THE ANNALS
OF "DUNAREA DE JOS"
UNIVERSITY OF GALATI
LEGAL SCIENCES. FASCICLE XXVI

Strategies of the European Institutions on Cyber Security, Artificial Intelligence, Algorithms

Adriana-Iuliana STANCU[1]

Abstract: *Objectives: Algorithms are becoming more widely used in decision making. However, as they become more prevalent in everyday life, there is a concerning lack of information among individuals, governments, and researchers about how they work, according to CEPA - the Center for European Policy Analysis. Only now are governments in Europe and the United States becoming aware of the possible ramifications of algorithmic judgments, such as inherent prejudice. Unfortunately, there is limited coordination across transatlantic countries on how to increase openness in algorithmic judgments while respecting developers' intellectual property rights. Recommendations and strategies: In the United States, legislation governing technology, such as the Algorithmic Accountability Act of 2019, has been stuck in Congress. However, among EU member states, France has prioritized algorithmic openness. Results and implications: The European Union institutions collaborated to draft Regulation (EU) 2024/1689 of the European Parliament and Council of 13 June 2024 establishing harmonization provisions on artificial intelligence and amend Regulation (EC) n. 300/2008, (European Union) no. 167/2013, (European Union) no. 168/2013, (IU) 2018/858, (IU) 2018/1139 and (IU) 2019/2144 and Directives 2014/90/IU, (IU) 2016/797 and (IU) Guideline/1, which will be applicable from August 2, 2026.*

Keywords: *AI; algorithms; harmonization; legislation; cyber security*

[1] Associate Professor, PhD, Head of Department Legal Scinces, Faculty of Law and Administrative Sciences, "Dunarea de Jos" University of Galati, Romania, Address: Domneasca, no 111, Galati 800201, Romania, Corresponding author: adriana.tudorache@ugal.ro.

1. Introduction

Artificial intelligence was founded as an academic discipline in 1956, and has since gone through several waves of optimism, followed by disappointment and loss of funding, also known as "AI winters," followed by innovations, succeeding with new funding (Likano, 2018). AI research was traditionally split into subfields that rarely interacted with one another. These subfields are based on technical notions such as specific goals - such as "robotics" or "machine learning" - the use of specialized tools based on logic or artificial neural networks, or fundamental philosophical differences. The subfields were also organized around certain social phenomena, such as institutions or the work of specific academics.

AI research typically focuses on reasoning, logic, knowledge representation, planning, learning, natural language processing, and object manipulation. The field's long-term goals include general intelligence. Statistical methodologies, computational intelligence, and classical symbolic AI are among the approaches. AI employs a wide range of tools, including mathematical search and optimization variants, artificial neural networks, and projection, capacity, and economics-based methodologies.

Artificial intelligence is based on computer science, data engineering, mathematics, languages, psychology, sociology, philosophy, and a variety of other disciplines.

This field of inquiry was predicated on the assumption that the human mind "can be described so accurately that you can make a machine to simulate it." This raises philosophical issues concerning the nature of consciousness and the ethics of constructing artificial entities with human intelligence, which have been explored in mythology, folklore, and philosophy from ancient times. Some people worry that if AI continues to develop unchecked, it will pose a threat to humans. Others worry that, unlike earlier technical changes, AI will pose a threat of widespread unemployment.

2. Algorithms and Artificial Intelligence

According to theverge.com, during the hearing before the US Congress, Mark Zukerberg, the co-founder was asked how he could keep his Facebook free, and the answer became famous, posted in the form of memes and shared online: "Senator, we are executing processes." With an overabundance of user data, these ads influence users' interests, preferences, emotions, and behaviors to make them buy. It is desirable to insert the card as quickly and as often as possible. For example, Instagram recently changed the button for checking notifications with a button that leads to online stores.

The Norwegian Consumer Protection Authority published a report in 2018 that shows how technology companies are using design to discourage users from exercising their right to privacy description. (Arnold Rosenthal, 2010)

Also in 2018, the European Data Protection Supervisor published an opinion on online manipulation which highlighted how the processing of non-compliant data can lead, among other things, to influencing consumer decisions and, in extreme cases, to influencing votes in the election campaign. This problem was brought back into the discussion in 2020, by ECPD, which highlighted the fact that user segmentation by profile can affect their freedom of choice when shopping online or affect their choice preferences (Sfetcu, 2022).

