INTERNATIONAL
HELLENIC
UNIVERSITY

The draft AI Act through the lens of the GDPR

Fani Polyzou

UNIVERSITY CENTER OF INTERNATIONAL PROGRAMMES OF STUDIES
SCHOOL OF HUMANITIES, SOCIAL SCIENCES AND ECONOMICS

A thesis submitted for the degree of
LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation

February - 2024
Thessaloniki – Greece

Student Name: Fani Polyzou

SID: 110422006
Supervisor: Prof. Komninos Komnios

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

February - 2024
Thessaloniki - Greece

Abstract

This dissertation was written as part of the LL.M. in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation at the International Hellenic University.
This Dissertation addresses the relationship between the General Data Protection Regulation (GDPR) and the draft Regulation for Artificial Intelligence (AI Act). After introducing the key provisions of both Regulations, their background, scope, and objective, this study proceeds to a comparative analysis of the two legislations, in order to determine whether their relationship is characterized by tension or they are in harmony.

Keywords: Artificial Intelligence Regulation – GDPR - AI Act - data protection - privacy

Fani Polyzou
February 2024

Preface

I would like to thank Prof. Komninos Komnios for the introduction to the interesting world of the personal data protection law, for all his valuable advice during our classes and for his guidance during the writing of my Dissertation.

I would also like to thank my family for all their support during my LL.M. and especially my sister, Iliana, to whom I dedicate my Dissertation, for her constant love and support.

Contents

ABSTRACT ..... **III**

PREFACE ..... **I**

CONTENTS ..... **III**

INTRODUCTION **1**

1. OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION (GDPR) **5**

KEY PROVISIONS RELEVANT TO AI SYSTEMS 5

2. INTRODUCTION TO THE AI ACT **11**

2.1 BACKGROUND – OBJECTIVES AND SCOPE OF THE AI ACT 11

2.2 RELATIONSHIP BETWEEN THE AI ACT AND THE GDPR 14

3. COMPARATIVE ANALYSIS OF THE GDPR AND THE AI ACT **17**

3.1 PROCESSING OF PERSONAL DATA BY AI SYSTEMS 17

3.2 ROLES AND RESPONSIBILITIES OF ACTORS UNDER THE GDPR AND AI ACT 18

3.3 DATA MINIMIZATION 20

3.4 TRANSPARENCY AND THE BLACK BOX ISSUE 22

3.5 PROFILING AND AUTOMATED DECISION-MAKING 24

3.6 SECURITY OF PROCESSING AND PRIVACY BY DESIGN 27

3.7 ANONYMIZATION AND PSEUDONYMIZATION 29

3.8 ENFORCEMENT MECHANISMS AND SANCTIONS 30

3.9 CHALLENGES AND POTENTIAL CONFLICTS BETWEEN THE GDPR AND AI ACT 32

3.10 PRACTICAL IMPLEMENTATION AND COMPLIANCE CONSIDERATIONS 35

4. FUTURE PERSPECTIVES AND RECOMMENDATIONS .... ERROR! BOOKMARK NOT DEFINED.

4.1 BALANCING INNOVATION AND DATA PROTECTION 39

4.2 POTENTIAL AREAS FOR FURTHER LEGISLATIVE DEVELOPMENT 41

CONCLUSION **45**

BIBLIOGRAPHY 46

Introduction

As members of the digital age, we come across a variety of new technology practically every day. Digital assistants powered by Artificial Intelligence (AI), such as Siri or Alexa, are already a part of our daily lives. With a single command, these digital assistants simplify our lives by completing multiple tasks, from playing Christmas songs to regulating the lighting and temperature in our homes. However, a significant amount of data is required to be processed for these systems to function properly, not only during the «use stage» but also during the «training stage». Not to mention the amount of our personal data these systems require in order to be able to offer personalized services. Despite their obvious benefits, their potential risks didn't go unnoticed by the European Union's bodies.

ChatGPT's launching in November of 2022 made things far more complicated, with Italy's data protection authority, known as Garante, banning it over alleged breaches of European Union (EU) privacy and data protection rules. According to the Italian Garante, there was no legal basis to justify «the mass collection and storage of data for the purpose of 'training' the algorithms underlining the operation of the platform».[1] Additionally, it stated that the software «exposes minors to absolutely unsuited answers compared to their degree of development and awareness».

Legislation is probably the most sufficient solution to mitigate the risks associated with these new technologies. The first piece of legislation pertaining to the protection of personal data was the General Protection Regulation (GDPR), which was adopted in 2016. It gave data subjects the ability to control the processing of their personal data and placed obligations on companies to comply with in order to process personal data. GDPR was also the first piece of legislation referring to data processing via the Internet, however, when the GDPR was adopted, the development of AI technology was still at a very early stage of development. As a result, even though the GDPR still remains a very powerful tool for data protection, the Regulation was deemed insufficient to address some complex new issues, which were created by AI systems. As a result, in April 2021 the European Commission proposed a draft for a Regulation of AI systems, which, when finalized, shall be the first EU regulatory framework for AI, and hopefully bring legal certainty.

[1] See https://www.bbc.com/news/technology-65139406

1. **Overview of the General Data Protection Regulation (GDPR)**

The issue of the protection of personal data has already been raised in the European Union since 1995 when the European Data Protection Directive (Directive 95/46/EC) was adopted and became an international paradigm for data protection. However, the constant technological advances and the new risks that they entailed, made this piece of legislation inadequate and after almost four years of discussions the Data Protection Directive was finally replaced by the EU Regulation 2016/679, *the so-called General Data Protection Regulation (in short: GDPR)*. The GDPR, which was adopted in April 2016 and became effective in May 2018, lays down rules concerning the protection of natural persons with regard to the *processing of personal data* and rules regarding *the free movement of personal data*[2], and by personal data meaning «any information relating to an identified or identifiable person»[3], which is called a «data subject». The term processing of personal data is perceived under the GDPR as «any operation […] such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction» of personal data[4], which takes place by the so-called controllers or the processors of the aforementioned data. A controller is defined under the GDPR as the person who «alone or jointly with others determines the purposes and means of the processing of the personal data»[5] and it is the controller's responsibility to determine why and how data will be processed.

Key Provisions relevant to AI systems

The General Data Protection Regulation (GDPR) governs the processing of personal data independently of the technology employed, and even though it includes certain Internet-related terminology (website, Internet, links, etc.) -in contrast to the 1995 Data Protection Directive- it does not make any specific reference to Artificial Intelligence (AI) but instead controls how personal data is processed, irrespective of

[2] See Art. 1 §1 GDPR
[3] See Art. 4 (1) GDPR
[4] See Art. 4 (2) GDPR
[5] See Art. 4 (7) GDPR

the technology employed[6]. This illustrates how the GDPR is more concerned with the problems relating to the Internet and its uses -which did not exist when the Data Protection Directive was drafted- rather than the brand-new AI-related problems. However, as we already mentioned the GDPR applies to the processing of personal data in general, making data processed by AI technology fall within the scope of the Regulation. According to the European Data Protection Board (EDPB) «any processing of personal data through an algorithm falls within the scope of the GDPR»[7], meaning that any time an AI system processes personal data, all of the GDPR's provisions may be applicable. When dealing with AI systems it is important to make a distinction between the two separate stages in which an AI system processes data – the algorithmic training phase and the use phase. In the former, a set of data is used to train the AI's algorithm, enabling it to build a model by finding connections and patterns among various data points. In the latter stage, this model is applied to the specific use case for which AI was created, with the aim of offering a forecast or classification, supporting human decision-making, or making the choice itself. Thus, personal data is essential to an AI system's whole life circle.

Controllers must depend on one of the six grounds for legitimate data processing specified under Article 6 of the GDPR in order to process personal data using AI systems: consent, performance of a contract, processing required by a legal obligation, vital interests of the data subject or another natural person, processing necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller, legitimate interests of the controller or third party. It is essential that a proper legal basis is established during both the training and the use phases. At this point, it is important to note that identifying the «controller», as defined in the GDPR is a bit more complex in the context of AI. The controller may be the AI system's creator, the developer who trained it, the company selling it, or the company utilizing it, depending on the nature of the system, the

[6] Centre of Information Policy Leadership, (2020), Artificial Intelligence and Data Protection – How the GDPR Regulates AI, Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf

[7] EDPB' s reply to Sophie in't Veld's letter, (2019), Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf

reasons for which it is used, the stage at which it is utilized, and the degree of control each party has.

Meanwhile, the GDPR contains clauses that expressly highlight technologies or processing techniques that use AI elements, including the GDPR's rules regarding automated decision-making. The most relevant article to AI is Article 22 of the GDPR, which addresses automated decision-making. This clause, as will see in the below, combines a broad ban on automated decision-making with certain exceptions[8]. Article 22's first paragraph provides everyone the general right to be free from decisions that are entirely automated and have a substantial impact on the data subject or/and produce legal effects in relation to the data subject. However, even though the Article refers to a right provided to individuals, in reality, what this provision does, is that it poses data controllers a prohibition: automated decisions that impact data subjects are not permitted, unless they fall under one of the exceptions listed in paragraph 2. In order to apply Article 22 (1), there are four conditions that need to be met: 1) we need to have a decision, 2) that is solely based on automated processing, 3) that includes profiling, 4) that produces legal or significant effect to a data subject. The three exceptions to the general rule against the use of automated decision-making are outlined in paragraph 2 of Article 22. According to the provision, the general rule does not apply, when the processing upon which the decision is based a) is required in order for the data subject and a data controller to engage into or carry out a contract[9], b) is permitted by applicable Union or Member State law, which also specifies appropriate safeguards to protect the rights, freedoms, and legitimate interests of the data subject[10], c) is based on the data subject's explicit consent[11]. In the situations covered by Article 22(2)(a) and (c), Article 22(3) mandates appropriate safeguard measures, meaning that the data controller must put in place appropriate safeguards to protect the data subject's rights, freedoms, and legitimate interests in the situations covered by Article 22(2)(a) and (c). These safeguards must include the right to human

[8] STOA, Panel for the Future of Science and Technology, (2020), The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530
[9] Article 22 (2)(a) GDPR
[10] Article 22 (2)(b) GDPR
[11] Article 22 (2)(c) GDPR

intervention, the ability to voice one's opinion, and the ability to challenge the decision.

