reach a consensus on respecting private human rights in AI applications may be a possible first step in the regulation on the protection of personal data.

The GDPR example could be the starting point for a unanimously accepted legislative framework.

References

[1] Gheorghe, Maria. Drepturi și libertăți în epoca Inteligenței artificiale, Rev. Intelligence, nr. 42/21, pag.52-55
[2] Banciu, Doina; Mantykangas, Arja. Library management in the context of the GDPR, Vol. 4/DOI 10.12753/2066-026X-18-266 | Pages: 372-377, în eLSE 2018.
[3] https://legalup.ro/regulament-gdpr/
[4] https://www.marketnet.ro/resurse/analiza/gdpr-pe-intelesul-tuturor---implementare-in-7-pasi
[5] https://gdprcomplet.ro/consultanta-gdpr-firme-it/
[6] https://emerging-europe.com/voices/gdpr-looking-back-and-looking-forward/
[7] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf

[8] Getting The Future Right Artificial Intelligence and Fundamental Rights.