In an article he shows how Facebook created profiles of people who didn't even have Facebook accounts through plugins that were installed on websites such as the like button. The conclusion of this article is that Facebook tracks all Internet users, whether they have a Facebook account or not.

"Machine learning algorithms are designed to process large volumes of data and make connections that allow companies to construct excessive and voluntary information from individuals," and "often publish many types of personal information on different platforms that allow profiling of an individual and create certain information that may be incorrect or even fraudulent"

From profiling to manipulation is just one step. The European Data Protection Agency notes that Big Data and behavioral science can create behavioral profiles of engagement. The Spanish data protection authority stated that the development of AI could lead to the construction of human profiles to be used for marketing or electoral purposes.

The Norwegian Consumer Protection Authority wrote that digital services benefit from collecting personal information and that there are strong incentives to encourage users to voluntarily provide as much information as possible. If the digital service collects personal data and the user is unaware of the implications of this data collection, we are in the presence of a power imbalance in which the digital service holds too much power over the user.

In 2020, the European Commission published two documents defining Europe's digital future. The first is called the "Information Approach" and the second is the "Artificial Intelligence Approach". (Cross Wood, 2020)

These documents state that although data processing and artificial intelligence pose threats to human rights and fundamental freedoms, a common data space must be created as it is Europe's only opportunity to face the global race for AI.

The conclusion we draw from the above is that human rights and fundamental freedoms are at stake. Of course, at first glance, it doesn't seem to affect us much, but the mission of the law is to protect all people, including vulnerable neighborhoods: children, the elderly, etc. However, many works talk about secret operations, as in Kafka or Orwell's novels. And maybe we should plant We look at things from a future perspective, especially in the context where AI is still in its infancy and "no one can know" what the digital society of the future will look like.

3. Artificial Intelligence and Cyber Security

In accordance with the 2014 Cyber Defense Policy Framework and its 2018 update, the Council of Europe, hereinafter referred to as the Council, agreed to a joint relationship on EU cybersecurity policy to reinvest in our modern and cooperative forces and technologies next-generation capabilities, as well as cybersecurity and strengthening partnerships to address common challenges (Forbrukerradet, 2018). At a time when reliance on digital technologies is growing, cybernetics has emerged as a lucrative field. As a result, keeping an open, autonomous, reliable, and secure online presence is crucial. In addition to the already noticeable increase in Internet activity outside of the recent armed conflict, the use of cyber operations that supported and enabled Russia's unjustified and unwarranted war of aggression against Ukraine has an impact on global stability and security and poses a serious risk of escalation.

The conflict in Ukraine created a new geopolitical backdrop and reaffirmed the necessity for the EU, its member states, and its allies to fortify the EU's ability to combat cyberthreats and to bolster traditional cyber security and cyber defence against malevolent conduct and provocative acts online. The EU Cybersecurity Policy Joint Communication highlights the resolve of European institutions to offer prompt and efficient solutions to guarantee freedom of action in cyberspace and responses to threat actors who aim, among other things, to breach, interfere with, or destroy EU and its partner networks and IT systems. This Joint Communication is a significant step toward the EU's holistic approach to resilience, reaction, conflict prevention, collaboration, and stability in cyberspace. It complements the EU Cyber Security Strategy and is in line with the Strategic Guidelines. The Council of Europe underlined the necessity of sufficient and well-coordinated responses from the EU, its member states, and its partners in this regard. They also anticipate that the review of the EU Cyber Diplomacy Toolkit's implementation guidelines will be a major advancement in the development of the EU cyber platform (Leather, Zemskova & Groussot, 2019).

There is no hierarchy between the military and civilian communities, and recent cyberattacks on vital European infrastructure, the quick rise of cyberthreats, and the speed of technological advancement all emphasize the need for increased coordination and collaboration between the two. In compliance with international law, including human rights law and international humanitarian law, the EU's cybersecurity policy allows the EU and its Member States to improve their defense, detection, defense, and even deterrent capabilities by effectively utilizing the entire array of security options accessible to the military and civilian communities. According to Article 4(2) TEU, each Member State is still in charge of national security, including in the cyber domain. However, there is a need for significant individual and group investment in enhancing resilience, deploying cyber defense capabilities, and utilizing EU cooperation structures or financial incentives. To safeguard the Union, European citizens, EUIBA (European Union institutions, bodies and agencies), and the cyber missions and activities of the Continuing Security and Defense Policy (PCSD), Member States and EUIBA institutions, bodies, and agencies must step up their efforts. Additionally, it emphasizes the significance of the EU's cyber resilience by enhancing collaboration with a trusted return ecosystem and building cyber defense capabilities. A common action is therefore needed to strengthen cybersecurity.