Lastly, the GDPR includes provisions that particularly address some of the commonly encountered challenges and potential dangers surrounding AI. Examples of these include the requirements for processing personal data in a manner that is lawful and fair, as well as the data minimization principle. The notion of fair processing, as defined in Article 5 (1)(a) of the GDPR, encompasses many processing methodologies and intersects with the requirement for transparency regarding AI technologies, while suggesting an analysis of whether the processing will have an unjustifiable negative effect on the parties concerned. According to EDPB's definition of fairness in its Guidelines on Data Protection by Design and Default: «Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject».[12] Controllers must constantly reevaluate their usage of AI and take into account the potential effects on individuals in order to maintain adherence to fair processing standards. Specifically, bias-free AI systems are necessary for fair processing. Unintentional historical bias, incompleteness, and poor governance models may be present in data sets used by AI systems (both for training and operation), while sustaining such prejudices may result in unintentional (in)direct discrimination[13]. The Dutch DPA has also brought attention to the fact that the issue of whether or not an AI's outcome is «fair» is closely tied to the particular circumstances at hand as well as the subjective perception of justice. As a result, the capacity to justify the decisions an AI system makes becomes even more crucial. According to the Dutch DPA, a controller must actively explain and provide evidence for the fairness of an algorithm and ensure that its application does not produce undesirable outcomes[14].

Article 5 (1)(c) of the GDPR stipulates the data minimization principle, which states that personal data must be «adequate, relevant, and limited to what is

[12] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

[13] Ethics Guidelines for Trustworthy Artificial Intelligence by the High-Level Expert Group on Artificial Intelligence (AI HLEG)

[14] Autoriteit Persoonsgegevens, (2019), Available at : https://autoriteitpersoonsgegevens.nl/actueel/ap-legt-focus-in-toezicht-op-datahandel-digitale-overheid-en-ai

necessary in relation to the purposes for which they are processed». By definition, AI systems require large volumes of data in order to function properly, especially throughout the training stage, while in many cases it could be impossible for them to function properly without being trained on a substantial amount of data in the first place. Although this could be seen as creating conflict between the use of AI systems and data protection law, the principle itself does not restrict the processing of data by referencing a specific amount or set of data – rather, it refers to what is «necessary» for the purposes of the processing. This happens because it is not always possible to accurately predict what data elements may be relevant to the desired outcome of the system in question. The definition of «necessary» personal data varies depending on the AI system and the purpose for which it is used. However, the GDPR's oversight in this area should not prevent AI designers from letting perfection stand in the way of their goals; after all, limiting personal data does not mean rendering the AI system useless, especially since not all AI systems are required to produce exact outcomes.

2. Introduction of the AI Act

The emergence of Artificial Intelligence (AI) has great potential to enhance social welfare but bears risks at the same time[15]. As part of its digital strategy, the EU wants to regulate artificial intelligence, aiming to lay down rules for the development, placement on the market, and use of this innovative technology. In April 2021, the European Commission proposed the first EU regulatory framework for Artificial Intelligence, *the so-called AI Act*.

2.1 Background – Objectives and Scope of the AI Act

The proposal of the AI Act came as a result of the political commitment by President von der Leyen in her political guidelines for the 2019-2024 Commission «A Union that strives for more»[16], that the Commission would introduce a legislation for a coordinated European approach on the human and ethical considerations of AI systems, that where already being used in a large extent throughout the European Union. This extensive use of this innovative technology had raised concerns among the European Parliament and the European Council, which kept expressing calls for legislative action to ensure a well-operating internal market for the aforementioned new technological systems. As a response, in February 2020 the Commission published a White Paper on AI – A European Approach on Excellence and Trust[17], setting out policy options on how to achieve both the promotion of AI technology, leading to technological innovation and addressing the risks associated with it.

So if a White Paper on AI already existed, what was the need for an «AI Act»? The proposal of the AI Act focuses on addressing in a more extensive way the risks associated with certain uses of AI technology and cultivating trust by proposing a legal

[15] Mazzini G., (2019), A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law, in A. DE FRANCESCHI, R. SCHULZE (eds), Digital Revolutions – New challenges for Law.

[16] https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_en_0.pdf

[17] European Commission, (2020), White Paper on Artificial Intelligence - A European approach to excellence and trust.

framework for trustworthy AI. The «AI Act» is a regulation based on EU values and fundamental rights and more specifically is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU) concerning the approximation of the provisions laid down by law to improve the functioning of the internal market[18].

The Act divides Artificial Intelligence into four risk categories according to a system's intended application, each of which requires a different degree of regulation: 1) Unacceptable risk, 2) High risk, 3) Limited risk, and 4) Minimal risk. "High-risk AI" is the category that the AI is more concerned about out of these four, as evidenced by the fact that Title 3 of the Act -which consists of five chapters- is entirely dedicated to "High-Risk AI Systems", analyzing which systems should be deemed high-risk, defining the fundamental requirements AI systems need to meet and the obligations of those who provide and use AI systems, describing the procedures that notifying authorities and notified bodies should follow and specifying the kinds of conformity assessments that are necessary.

Even though the AI Act is referred to as a "risk-based" scheme, in reality it contains, as we already mentioned above, only one category of risk ("high risk") that -at least on paper- is heavily regulated. According to Art. 5 of the AI Act -which addresses unacceptable-risk AI applications- AI applications that are "considered unacceptable as contravening Union values, for instance by violating fundamental rights" are prohibited. These include a) *subliminal techniques* employed by AI to significantly alter someone's behavior in a way that either causes or is likely to cause harm, either physical or mental[19], b) *manipulation* employed by AI taking advantage of the weaknesses of a certain group of people (minority, disability etc.) and significantly altering a person's behavior in a way that could endanger their physical or mental health[20], c) *social scoring* and d) "real-time" *remote biometric identification technologies* (with major exceptions). As we examine the AI risk categories in decreasing order of concern, we move to the second category, or high-risk application, which – as mentioned above- is the most regulated. Even though they are not thought

[18] STOA, Panel for the Future of Science and Technology, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020, Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530
[19] Art. 5 (1)(a) AI Act
[20] Art. 5 (1)(b) AI Act

to be so fundamentally objectionable to be banned, high-risk AI technologies are subject to a thorough certification regime. The Act distinguishes three different categories of high-risk AI technologies[21]: A) AI systems designed to be employed as a safety feature of a product, or as a product itself (e.g. toys, medical devices), that are already covered by the New Legislative Framework (NLF)[22] are listed in Annex II(A); other areas of harmonized EU law, such as boats, trains, etc., are listed in Annex II(B), B) an exhaustive list of eight "new" high-risk AI systems, which includes: i) critical infrastructures, such as transportation, that may endanger people's lives or health, ii) biometric identification systems, iii) educational and occupational preparation, such as automated exam scoring, which could impact an individual's ability to access education and pursue a career, iv) employment, workers management and access to self-employment, such as automated hiring, v) essential private and public services, such as automated systems for social benefits, vi) law enforcement systems that could interfere with people's fundamental rights, such as "pre-crime" detection, vii) mitigation, asylum and border control management, such as verification of authenticity of travel documents, viii) administration of justice and democratic processes, such as "robo-justice" and C) new sub-areas which, if they represent an equal or higher risk than the systems already covered, can be added to Annex III by the Commission through a delegated act. However, the Commission is not permitted to add completely new top-level categories. Article 52 of the AI Act provides a comprehensive definition of three "limited-risk" AI systems: i) chatbots, ii) emotion recognition and biometric categorization systems, and iii) systems generating "deepfake" or synthetic content. Here, the only obligations posed to the providers and users are to ensure transparency by disclosing instances of manipulating content through labeling. However, technically speaking, as well as in terms of how it overlaps with the GDPR, which already requires controllers processing personal data to be open about the use of automated decision-making and profiling, this has questionable

[21] Art. 6 AI Act

[22] Available at: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

usefulness[23]. The following chapters will provide a more thorough analysis of this issue. When it comes to chatbots, according to the Act, transparency obligations apply only to providers and not to users. It is imperative for providers to design a system that notifies users that they are interacting with a machine instead of a human. Concerning emotion ID and deepfakes, on the other hand, users are the only ones responsible for providing transparency. The AI Act's final risk category, "limited-risk," contains a few minimal transparency requirements for a select few "limited-risk" systems. Video games with AI capabilities and spam filters fall under this category. According to the Commission, these applications should be primarily regulated by voluntary codes of conduct[24].

2.2 Relationship between the AI Act and the GDPR

The AI Act and the General Data Protection Regulation (GDPR) are complementary regulations that address different aspects of AI and data protection within the European Union (EU). The GDPR focuses on data protection and privacy rights related to the processing of personal data, while the AI Act specifically targets the regulation of AI systems. Despite being separate regulations, there is overlap in their scope, particularly concerning the use of personal data by AI systems. AI systems operating within the EU must comply with both the GDPR's data protection requirements and any relevant provisions of the AI Act. The AI Act and GDPR aim to harmonize their requirements to ensure consistency and coherence in the regulatory framework governing AI technologies and data protection. Both regulations require organizations to conduct impact assessments to evaluate potential risks and implications of their AI systems and data processing activities. Compliance with both sets of requirements is crucial when developing or using AI systems that involve personal data. Both regulations emphasize ethical considerations in the development and deployment of AI systems, albeit from different perspectives. The GDPR includes principles such as fairness, transparency, and accountability in the processing of

[23] Edwards L., (2022) The EU AI Act: a summary of its significance and scope, Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf
[24] Art. 69 AI Act

personal data, while the AI Act incorporates ethical guidelines and requirements, such as human oversight and risk management, to ensure the trustworthy and responsible use of AI. Non-compliance can result in significant penalties, including fines and sanctions.

In summary, the relationship between the AI Act and GDPR reflects the EU's comprehensive approach to regulating AI technologies and protecting individuals' rights and freedoms regarding the processing of personal data in the digital age.

3. Comparative Analysis of the GDPR and the AI Act

It has been argued that the GDPR would be in conflict with both big data and Artificial Intelligence given that it is based on principles that are incompatible with the widespread application of AI to big data, including purpose limitation, data minimization, special treatment of «sensitive data» and the limitation on automated decisions. According to this opinion, the European Union would have to decide whether to abandon the GDPR or fall behind other information-based economies that can fully utilize big data and AI, like the USA and China[25]. However, as we will see below, it is realistic to argue that the GDPR could be interpreted in a way that satisfies both requirements: safeguarding data subjects and encouraging beneficial applications of AI technology.

3.1 Processing of personal data by AI systems

As stated in the European Commission's Communication on AI[26], Artificial Intelligence (AI) describes systems that exhibit intelligent behavior by analyzing their surroundings and acting, sometimes autonomously, to accomplish certain goals and can be found in both software and hardware systems. However, the EU's High-Level Expert Group (HLEG) on AI released a revised definition of AI in 2019 that covered its primary functions and related scientific fields[27]. This definition states that artificial intelligence (AI) systems are created by people and can take many different forms, including robotics, machine learning, and machine reasoning. Artificial intelligence (AI) can currently gather, process, and understand vast amounts of data, make judgments based on those decisions, and implement those decisions in variable degrees across all forms of AI. Four distinct qualities emerge from the capabilities of AI; they, however,

[25] Zarsky, Tal, (2017), Incompatible: The GDPR in the Age of Big Data, Seton Hall Law Review, Available at: https://ssrn.com/abstract=3022646

[26] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, COM (2018)

[27] High-Level Expert Group on Artificial Intelligence (HLEG), A Definition of AI: Main Capabilities and Disciplines, Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

are not just advantageous but also raise questions about fundamental rights. First, because AI depends on data, it is more competent to gather and analyze vast volumes of data. This raises privacy concerns by giving AI the ability to observe humans more closely, for example through biometric identification in public spaces[28]. Second, even though these data sets don't contain personal information in and of itself, AI may be used to deanonymize huge data sets by analyzing vast volumes of data, finding connections between them, and establishing connections between several AI systems[29]. Thirdly, AI can identify patterns of correlation within datasets without necessarily concluding that there is a cause and effect relationship. This is due to AI's ability to learn on its own, which increases its autonomy, as well as its improved ability to learn quickly and consider alternative courses of action[30]. As a result, by making decisions without disclosing the motivations, AI may generate novel solutions that are hard for humans to understand, thus leading to AI opaqueness. This opaqueness sometimes referred to as the "black-box phenomenon," significantly reduces AI's explainability. Fourthly, AI systems may produce discriminating outcomes if their training data contains prejudice.

3.2 Roles and responsibilities of actors under the GDPR and AI Act

It is theoretically unclear who of the parties from the AI Act will be the controller for purposes of the GDPR when personal data is processed by AI systems. Given the significant roles that providers and users typically play, one of these actors may be the controller for purposes of the GDPR. In the event that the controller uses AI systems to handle personal data, in addition to the duties mandated by the GDPR to ensure processing security[31], they will also need to adhere to additional requirements under the upcoming AI Act. The controller's responsibilities are determined by what role they will play in the AI Act.

---

[28] Communication COM(2020) 64 final of 19 February 2020 from the Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, p. 2; White Paper on Artificial Intelligence

[29] White Paper on Artificial Intelligence, COM (2020)

[30] High-Level Expert Group on Artificial Intelligence (HLEG), A Definition of AI: Main Capabilities and Disciplines, Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[31] Articles 24-31 GDPR

The majority of the obligations under the AI Act will fall on the providers, as it can be concluded after evaluation of the Act. A provider is defined as the person or organization that develops an AI system or has one produced with the intention of putting it on the market or putting it into service under its own brand or trademark under Article 3(2) of the AI Act. On the contrary, the majority of the responsibilities under the GDPR applied to the controllers. The legal definition of a data controller, as stated in Art. 4(7) GDPR, is any natural or legal person, public authority, agency, or other body that, either alone or in conjunction with others, determines the purposes and means of processing personal data. It can be concluded from this that while processing personal data via an AI system, the provider will also act as a controller. That is only the case, though, if the provider determines the means and purposes of the processing of personal data[32]. As a result, the provider would have to abide by the requirements set forth in the AI Act. These obligations would comprise, among others, the obligation to prepare technical documentation under Article 18 of the AI Act, to to guarantee that their systems go through the necessary conformity assessment under Article 19 of the AI Act and maintain the logs that their high-risk AI systems automatically generate under Article 20 of the AI Act. At the same time, it is imperative that the provider fulfills the controller's responsibilities under the GDPR, such as conducting a Data Protection Impact Assessment, as provided in Article 35 of the GDPR.

Nevertheless, there are also scenarios where providers do nothing more than act as vendors of AI systems and do not process any personal data. Under these circumstances, the supplier would not be considered a controller and would not be subject to GDPR obligations. The providers, however, need to comply with their responsibilities under the AI Act. Since the users determine the purpose and method of processing, they would be the controllers in this scenario rather than the providers, and they would be responsible for satisfying the controller's obligations under the GDPR. In the event that the providers process the personal data, it needs to be decided whether they will function more like joint controllers or, in accordance with Article 28 of the GDPR, assume the role of processor. It is especially crucial in this

[32] Article 4 (7) GDPR

situation to make sure they fulfill the transparency principle and let the data subjects know which of the two actors is in charge of which processing activity, according to Article 26 of the GDPR.

In today's world, where many businesses are progressively outsourcing their processes and having them completed by other businesses, these specific cases are probably going to be crucial[33]. In the event that the provider is contracted to handle personal data, they will be considered processors if the user is the only one who determines the goals and methods of the processing. The user could instruct the AI provider to finish the application procedure, for instance. According to the GDPR, in this scenario, the provider would be a processor and the user would be the controller. A corresponding processing contract and corresponding support obligations must be signed by the provider and the controller, respectively, if the provider is to function as a processor.

3.3 Data minimization

The GDPR's "data minimization" principle and the requirement to train the system data are two well-known contradictory features of the regulation and the processing of personal data by AI systems[34]. As mentioned above, massive volumes of data are necessary for AI systems to advance in intelligence. However, every phase of the AI system cycle of life must adhere to the GDPR's data minimization principle, which is incorporated into numerous organizational and technical measures[35]. As a result, artificial intelligence systems could only be trained with limited data, which could pose a serious disadvantage and hinder system development, which could impede the expansion of the internal market. Despite the fact that AI learning and training require vast volumes of data, the GDPR does not allow any exceptions. If data is reduced during the training of AI systems – as mandated by the GDPR – the quality of the outcome could deteriorate. Essential data sets, exceptions and important links

[33] Lacity M. et al., (2011), "Business Process Outsourcing Studies: A Critical Review and Research Directions,"
Journal of Information Technology 26, Available at: https://doi.org/10.1057/jit.2011.25
[34] STOA, Panel for the Future of Science and Technology, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020, Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530
[35] Recital 78 GDPR

could be missed as a result of data minimization, leading potentialy to biased, incomplete or misleading results. This issue is among the most crucial – if not the most crucial – to bring up when talking about AI systems and data protection. As a result, data minimization during the learning or training phase may be substituted by additional steps to guarantee a high level of security of personal data. Falsified findings are unacceptable under both the GDPR along with AI systems.

Goldsteen, Enzoy, Shmelkin et al.[36] made a proposal for a method that can lessen the volume and precision of input data that machine learning models utilize to make predictions. This method includes the minimization of data that is newly acquired for analysis (also known as runtime data) and not the data that was used to train the model. Their proposal for a method provides a simple and practical solution for addressing data minimization in existing systems, since it does not require retraining the model. The goal of this data minimization is to decrease the quantity and/ or accuracy of features gathered for analysis, which can be generalized or fully removed. A value is replaced by generalization with a less precise but semantically compatible value. This issue has also been addressed by the French data protection supervisory authority, CNIL, which suggests a similar course of action: It focuses on the AI system's learning phase and suggests that this phase be conducted with proper monitoring, with data being accessible to a limited number of individuals. In addition, further organizational and technical safeguards like pseudonymization are in place to guarantee the security of the learning data. Following this stage, there should be a larger minimization of data[37].

Even though the aforementioned methods provide solutions to some issues concerning the compatibility of AI systems to the data-minimization principle, a regulation addressing this conflict, could provide more legal certainty. However, the AI Act does not address this issue. The AI Act's Article 10's data governance provision is the only one that may resemble the data minimization clause.