Building trust is crucial for the future development of an EU cybersecurity compliance crisis management mechanism in cyberspace, and this requires a progressive, open, and inclusive approach. The Council is responsible for developing the crisis management roadmap. By means of enhanced situational awareness, capability development, training, exercises, and resilience, as well as a firm response to cyberattacks against the EU and its Member States, as well as against EUIBA, CSDP missions, and operations, the Council reaffirms the necessity of continuing to strengthen our ability to defend, detect, defend against, and prevent cyberattacks. To reduce cyber tensions, avoid unnecessary tasks, and ensure that ongoing initiatives are coordinated, the Council strongly advises the High Representative and the Commission to take this action. The cooperation and coordination of cybersecurity experts between the EU and its member states, between the military and civilian Internet communities, and between a dependable private ecosystem and a public ecosystem must all be improved. In this regard, Member States are urged to investigate and enhance their national civil-military coordination systems, promote information sharing, exchange lessons learned, help create interoperable standards, conduct risk assessments, and create reliability platforms for joint operations and disasters, particularly at the European level, all while adhering strictly to the directive's requirements. on steps to ensure a high standard of cybersecurity throughout the Union (NIS2) (Polito C. Pupillo L, 2024)

Therefore, it is recalled that to guarantee preparedness and efficacy, online education, training, and exercises are necessary. Additionally, national jobs are required, in addition to services offered by the EU through the European Security and Defense Academy (AESD), EDA, ENISA, and upcoming PESCO implementation projects like the Associations for the Internet Environment and the EU Internet Academy and Innovation Hub (CAIH). European institutions anticipate that the EDA CyDef-X framework project for synchronization and support of cybersecurity services will be established to further strengthen these efforts. In close collaboration with Member States and the European Union Foreign Affairs Agency (EEAS), the Council urges the European Defense Agency (AED) to investigate how CyDef-X can also support operations like CYBER PHHALANX. This includes mutual assistance under Article 42, paragraph 7 TEU and the solidarity clause under Article 222 TFEU, as well as the Commission and ENISA regarding civil actions.

The Council also promotes the CyDef-X cybersecurity test environment's wider use and advancement. Initiatives like Cyber Range Federations are also in place at the moment. The Council stresses that the mahu 'inga should routinely conduct large-scale national exercises at the member countries' decision-making level to guarantee a prompt and efficient decision-making process on a cyber crisis issue.

4. The 2024 EU Regulation and its Implications for the Promotion of Artificial Intelligence

The presence of unacceptable risks posed using AI in certain ways will inevitably lead to prohibitions and general provisions of the Regulation for use from 2 February 2025. Although the full effect of each prohibition is related to the establishment of control and. In applying this regulation, the intended use of prohibitions is essential to explain unacceptable risks and to have effects in other processes such as civil law. Moreover, the provisions pertaining to notified bodies and the governance structure should take effect on August 2, 2025, since the implementation of the relevant infrastructure governance and policy evaluation system is required to be completed by August 2, 2026. In the first century of technological advancement and adoption of general-purpose AI models, the roles of AI model providers AI should be used for general exploration from August 2nd. The Office of AI must ensure that classification policies and practices are updated in line with technological developments. Furthermore, Member States must establish and inform the Commission about the rules regarding sanctions, including administrative fines, and determine whether they are duly and effectively implemented on the date of entry into force of this Decree (Acemoglu, 2021).

The harmonization provisions set out in the Regulation should apply to all sectors and, subject to the new legal framework, existing Union legislation should not be affected, data protection, consumer protection, fundamental rights, operational workers, worker protection. and product safety, which complements this regulation

(English Data Protection Agency, 2020). The Council Directive 85/374/EEC's provisions for damages compensation are still in effect and fully applicable. Additionally, this regulation should not impact national labor laws and Union law on social policy for employment and working conditions in the context of worker protection and employment. work, such as doing good deeds, staying safe at work, and communicating with employers. The right to strike or perform other tasks related to specific operational communication systems of members or governments, as well as the right to negotiate, reach and enforce collective agreements or take collective action in compliance with national law, are among the fundamental rights recognized in member countries and in the case of the Union that will not be impacted by this regulation (Solove, 2004).

Suppliers must make sure that AI systems that are intended to communicate directly with people are created and designed so that the people in question engage with the AI system, unless this is obvious for a good reason., a naturally cautious and prudent person, considering the situation and degree of use. This duty does not apply to artificial intelligence (AI) systems that are legally permitted to identify, stop, look into, or prosecute crimes as long as third parties' rights and liberties are sufficiently protected, and the systems are accessible to the public for reporting crimes (Baiaş, 1999).

AI system providers, particularly general-purpose AI systems that produce synthetic content in text, voice, image, or video formats, must make sure that the system's output is identified as artificially modified or generated in a manner that can be automatically processed and discovered.

Providers must make sure that their technical solutions are robust, dependable, collaborative, and effective to the extent that they are technically feasible. They must also consider the limitations and quirks of various content types, implementation costs, and the technology's generally acknowledged stage of development, and how these factors can be represented in the pertinent technical standards. This duty is not applicable if AI systems carry out supplemental routine editing tasks, do not significantly change the data supplied by the implementer or its semantics, or if they are legally permitted to identify, stop, investigate, or prosecute criminal activity (Working Group, 2018).

If these suppliers are from third-world nations, they are required to send a representative to the EU to explain the Order's requirements. Implementers of biometric classification or emotion recognition systems notify natural persons who are exposed to them about how the system works and how personal data is processed in compliance with Directive (EU) 2016/680 and Regulations (EU) 2016/679 and (EU) 2018/1725, as applicable. AI systems used for biometric categorization and emotion recognition are exempt from this duty since they are legally permitted to identify, stop, or investigate criminal activity, provided that third parties' rights and freedoms are adequately protected, and that Union law is followed (Edwards & Veale, 2017).

When an AI system is used to create or modify images, audio, or video content, deepfakes are produced, which demonstrate that the content was produced or altered artificially. If using it for the discovery, prevention, investigation, or repression of crimes is permitted by law, this duty is not applicable. In cases where the content is a part of a program or work that is clearly artistic, creative, satirical, opinionated, or of a similar nature, the disclosure requirements outlined in this paragraph are meant to show that such content exists and is generated or manipulated appropriately, without preventing the work from being shown or accepted. To protect the integrity of the EU legal system, the standards become necessary (EDPS, 2018).

To enlighten the public about topics that are relevant to the people who indicate that the book was written or utilized, implementers of AI systems create, or process published papers. This requirement is not applicable if the use is permitted by law to identify, stop, investigate, or prosecute "cognizable crimes," if the AI-generated content has undergone editorial testing or human review and editorial responsibility for publication, or if the content belongs to a person or organization. At the latest, at the initial contact or presentation, all this information is given to interested parties in an understandable and unique way. The data must adhere to the relevant accessibility standards.

To support the efficient execution of tasks pertaining to the identification and naming of substances created or processed by the creative process, the AI Office promotes and assists the creation of good practice policies at the Union level. Each of the excellent practice provisions may be approved by the Commission through the adoption of implementing legislation (Oprea & Șandru, 2015).

The market surveillance authority of a Member State must evaluate whether the AI system in question complies with all set rules and obligations when it has good reason to believe that it poses a risk as specified in the regulation. beyond the purview of this rule, with a focus on AI systems that endanger vulnerable populations. "The market surveillance authority must also notify and fully cooperate with the government in charge of controls, or the pertinent bodies listed in the order when threats to fundamental rights are identified."

5. Conclusions

To find possible synergies between their respective voluntary commitments to develop national cybersecurity capabilities and crisis management frameworks, protect critical infrastructures, improve knowledge exchange on the state of Internet services, and engage in activities in third countries, the EU and NATO must establish links at the appropriate levels in the areas of education and training, platform knowledge, ratings, and R&D levels. This includes improved policy debates on cybersecurity challenges at all levels, as well as the NATO Technical Agreement on Cyber Incidents (NCIRC) and the Cyber Emergency Response Team – EU (CERT-EU).