[36] Goldsteen, A., Ezov, G., Shmelkin, R. et al., (2022)Data minimization for GDPR compliance in machine learning models. AI Ethics 2. Available at: https://doi.org/10.1007/s43681-021-00095-8

[37] CNIL, "AI: Ensuring GDPR Compliance" (2022), Available at: https://www.cnil.fr/en/ai-ensuring-gdpr-compliance

3.4 Transparency and the blackbox issue

Complex artificial intelligence problems are becoming easier for computer systems thanks to machine learning (ML) programming. Sadly, these systems continue to be characterized by their inherent opaqueness, making it challenging to "look inside" and understand how they operate[38]. The Black Box Issue in AI, which has theoretical, legal, and practical implications, is centered on opacity. This issue typically arises when deep learning and artificial neural networks are used in place of simple algorithms and when the input data and outcome are accessible, but the decision-making process is not disclosed. This technology's main drawback is that neither the system nor its creators can explain how the outcome was arrived at, which outweighs the benefits of utilizing it. At the same time, there is a chance that the outcomes of this technology will be inaccurate or biased, without always being able to determine the reason behind it[39].

From a practical standpoint, end users are unlikely to trust and relinquish control to machines whose inner workings they do not comprehend[40], while software engineers might not be able to step in to quickly and methodically enhance performance[41]. The Black Box Problem theoretically makes it challenging to assess whether artificial neural networks and biological brains are similar[42], as well as whether computers developed with machine learning should be regarded as truly intelligent[43].

---

[38] Zednik, C., (2021), Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. Philos. Technol, Available at: https://doi.org/10.1007/s13347-019-00382-7

[39] Savage N., (2022) “Breaking into the Black Box of Artificial Intelligence: Scientists Are Finding Ways to Explain the Inner Workings of Complex Machine-Learning Models, Available at: https://doi.org/10.1038/d41586-022-00858-1

[40] Burrell, (2016), How the machine ‘thinks’: Understanding opacity in machine learning algorithms. Big Data & Society, Available at: https://doi.org/10.1177/2053951715622512

[41] Hoffman et al., (2018), Metrics for Explainable AI: Challenges and Prospects, Available at: https://www.researchgate.net/publication/329587571_Metrics_for_Explainable_AI_Challenges_and_Prospects

[42] Buckner, (2018) C. Empiricism without magic: transformational abstraction in deep convolutional neural networks. Synthese 195, Available at: https://doi.org/10.1007/s11229-018-01949-1

[43] Zednik, (2018) Will Machine learning yield machine intelligence?, Available at: https://link.springer.com/content/pdf/10.1007/978-3-319-96448-5_23.pdf

From the perspective of data protection, a controller violates Article 5 of the GDPR, if they are unable to inform the data subject about the decision-making process. Article 22 of the GDPR – as mentioned above- regulates automated decision-making by AI systems and mandates that data subjects must be informed about the logic behind the processing of their personal data. Furthermore, Article 13(2)(f) (for cases that personal data are collected from the data subject) and 14(2)(g) (for cases that personal data have not been collected from the data subject) of the GDPR provide that in the event that automated decision-making involves profiling, the controller is required to provide the data subject with additional information at the time that personal data is obtained. This information must include meaningful details about the reasoning behind the profiling, as well as the importance and anticipated outcomes for the data subject. As a result, it is concluded that the processing of the data subject's information is not permissible under the GDPR, because the AI's method of arriving at the outcome is inexplicable. From a data protection standpoint, processing cannot occur without adhering to the concept of transparency. Consequently, the creation of artificial intelligence systems that employ these machine learning techniques is precluded.

Concerns about AI systems acting as black boxes have led to demands for increased AI ethics, trustworthiness, and transparency[44]. To address this issue, experts are already working on developing potential solutions. However, since AI learns from its surroundings and past mistakes, even programmers find it difficult to comprehend the internal reasoning and decision-making process of «intelligent» computers. Currently, the US Department of Defense is conducting an institutional project titled "Explainable Artificial Intelligence" (XAI), with the goal of developing a set of machine learning techniques that will: a) Increase the number of explainable models while preserving a high level of learning performance (prediction accuracy); and b) Make it possible for human users to comprehend, appropriately trust, and efficiently manage

[44] Yu Ronald and Gabriele Spina Alì, (2019), "What's Inside the Black Box? AI Challenges for Lawyers and Researchers," Legal Information Management 19, Available at https://www.researchgate.net/publication/332612588_What's_Inside_the_Black_Box_AI_Challenges_for_Lawyers_and_Researchers

artificial intelligence outputs[45], with the goal of replacing AI black boxes. XAI would assist AI in complying with the GDPR's provisions, while given that the GDPR requires that the relevant information has to be provided in a concise, transparent, intelligible, and accessible manner[46], XAI would be quite useful.

Experts and academics have already stressed that moral decisions cannot be slavishly delegated to algorithms. From this angle, guaranteeing complete accountability for computerized legal research and automated legal conclusions requires first understanding AI's underlying logic.

3.5 Profiling and automated decision making

Article 22 of the GDPR governs profiling and automated decision-making, and it is – as already mentioned above - one of the provisions that most closely approaches regulating the processing of personal data by AI systems. According to Article 4 (4) GDPR «profiling is the use of personal data by automated means to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or change of location». As was previously indicated, when a decision has a legal effect on or a significant impact on a natural person, Article 22(1) of the GDPR forbids automated decision-making, particularly automated decision-making based on profiling[47].

In its paper from 2017[48], Article 29 Working Party (WP) states that the purpose of profiling is to categorize individuals into groups based on shared characteristics: In general, profiling refers to the process of obtaining data about an individual (or group of individuals) and assessing traits or patterns of behavior to classify or group them. In particular, profiling involves analyzing and/or forecasting factors such as the individual's: task-performance ability; interests; or likely behavior.

---

[45] Gunning David (2018), 'Explainable Artificial Intelligence (XAI)', DARPA, [online]. Available at https://www.researchgate.net/publication/338039379_XAI-Explainable_artificial_intelligence

[46] Article 12 GDPR

[47] Article 22 GDPR

[48] Article 29 Data Protection Working Party, (2017) "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679", Available at: https://ec.europa.eu/newsroom/article29/items/612053/en

The possibilities for profiling have significantly expanded thanks to AI, big data, and the accessibility of vast computer power. In fact, when machine learning-based techniques are used on personal data, they frequently aim to yield conclusions—classifications, predictions, or decisions[49]. The information obtained by profiling should be regarded as personal data. In this relationship, it's important to distinguish between the general correlations that the learnt algorithmic model captures and the outcomes of using that model to describe a specific individual. It is easier to understand this concept, by taking into consideration, for example, a machine learning system that has acquired a model from a training set comprised of past college applications and their corresponding results. The system's training set includes personal data, such as student's name, age, economic condition and education. The algorithmic model links input values to a corresponding default likelihood, which is not personal data but group data. When applied to a new applicant's description, both the description and default risk represent personal data, with the first being collected data and the second inferred data. Inferred data concerning individuals under the GDPR should be considered personal data, with data protection rights applying. In automated inferences, data subjects have the right to access both input and output data. However, the right to rectification only applies to a limited extent. When processed by public authorities, review procedures should be considered, and private controllers should balance the right to rectify data with respect for autonomy. Data subjects have the right to rectification of inferred information when it is «verifiable» or the outcome of unverifiable or probabilistic inferences. Legal scholars argue that data subjects should have a right to «reasonable inference», which means that automated inferences should be reasonable and ethically and epistemically sound. This includes the right to challenge inferences made by AI systems, such as credit scores, and to ensure that the inferences are relevant and accurate. Controllers should be prohibited from using unreasonable inferences in their assessments or decisions, and they should demonstrate the reasonableness of their inferences.

[49] STOA, Panel for the Future of Science and Technology, (2020) The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530

Because it is so effective and saves labor and time, profiling can be quite advantageous for many sectors, both public and private (AI providers). Many tasks that would take significantly longer to complete if handled by a human can now be completed much more quickly due to profiling. However, profiling, and automated decision-making may present certain risks, including the possibility of injustices like exclusion or discrimination, from the standpoint of the data subject. For instance, the system can ignore data that might have produced different results due to an algorithmic error. Profiling and automated decision-making can only be used if there are no legal ramifications or major drawbacks. Moreover, under certain predetermined exceptional circumstances, decisions based on profiling may also be carried out automatically[50]. The General Data Protection Regulation (GDPR) encompasses more than just decisions made through automated processing or profiling; it also covers the data gathering process used to create profiles and the application of those profiles to specific individuals.

The scope of automated decision-making is varied, and it may arise from or partially overlap with profiling[51]. The capacity to make decisions solely through technology and without human intervention is known as solely automated decision-making. Any kind of data can be used as the basis for automated choices, including: deduced or inferred data, such as an already-created profile of the individual; data observed about the individuals; and data provided directly by the individuals in question. Profiling can be done independently of automated decision-making, and automated decisions can be produced with or without profiling. Nevertheless, automated decision-making and profiling are not always distinct processes. The way the data is handled can change something that begins as a straightforward automated decision-making process into one that is based on profiling.

On the other hand, AI Act does not specifically mention profiling or automated decision-making. However, according to Annex III of the AI Act, the regulation identifies as high-risk the AI systems that will conduct student assessments and AI systems that will make choices about hiring, human resource management, eligibility

[50] Article 22(2) GDPR

[51] Article 29 Data Protection Working Party, (2017) "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679"

for benefits or access to education, posing -as mentioned above- stringent requirements on them.

3.6 Security of processing and privacy by design

According to Article 25 (2) of the GDPR, controllers are required to implement the necessary organizational and technical safeguards to guarantee that the GDPR's criteria are met, both before and during processing operations, and that the data protection principles are effectively implemented. When processing data, controllers must, above all, take into account the dangers involved, and the kind and intensity of the processing. Data protection needs to be a main concern from the beginning of the design of AI systems, not something that is left until the very end of the system's development or use[52]. Systems and procedures known as technical and organizational measures are designed to guarantee access to and permanent processing of personal data. In the event of a loss, these protocols ought to facilitate the quick recovery of data. The information has to be pseudonymized and encrypted, if at all feasible. Lastly, since new risks could materialize or old ones could get significantly worse, processes for routinely reviewing and assessing the steps taken must be established[53].

According to Article 12 of the AI Act, high-risk AI systems must be designed and developed with features that allow for the automatic recording of events (also known as «logs»), while the system is in operation. These tracking capabilities need to conform to generally recognized standards or shared guidelines. This recording is mainly meant to provide evidence that the AI system's intended purpose has been followed for the duration of its life cycle and that its operation is monitored to determine whether a danger, as define by Article 65(1) of the AI Act, exists. The main goal of this precaution is to guarantee the AI system's operational security. For example, it might be incorporated into the GDPR as a supplement to the relevant organizational and technical measures listed in Article 32(1)(c) and (d) of the GDPR. At the same time, in the event of loss, data might be restored by using the records, while

[52] Centre of Information Policy Leadership, (2020) Artificial Intelligence and Data Protection – How the GDPR Regulates AI, Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf

[53] Article 32 GDPR

the efficiency of the technological and organizational measures might be regularly reviewed and evaluated using these records as a basis.

The GDPR's Article 5's data minimization and storage limitation principle, however, could conflict with the automatic recording of every system operation during the course of a high-risk AI system's processing of personal data, since record-keeping during the processing of personal data could lead to more risks for the data subject. Some of the issues that could arise from the automatic record-keeping in relation to the GDPR are the following: 1) the length of the AI system's life cycle is unknown, so most likely, an estimate of the life cycle would be required; 2) it could not be legal to store data for an indefinite amount of time because the goal will likely be fulfilled much sooner than the AI system's lifetime; 3) it might be possible to monitor the AI system's operation with fewer resources. As a result, the issues arising from data minimization and storage limitation principles need to be addressed and clarified before this provision can be added to the General Data Protection Regulation. Article 15 of the AI Act is a provision that is appropriate to guarantee the secure processing of personal data by AI systems and can be compared to Article 32 of the GDPR. It regulates the way that high-risk AI systems shall be designed and developed, in order to provide a suitable degree of accuracy, resilience, and cybersecurity, and to function reliably in those areas over the course of their lifetime. Similarly, in accordance with Article 32 of the GDPR, the risks associated with processing, specifically those arising from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed, must be taken into consideration when determining the appropriate level of security. The safeguards provided by the AI Act's Article 15 go even further in several areas since the Article even addresses the training that high-risk AI systems that keep learning even after being placed on the market, need to receive to avoid biased outputs. To guarantee the secure processing of personal data by AI systems, the provisions of Article 15 of the AI Act could potentially be incorporated into Article 32 of the GDPR or Article 32 of the GDPR could make reference to Article 15 of the AI Act.

3.7 Anonymization and Pseudonymization

Anonymization and Pseudonymization are among the most often cited safeguards for personal data. Both seek to uphold the data minimization principle while facilitating the thorough processing of personal data[54].

Unlike pseudonymization, anonymization is only stated in Recital 26 of the GDPR and is not specified within the Regulation. This means that anonymized data is exempted from the GDPR's provisions. Data is considered anonymous if it is «reasonably likely» that it cannot be connected to an identified or identifiable natural person, as stated in Recital 26 of the GDPR. In contrast to the GDPR's risk-based methodology, the Article 29 Working Party in its 2014 guidelines, seems to believe that no level of risk can be acceptable. In fact, the ideas of permanence, irreversibility, and impossibility advocate for a considerably stricter stance than the legal text itself. The Working Party's absolutist position suggests that anonymization should be permanent, notwithstanding Recital 26's acknowledgment that it can never be absolute due to factors like technological advancements. As a result of these conflicting views, there is no legal certainty regarding which test should be applied in practice[55].

In the GDPR, pseudonymization[56] (which does not involve a reduction in the amount of data) is crucial and is embodied in the data minimization principle. Pseudonyms and codes are used in place of specific data, typically names, and are listed in a separate list, with the help of which these data can be associated with the individual – data subject. Therefore, it is of great importance – in accordance with the GDPR's obligations – for these lists to be appropriately protected.

The AI Act also addresses the crucial role of data minimization in the processing of personal data. Pseudonymization or anonymization is specifically mentioned in the proposed AI Act as a way to secure and, if needed, mitigate these data that need further protection. According to Article 10 (5) of the AI Act, providers of

[54] STOA, Panel for the Future of Science and Technology, (2020), The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530

[55] El Emam Khaled, Cecilia Álvarez, (2015) A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques, International Data Privacy Law, Volume 5, Issue 1, Available at: https://doi.org/10.1093/idpl/ipu033

[56] Article 4 (5) GDPR

high-risk artificial intelligence systems may process special categories of personal data mentioned in Articles 9 and 10 of the GDPR, as long as they take appropriate measures to protect natural persons' fundamental rights and freedoms. These measures can include privacy-preserving measures, such as pseudonymization, or encryption where anonymization could significantly affect the purpose pursued. The AI Act maintains the requirement that anonymization should only be granted if doing so would materially undermine the goal of the processing in order to comply with the GDPR's objective of data minimization[57].

3.8 Enforcement mechanisms and sanctions

Adopting legal measures alone won't be enough to guarantee personal data privacy in Europe. In order for European data protection regulations to be effective, it is imperative that channels be established through which people can challenge infringements on their rights and pursue damages. Furthermore, it's crucial that supervisory authorities are able to impose penalties that are appropriate for the alleged infringement, effective in discouraging behavior, and fair. Individuals whose rights are at risk, known as data subjects, are able to defend their rights under data protection laws[58]. Nonetheless, other individuals who meet the standards set forth by national law may also act as data subjects' representatives when they exercise their rights (e.g. children). The national laws of the Contracting Parties are required by Article 12 of the Modernized Convention 108 to establish suitable remedies and punishments against violations of the right to data protection. In addition to the right to be compensated and to an efficient legal remedy, data subjects are entitled to file a complaint about suspected violations of the regulation with a supervisory body. The GDPR's Article 83 gives the supervisory authorities of Member States the authority to apply administrative fines for violations of the regulation. Article 83 further specifies the maximum amount of fines that can be imposed, the circumstances that national authorities consider before imposing a fine, and the level of such fines. As a result, the sanctions system is uniform throughout the EU. Nonprofit organizations that operate

[57] Article 10 (5) AI Act

[58] FRA European Union Agency for Fundamental Rights (2018), Handbook on European data protection law, pages 236-248

in the data protection sector may represent individuals in the exercise of their right to an effective remedy. In the event that the infringement results in substantial or non-material damage, the controller or processor is accountable. For violations of the regulation, the supervisory authorities have the authority to impose administrative fines of up to € 20,000,000 or, in the case of an undertaking, 4% of the total annual sales globally, whichever is higher. The following variables will determine the amount of the fine: whether the violation was deliberate or careless; whether mitigating actions were taken; whether the controller or processor complied with an established code of conduct or certification scheme; and whether the controller or processor cooperated with the supervisory authority. As a last resort and under specific circumstances, data subjects may file complaints with the ECtHR over infringement of data privacy law. Under the conditions specified in the Treaties, any natural or legal person has the right to petition the CJEU to have decisions made by the European Data Protection Board annulled.

On the other hand, according to the European Parliament's Briefing on Legislation in Progress – Artificial Intelligence Act[59], many critics of the Proposed Regulation point out that the AI Act lacks strong enforcement mechanisms since the Commission suggests letting providers self-evaluate when it comes to determining whether a certain situation qualifies as high-risk. Concerns are also expressed regarding the disproportionate devolution of regulatory authority to private European Standardization Organizations (ESOs), given the absence of democratic supervision, the inability of interested parties (consumer associations, civil society organizations, etc.) to impact the standards' creation, and the absence of legal recourse for standards that have already been adopted. Rather, they advise that a set of legally obligatory norms for high-risk AI systems be codified in the AI legislation (such as forbidding certain types of algorithmic discrimination), which ESOs can then define through harmonized standards. Moreover, they support enhancing democratic monitoring of the standardization process by European policymakers. Furthermore, another issue that critics point out is the fact that the AI Act is missing a key provision—that is, it does

[59] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

not grant individual enforcement rights. Ebers and others emphasize that people impacted by AI systems and civil rights organizations do not have the right to file a complaint with authorities overseeing market surveillance or to bring legal action against a supplier or user for noncompliance. Similar to this, Veale and Zuiderveen Borgesius caution that although some of the proposed legislation's sections seek to impose requirements on users of AI systems, they are not provided with a complaint or judicial redress process. Smuha and others suggest revising the proposal to include, among other things, a clear right of individual remedy and rights to involvement and engagement for EU citizens in relation to the choice to modify the list of high-risk systems in Annex III. It has also been emphasized that the current text does not have adequate channels for authorities to coordinate with one another, particularly when it comes to cross-border violationS. As a result, it is necessary to make clear the authority of the pertinent national authorities. Guidance on how to maintain compliance with information and openness standards while also safeguarding trade secrets and intellectual property rights would also be helpful. This is especially important to prevent inconsistent practices among Member States.

3.9 Challenges and potential conflicts between the GDPR and the AI Act

The AI regulation draft will regulate the usage, reuse, and sharing of data as another piece of protection legislation, but it will also heavily overlap with the GDPR (if nothing major changes throughout the legislative process)[60]. Due to this overlap, it becomes unclear how data users and holders might mitigate the legal and organizational risks associated with complying with these regulations. The massive overlap is caused by two factors: first, the extremely broad definition of artificial intelligence (AI) in Annex I of the AI Act, which includes «even the simplest search, sorting and routing algorithms[61]»; and second, the fact that the legal draft's «high risk»

[60] Grafenstein, M. v. (2022). Reconciling Conflicting Interests in Data through Data Governance: An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the AI Regulation Draft, as well as the GDPR). HIIG Discussion Paper Series 2022-2. Available at: https://doi.org/10.5281/zenodo.6457735.