Considering cybersecurity reports and EU policy on Internet protection, the European Council asked the Commission and the High Representative to create a security strategy for the implementation of uniform regulations, which Member States would then have to approve. To increase their influence at the EU level, member states should also freely express their cybersecurity goals and initiatives within the framework of the EU's cyberspace security policy. They should also fully utilize voluntary non-legislative proposals and commitments to bolster their governments' national and international cyber defenses initiatives. Every year, the High Representative, the Commission, and the Member States are invited to report on and discuss the ongoing progress of putting the elements of cooperative engagement into practice with their implementation plan.

The fact that the European Union's institutions collaborated to revise Regulation (EU) 2024/1689 of the European Parliament and Council on June 13, 2024, which suggested harmonization norms for human thinking, is not inconsequential. At a time of substantial change in the regulation of algorithms and artificial intelligence (AI), (TS) no. 300/2008, (European Union) no. 167/2013, (European Union) n. e (EU/1 8280 and regulation) is meant to be implemented throughout the EU and should go into effect on August 2, 2026.

6. References

Acemoglu, D. (2021). Opinion: The AI we should fear is already here. *The Washington Post,* https://www.washingtonpost.com/opinions/2021/07/21/ai-we-should-fear- is-already-here/ accessed on 18.08.2024

Agencia Española de Protección de Datos (2020). *RGPD compliance of processes that embed Artificial Intelligence. An introduction*, p. 6.

Baiaş I. (2020). How you can catch a criminal using artificial intelligence (AI) algorithms and techniques. *HotNews.ro*, https://www.hotnews.ro/stiri-superputerile_tehnologiei-24433285-interviu-cum-poti-prinde-criminal-using-technical-algorithms-artificial-intelligence-vladniculescu-since-researcher-the-hague-important-we-find-balance-between-the-need-of-forces-effective-order-the-need- of-society.htm accessed on 04.08.2024

Builtln (2017). *What is Artificial Intelligence*? https://builtin.com/artificial-intelligence accessed on 14.08.2024

Chohlas-Wood, A. (2020). Understanding risk assessment instruments in criminal justice. *The Brookings Institution*, https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice/ accessed in dated 14.08.2024

Daniel, J. Solove (2004). The digital person. Technology and Privacy in the Information Age. New York: New York University Press.

EDPB (2020). *Guidelines 8/2020 on the targeting of social media users, Version 1.0, Version for public consultation*, 2 September.

EDPS (2018). Opinion on online manipulation and personal data. *Opinion* 3/2018, p. 8.

Edwards, Lilian & Veale, Michael (May 23, 2017). Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *16 Duke Law & Technology Review* 18.

Forbrukerradet, (2018). *Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*.

Gill Pedro, Eduardo; Zemskova, Anna & Groussot, Xavier (2019). Towards general principles 2.0: the application of the general principles of European Union law in the digital society. *Romanian Journal of European (Community) Law no. 4*. Electronic version provided by the platform sintact.ro.

Opre, Ancuța Gianina & Șandru, Simona (2015). *The right to be forgotten on the Internet, a means of combating discrimination* in Tomescu, M. (ed.). *Non-discrimination and equal opportunities in contemporary society*. Bucharest: Pro Universitaria.

Polito, C. & Pupillo, L (2024). Artificial Intelligence and Cybersecurity. *Forum Journal,* Volume 59, No. 1.

Rigano, C. (2018). Using Artificial Intelligence to Address Criminal Justice Needs. *National Institute of Justice*. https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs accessed on 09.08.2024.

Roosendaal, Arnold (2011). Facebook Tracks and Traces Everyone: Like This! (November 30, 2010). *Tilburg Law School Legal Studies Research Paper Series* No. 03.

Sfetcu, Nicolae (2022). *Introduction to artificial intelligence.* Bucharest: MultiMedia Publishing, https://www.telework.ro/ro/e-books/introducere-in-inteligentaartificiala/ accessed on 16.08.2024

Working Group (2018). *Article 29 For Data Protection, Guidelines on automated individual decision-making and profiling within the meaning of Regulation (EU) 2016/679, Adopted on 3 October 2017 as last revised and adopted on 6 February 2018.*