[61] BDVA/ DAIRO position paper, Response to the European Commission's proposal for AI Regulation (2021), Available at: https://www.bdva.eu/sites/default/files/BDVA_DAIRO%20response-feedback%20AI%20Regulation_Final.pdf

AI-systems are defined for areas where the AI systems primarily process personal data (Annex III AI Regulation draft). This is largely the case for the areas as follows: biometric identification and classification of natural persons; education and vocational training; employment, workers' management, and access to self-employment; law enforcement; migration, asylum, and border control management; administration of justice and democratic processes (since the relevant laws and facts of a particular case interpreted by an AI system refer to natural persons involved in that case). The only area where personal data is not necessarily processed by AI systems is the area of critical infrastructures. Thus, the regulation would have a very independent scope of applicability in this area. However, in all the other areas mentioned above the GDPR is typically applicable, making the scopes of the two Regulations overlap.

When comparing the regulatory approaches of the GDPR and the AI Regulation draft, it becomes evident that both laws are quite similar, even at the very latest[62]. To begin with, the focus of both regulations is on the objective of processing personal data[63] or of using AI systems[64]. Additionally, both laws mandate that the regulation addresses to identification of the risks to fundamental rights based on the purpose of the data processing or AI system and implement organizational and technical measures to lower these risks to a level that complies with the law[65][66]. And this assessment recommences if the purpose changes[67][68].

Naturally, there are differences as well between the two Regulations. There are three basic differences: The first one is related to the scope of the two Regulations and more specifically, the GDPR's scope of application is determined by its cross-purpose and cross-sectoral approach, as well as by specific purposes or areas that are defined by the law. This means that rather than relying solely on predefined risks to fundamental rights, as defined by the purpose in one of these areas, the GDPR's protection effect unfolds early on, before a particular purpose poses a particular risk to

[62] Grafenstein, M. v.,(2022), Reconciling Conflicting Interests in Data through Data Governance: An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the AI Regulation Draft, as well as the GDPR). HIIG Discussion Paper Series 2022-2.
[63] Article 5 (1) (b) of the GDPR
[64] e.g. Article 7 (2) (a) of the AI Act draft
[65] Article 1 (2), 24, 25, 32 GDPR
[66] Article 7 (1)(b), 9 (2) AI Act
[67] Article 6 (4), 13 (3), 14 GDPR
[68] Article 43 (4), 28 (1)(c) AI Act

one or more fundamental rights[69]. Secondly, as stated in Article 16 of the AI Regulation draft, the draft's provisions are primarily directed at the providers—that is, in this case, the developers—of AI systems, and secondly at the actual users of the systems along with all intermediaries. By establishing developer liability in this manner, the legislator complies with a long-standing demand for the GDPR in the proposed AI Regulation[70]. Lastly, by requiring providers, users, and intermediaries to inform one another of any new risks that may arise[71], the legislator appears to be adopting a strategy also used by the REACH Regulation, which states that a major issue with risk identification and control is that the necessary information chain of all involved parties is not closed, at least not in a timely enough manner[72]. This is only partially accomplished under the GDPR, particularly with regard to the recently extended concept of joint controllership, whose application in legal interpretation is filled with several legal uncertainties[73].

In summary, the AI regulation draft's regulatory approach differs slightly from that of data protection, which may be disappointing. There's a need for more extensive protection beyond personal data processing, especially in areas like environmental protection. However, the laws' alignment in some areas may lead to redundant and disproportionate regulation[74].

---

[69] Grafenstein, Maximilian, (2020) Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III: Consequences for the Interpretation of the GDPR (And the Lawmaker's Room for Maneuver), Available at: https://ssrn.com/abstract=3840126 or http://dx.doi.org/10.2139/ssrn.3840126

[70] Sydow, Jörg and Braun, Timo, (2018), Projects as Temporary Organizations: An Agenda for Further Theorizing the Interorganizational Dimension, Forthcoming in International Journal of Project Management 36, Available at: https://ssrn.com/abstract=3116958 or http://dx.doi.org/10.2139/ssrn.3116958

[71] Articles 26 (2), 27 (4), and 29 (4) AI Act

[72] See https://ec.europa.eu/environment/chemicals/reach/reach_en.htm#:~:text=REACH%20(EC%201907%2F2006),authorisation%20and%20restriction%20of%20chemicals

[73] Gierschmann S, Schlender K, Stentzel R, Veil W, Gaitzsch P, Buchholtz G, Moser J (2017) Kommentar Datenschutz-Grundverordnung (E-Book). Bundesanzeiger Verlag, Köln

[74] von Grafenstein, Max & Heumüller, Julie & Belgacem, Elias & Jakobi, Timo & Smiesko, Patrick. (2021). Effective Regulation through Design – Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection by Design Approach. SSRN Electronic Journal. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3945471

Given this, it is even more crucial to explain how the two laws interact, particularly in the areas where their compliance assessments intersect. However, the reader is taken aback even in this regard. There are just two specific clauses in the proposed AI regulation that address this: 1) When processing is "strictly necessary for the purposes of ensuring bias monitoring, detection, and correction in relation to the high-risk AI systems," as stated in Article 10 (5) of the AI Act, even special categories of personal data may be processed, and 2) Article 29 (6) mandates that users of AI systems perform an eventual necessary data protection impact assessment in accordance with Article 35 of the GDPR, using the information supplied by the developer[75]. However, there is at least one additional potential for additional synergistic effects in the compliance efforts -even if not specifically stated- coordinating the AI conformity assessments and, specifically, the certification mechanisms of the GDPR.

3.10 Practical implementation and compliance considerations

Implementing and ensuring compliance with both the AI Act and GDPR requires careful consideration of various practical aspects. The fact that the AI Act may serve as a supplement or reinforcement to the GDPR with regard to the processing of personal data by AI systems is one of the major potential effects on the GDPR. This argument is based on the fact that several of the AI Act's provisions reflect the GDPR's principles.

As previously stated, the AI Act takes a risk-based approach and implements measures to limit the risks that AI systems bring. Developing a risk management system is one of these steps that needs to be done for AI systems in the future[76]. Throughout the AI's life cycle, the established risk management system must be updated and maintained[77]. It is clear from the above that there are many similarities between the risk management system and the GDPR's data protection impact assessment. Both processes seek to anticipate dangers that may affect the freedoms and rights of individuals and, if required, to reduce those risks as much as possible. The risks should be taken into consideration when designing the AI system so that they are

[75] Article 13 AI Act
[76] Article 10 AI Act
[77] Article 9 AI Act

either completely eliminated or present in a minor form. The latter is very similar to GDPR standards, Privacy by Design and Privacy by Default, which require the controller to use technological default settings to design data processing in a way that ensures data protection. Following the completion of the AI system, steps need to be taken to reduce additional (residual) risks. This point broadly relates to implementing organizational and technical safeguards mandated by the GDPR to guarantee the safe processing of personal data. Lastly, relevant information about potential dangers that should be anticipated needs to be provided[78]. Strong alignment with the GDPR is also evident here, which guarantees data subjects' access to information about the data processors' process. Here is where the AI Act takes things a step further by offering users the essential training regarding appropriate risk mitigation and control measures that cannot be excluded. Therefore, the controller has to make sure that a risk management system of this kind is in place when processing personal data using a high-risk AI system. To further secure the safety of personal data, the risks identified by the risk management system could be assessed and mitigated in accordance with data protection principles.

The establishment of a data governance and data management process for high-risk AI systems is another measure proposed by the AI Act, which likewise mirrors the fundamental ideas of the GDPR. By ensuring that only the appropriate data is processed in the appropriate quantities as needed, they should guarantee high data quality for training, validation, and test data preparation. The data must, above all, be complete, accurate, and representative[79]. This clause upholds the GDPR's accuracy principle, as described in Article 5 (1)(c) of the GDPR since it likewise emphasizes the timeliness and accuracy of personal data and strives for a similar high standard of quality. In addition, the data need to be examined for potential bias. In this sense, preventing discrimination and enhancing the protection of natural persons are goals shared by the GDPR and the AI Act. Therefore, the GDPR's Article 5's accuracy principle must be followed if personal data are contained in the training, validation, and test sets.

[78] Article 9 (4)(c) AI Act
[79] Article 10 AI Act

The AI Act mandates that a provider of a high-risk AI system creates technical documentation prior to releasing it onto the market. This documentation ought to demonstrate that the AI system satisfies every need that high-risk AI systems have to meet[80]. The AI Act's Annex IV outlines the requirements for the technical documentation's content. Aside from the AI system's goal and other relevant information, the logic involved, the AI's algorithms, the decision-making process regarding the individuals to whom the system is to be applied, and other content points must be mentioned. Every step of the AI system's life cycle requires that the technical documentation be updated and maintained up-to-date under Article 11 of the AI Act. The technical paperwork of the AI Act is comparable to that of the GDPR's data protection impact assessment, which, must also be carried out before processing personal data that is anticipated to be at high risk. The GDPR's accountability under Article 5 may be expanded in the context of high-risk AI systems processing personal data by incorporating into the DPIA the measures to mitigate the documented risks included in the technical documentation, which primarily concern personal data. These measures could also be further evaluated from a data protection perspective. The development of this kind of technical documentation may also be beneficial for controllers, since the risks identified therein may align with the dangers associated with processing personal data. Data protection risks might thus also be recorded and controlled through the integrated risk management system, which aims to reduce the risks listed in the technical documentation. For controllers, this would mean significant time and resource savings. Since the technical documentation is evaluated as part of the conformity assessment, a favorable evaluation of the assessment could also positively affect the DPIA's risks because some risk-minimization strategies have already been deemed adequate[81]. A crucial mandate of the AI Act, which is a more stringent legislation governing the use of AI, is the inclusion of additional information in the technical documentation. In line with this, comprehensive details regarding the way the AI operates and the degree of accuracy are compared to the intended goal of the actions taken to assist users in understanding the AI system's outcomes. In this case, it would seem acceptable to assume that it is known that the AI system's output

[80] Article 11 AI Act
[81] Article 43 AI Act, Annexes VI und VII AI Act

must be both accurate and understandable to humans. Additionally, this needs to be documented and disclosed to the individuals to whom the system is directed. This information is needed to comply with the information obligations set in Articles 12, 13 and 14 of the GDPR. An AI-powered controller would not be able to openly notify data subjects about how their data is being processed without interpretability. More legal certainty and transparency could result from incorporating this clause into the GDPR.

Integrating human oversight is one of the provisions of the upcoming AI Act that is already present in the GDPR in a similar manner[82]. The AI Act mandates that, in order to operate high-risk AI systems, a human supervisor must be involved in the process through suitable mechanisms such as human-machine interface. This person's main responsibility is to minimize risk and avoid mistakes. In order to achieve this, the supervisor must, above all, comprehend the system's architecture as well as the outcomes and how to interpret them. Furthermore, according to Article 14 of the AI Act, the supervisor ought to have the authority to determine whether the system needs to be disregarded or whether the system's outcomes have to be reversed. This clause appears somewhat familiar when compared to Article 22 of the GDPR, which mandates that the data subject has the right to request human intervention from the controller in cases of automated decision-making processes, including profiling[83]. This right can primarily guarantee the data subject that the data is of excellent quality and that they can trust the AI system to process it. But in the event that the AI system makes a mistake, the human supervisor might step in and reverse the results, using their training and experience to prevent discrimination or other negative outcomes for the data subject.

[82] Article 14 AI Act
[83] Article 22 (3) GDPR

4. Future Perspectives and Recommendations

The rapid advancements of AI and the need for effective regulation have led to the development of "AI regulatory sandboxes", in an attempt to balance innovation and data protection, which provide a controlled environment for experimentation while navigating the complex intersection of innovation, regulation, and societal impact, thereby enhancing the lives of others.

4.1 Balancing Innovation and Data Protection

These days, individuals are always pushing the boundaries of creativity and technology in an effort to create the next big thing and improve the lives of others. While this fiercely competitive race to the top is undoubtedly exciting, however, «changing lives» frequently results in unanticipated outcomes and may lead to unforeseen problems[84]. One of the basic roles of legislation is, of course, risk mitigation. However, the issue with regulating revolutionary technologies like Artificial Intelligence arises from a combination of the traditional approach to legislation, which is reactionary and too slow to be adopted and amended, and the highly unexpected and dynamic nature of the aforementioned technologies. On the other hand, technological opacity is another significant problem, which emphasizes the necessity of involving a range of individuals with expertise in the drafting of legislation, in order to ensure legal certainty[85].

Why, someone would wonder, the traditional way of legislation would not be efficient on AI? First off, compared to other technologies developed thus far, AI technology is undoubtedly more complex and has the potential to impact society in more areas, than any other form of technology can, since it is frequently classified as a disruptive technology and as such, it bears unpredictable dangers. Secondly, compared to other technologies, AI is far more opaque, in the sense that even a person with sufficient knowledge in the field of AI cannot always predict or/and comprehend the AI-generated results. Another key difference is the so-called AI regulation pacing

[84] Antunes, Freitas et al., Multidisciplinary Perspectives on Artificial Intelligence and the Law (2024). Available at: https://doi.org/10.1007/978-3-031-41264-6

[85] Kaal WA Dynamic regulation for innovation. (2016), Available at: https://doi.org/10.2139/ssrn.2831040

problem. When referring to the «pacing problem», we mean the notable gap between the rate of advancement in AI and the development of the necessary regulatory instruments. Lastly, a clearly stated legislation's aim is necessary for it to effective and fulfill its role in risk mitigation, since a well-written and functional legal text must address the widest variety of real-life situations possible.

The draft AI Act's definition of AI systems in Article 3 (1), which reads «a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with», goes a long way toward mitigating the aforementioned issues. However, as we already mentioned above, this broad definition comes with some flaws (e.g. fails to explain the distinction between AI and AI systems).

Annex I, which includes AI approaches and techniques like symbolic reasoning and reinforced learning and can be updated through delegated acts in line with Article 4 and Article 73 of the draft AI Act, is crucial to this definition. This is meant to solve the pacing problem and allow for faster reaction times in the event of technological advancement that is not covered by the legislation, yet it may not be quick enough given how long it takes for a delegated act to become effective. The European Parliamentary Research Service in its briefing notes that the pace issue has to be properly addressed and recommends «flexible instruments such as delegated acts, sunset clauses, and experimental legislation»[86].

These new regulatory tools are nothing new; they existed long before it became necessary to regulate AI[87]. They go by many different names and are frequently combined, but they all share a few characteristics: they are more flexible than traditional laws, they let in a wider range of stakeholders, and they give the regulator insightful input that helps them better understand the subject of the regulation and the advantages and disadvantages it entails. Regulatory sandboxes are without a doubt one of the technologies that attracted the greatest attention.

[86] Kritikos M (2019) Artificial intelligence ante Portas: legal & ethical reflections. Eur Parliament Res Serv, Brussels

[87] Ranchordás S (2014) Constitutional sunsets and experimental legislation: a comparative perspective. Elgar monographs in constitutional and administrative law series. Edward Elgar, Cheltenham, UK

4.2 Potential Areas for further legislative development

The AI Act aims to establish coordinated «regulatory sandboxes» for artificial intelligence, in order to promote AI innovation within the European Union. Under the watchful eye of the regulator, businesses can explore and experiment with new and innovative products, services, or business models by using a regulatory sandbox. In the long run, a regulatory sandbox promotes consumer choice, gives innovators incentives to test their ideas in a controlled setting, and helps regulators better understand the technology. Regulatory sandboxes must have the right legal framework in order to be successful but also carry the risk of being misused or abused[88].

Regulatory sandboxes are a type of regulatory instrument that allows companies to experiment with novel and innovative products, services, or businesses for a set amount of time under the supervision of the regulator. According to Article 53 of the AI Act, regulatory sandboxes in addition to promoting regulatory learning by creating experimental legal frameworks that guide companies in their innovation efforts under the supervision of a regulatory body, promote business learning through the creation and testing of innovations in real-world setting. The objective of the strategy is to increase regulators' comprehension of emerging technologies by facilitating experimental innovation within a framework of regulated risk and monitoring. In the EU, the sandbox approach has become increasingly popular as a tool to assist regulators in addressing the creation and application of innovative technologies, such as blockchain and artificial intelligence, in a variety of industries. Regulatory sandboxes are increasingly utilized in the transportation, energy, telecommunications, and health sector, as well as in the financial technologies industry. A more flexible approach to innovation and regulation in the high-tech industry is being favored by EU policymakers, who have proposed regulatory

[88] EPRS, European Parliamentary Research Service, (2022), Briefing «Artificial Intelligence act and regulatory sandboxes, Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf

sandboxes for testing surveillance solutions, established a framework for data access and use, and assisted start-ups in introducing challenging technologies to the market[89].

Regulatory sandboxes provide the industry with a number of advantages, such as helping regulators create appropriate policies for supervision, rule-making, and enforcement, encouraging collaboration amongst different stakeholders, and enabling innovators to create products and services that adhere to the legislation. This reduces risks and unforeseen consequences when introducing new technologies to the market and helps to the avoidance of potential legal issues. Additionally, regulatory sandboxes give users the chance to experiment with new technologies without having to adhere to all legal requirements – this is especially useful for innovations that don't fit into an established framework. But there's also a chance that these sandboxes may be misused. Critics contend that they may result in regulatory arbitrage, lowering safeguards to attract innovators, and jeopardizing consumer protection[90]. Critics also draw attention to the possibility that regulators would prioritize innovation over implementing sufficient safety measures to protect the general public and consumers. They also stress that while testing AI systems, private organizations processing personal data can deviate from the relevant data protection laws[91]. Lastly, if testing criteria in a regulatory sandbox differ significantly among Member States, there is a risk of fragmentation inside the EU single market. In general, regulatory sandboxes provide a setting for consumer choice and innovation, but there is a chance that they may be abused or misused.

Articles 53 and 54 of the draft AI Act introduce the concept of «AI regulatory sandboxes» as specific measures supporting innovation. The purpose of these sandboxes is to provide a controlled experimentation environment for innovative AI products and services during the development stage prior to their placement on the

[89] Mundell I., (2022), The ecosystem: Challenging tech? There's a sandbox for that, Science Business Network, Available at: https://sciencebusiness.net/news/start-ups/ecosystem-challenging-tech-theres-sandbox

[90] Allen H., (2020), 'Sandbox boundaries', Vanderbilt Journal of Entertainment & Technology Law . Available at : https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)652752

[91] Ranchordas, (2021), Experimental lawmaking in the EU: Regulatory sandboxes, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3963810

market[92]. The Regulation suggests creating standardized guidelines to guarantee consistent application throughout the EU and coordinating AI sandboxes at the national level. The competent authorities of the Member States are urged to create regulatory sandboxes and establish a fundamental structure for governance and supervision, under Article 53 of the draft AI Act. A single Member State, a number of Member States, or the European Data Protection Supervisor may establish these sandboxes, which need to be supervised by national competent authorities in compliance with the existing national and EU laws. Under applicable EU and Member States laws, participants in AI regulatory sandboxes are nevertheless accountable for any harm caused to third parties as a result of experimentation. The terms under which AI regulatory sandboxes will operate, including eligibility requirements, application process, selection process, participation and withdrawal, and participant rights and obligations, will be outlined in implementing acts[93]. The draft AI Act also makes clear how existing data protection laws and new horizontal AI rules interact. Member States must coordinate the functioning of AI regulatory sandboxes with their national data protection authorities or other competent authorities. For the purposes of creating AI systems that serve the public interest – such as preventing criminal offenses, promoting public health and safety, or protecting the environment – further processing of personal data in the AI regulatory sandbox is permitted[94].

Concerns regarding the AI idea of sandboxes have been voiced by experts, stakeholders, and academics. Some point out that because the proposed AI Act would not exempt participants from AI liability, innovative businesses would be deterred from taking part in these sandboxes[95]. Others want more information on the benefits of liability protection and feel that the draft's wording is ambiguous regarding what kind of regulatory relief innovators can receive. Although the proposed AI Act leaves room for one or more EU Member States to create an AI regulatory sandbox, it is

[92] European Commission impact assessment of the regulation on artificial intelligence, (2021), Available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence

[93] Article 53(6) AI Act

[94] Article 54 AI Act

[95] Truby J. and others, (2021), A sandbox approach to regulating high-risk artificial intelligence applications, Available at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence-applications/C350EADFB379465E7F4A95B973A4977D#fn18

entirely optional, thus various frameworks and guidelines may be applied across the EU, increasing the possibility that national sandboxing regulations will differ. The fact that AI developers may select EU Member States with looser sandbox regulations has also brought attention to forum shopping. Complexity is increased by the possible spread of overlapping regulatory sandboxes at the national and EU levels. Industry stakeholders want additional information about how European and national AI sandboxes interact, especially if it's possible to create multi-jurisdictional regulatory sandboxes. Standardization of sandboxes is also required to facilitate cross-border service delivery. The draft AI Act's data protection rules have drawn criticism from experts who worry that they may not comply with the «purpose limitation principle» established in the GDPR. In order to prevent future AI regulations from being implemented in conflict, the European Data Protection Supervisor and the European Data Protection Board advise defining the goals and scope of sandboxes, avoiding contradictions and potential conflicts with the GDPR, and finding a balance between European coordination and national processes.

Conclusions

To sum up, the analysis of the AI Act and the General Data Protection Regulation (GDPR) highlights the complex relationship that exists between promoting AI innovation and protecting people's privacy and data rights. It is clear from a thorough study and comparative analysis that both rules have the same goal of advancing technological innovation while defending the rights of persons. But there are subtleties when using these principles in the context of artificial intelligence, especially when it comes to data minimization, transparency, anonymization, and pseudonymization.

A key principle of the GDPR is data minimization, which attempts to restrict the amount of personal data that is gathered and processed to that which is absolutely required for a given purpose. The idea of data minimization is challenged by the fact that AI algorithms frequently need large datasets for training and optimization. Furthermore, maintaining openness in AI systems is crucial for developing responsibility and trust, while due to the fact that AI algorithms are inherently complex and opaque, there are worries regarding the "black box" problem, in which AI systems' decision-making processes remain opaque.

In the context of AI, anonymization and pseudonymization techniques—mandated by the GDPR to safeguard individuals' privacy—present new challenges. Although the goal of anonymization is to permanently alter data so as to avoid identification, the increasing power of AI algorithms raises the question of how successful traditional anonymization methods are against attacks that allow for re-identification, while pseudonymization techniques—which substitute identifying information with pseudonyms—must be carried out with caution to guarantee that re-identification is not possible.

As we move forward, it will be crucial to overcome these obstacles and strike a balance between the need to safeguard people's data rights and privacy and the necessity to advance AI innovation. The AI Act's planned regulatory sandboxes offer a possible solution to these challenges by offering a regulated setting that complies with GDPR regulations and encourages experimentation and innovation, however, to

reduce possible risks like regulatory arbitrage and insufficient data protection measures, regulatory sandboxes must be carefully designed and implemented.

Policymakers need to provide constant communication and cooperation between legal and technical experts top priority in order to guarantee that AI regulation is in line with the GDPR. For the purpose of creating complex legal frameworks that properly balance innovation and data protection, an interdisciplinary approach is essential, while in the same time, in order to update and improve regulatory frameworks in response to changing social requirements and technology breakthroughs, legislators should take a proactive and flexible approach to regulation.

Bibliography

Allen H., (2020), 'Sandbox boundaries', Vanderbilt Journal of Entertainment & Technology Law . Available at : https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)652752

Antunes, Freitas et al., Multidisciplinary Perspectives on Artificial Intelligence and the Law (2024). Available at: https://doi.org/10.1007/978-3-031-41264-6

Article 29 Data Protection Working Party, (2017) "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679", Available at: https://ec.europa.eu/newsroom/article29/items/612053/en

Autoriteit Persoonsgegevens, (2019), Available at : https://autoriteitpersoonsgegevens.nl/actueel/ap-legt-focus-in-toezicht-op-datahandel-digitale-overheid-en-ai

Buckner, (2018) C. Empiricism without magic: transformational abstraction in deep convolutional neural networks. Synthese 195, Available at: https://doi.org/10.1007/s11229-018-01949-1

Burrell, (2016), How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, Available at: https://doi.org/10.1177/2053951715622512

BDVA/ DAIRO position paper, Response to the European Commission's proposal for AI Regulation (2021), Available at: https://www.bdva.eu/sites/default/files/BDVA_DAIRO%20response-feedback%20AI%20Regulation_Final.pdf

Centre of Information Policy Leadership, (2020), Artificial Intelligence and Data Protection – How the GDPR Regulates AI, Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf

CNIL, "AI: Ensuring GDPR Compliance" (2022), Available at: https://www.cnil.fr/en/ai-ensuring-gdpr-compliance

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, COM (2018)

EDPB' s reply to Sophie in't Veld's letter, (2019), Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf

Edwards L., (2022) The EU AI Act: a summary of its significance and scope, Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf

El Emam Khaled, Cecilia Álvarez, (2015) A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques, International Data Privacy Law, Volume 5, Issue 1, Available at: https://doi.org/10.1093/idpl/ipu033

EPRS, European Parliamentary Research Service, (2022), Briefing «Artificial Intelligence act and regulatory sandboxes, Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf

European Commission, (2020), White Paper on Artificial Intelligence - A European approach to excellence and trust.

European Commission impact assessment of the regulation on artificial intelligence, (2021), Available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence

FRA European Union Agency for Fundamental Rights (2018), Handbook on European data protection law, pages 236-248

Gierschmann S, Schlender K, Stentzel R, Veil W, Gaitzsch P, Buchholtz G, Moser J (2017) Kommentar Datenschutz-Grundverordnung (E-Book). Bundesanzeiger Verlag, Köln

Goldsteen, A., Ezov, G., Shmelkin, R. et al., (2022)Data minimization for GDPR compliance in machine learning models. AI Ethics 2. Available at: https://doi.org/10.1007/s43681-021-00095-8

Grafenstein, Maximilian, (2020) Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III: Consequences for the Interpretation of the GDPR (And the Lawmaker's Room for Maneuver), Available at: https://ssrn.com/abstract=3840126 or http://dx.doi.org/10.2139/ssrn.3840126

Grafenstein, M. v., (2022), Reconciling Conflicting Interests in Data through Data Governance: An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the AI Regulation Draft, as well as the GDPR). HIIG Discussion Paper Series 2022-2. Available at: https://doi.org/10.5281/zenodo.6457735.

Gunning David (2018), 'Explainable Artificial Intelligence (XAI)', DARPA, [online]. Available at https://www.researchgate.net/publication/338039379_XAI-Explainable_artificial_intelligence

High-Level Expert Group on Artificial Intelligence (HLEG), A Definition of AI: Main Capabilities and Disciplines, Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Hoffman et al., (2018), Metrics for Explainable AI: Challenges and Prospects, Available at: https://www.researchgate.net/publication/329587571_Metrics_for_Explainable_AI_Challenges_and_Prospects

Kaal WA Dynamic regulation for innovation. (2016), Available at: https://doi.org/10.2139/ssrn.2831040

Kritikos M (2019) Artificial intelligence ante Portas: legal & ethical reflections. Eur Parliament Res Serv, Brussels

Lacity M. et al., (2011), "Business Process Outsourcing Studies: A Critical Review and Research Directions,"

Journal of Information Technology 26, Available at: https://doi.org/10.1057/jit.2011.25

Mazzini G., (2019), A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law, in A. DE FRANCESCHI, R. SCHULZE (eds), Digital Revolutions – New challenges for Law.

Mundell I., (2022), The ecosystem: Challenging tech? There's a sandbox for that, Science Business Network, Available at: https://sciencebusiness.net/news/start-ups/ecosystem-challenging-tech-theres-sandbox

Ranchordás S (2014) Constitutional sunsets and experimental legislation: a comparative perspective. Elgar monographs in constitutional and administrative law series. Edward Elgar, Cheltenham, UK

Ranchordas, (2021), Experimental lawmaking in the EU: Regulatory sandboxes, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3963810

Savage N., (2022) “Breaking into the Black Box of Artificial Intelligence: Scientists Are Finding Ways to Explain the Inner Workings of Complex Machine-Learning Models, Available at: https://doi.org/10.1038/d41586-022-00858-1

STOA, Panel for the Future of Science and Technology, (2020), The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530

Sydow, Jörg and Braun, Timo, (2018), Projects as Temporary Organizations: An Agenda for Further Theorizing the Interorganizational Dimension, Forthcoming in International Journal of Project Management 36, Available at: https://ssrn.com/abstract=3116958 or http://dx.doi.org/10.2139/ssrn.3116958

Truby J. and others, (2021), A sandbox approach to regulating high-risk artificial intelligence applications, Available at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence-applications/C350EADFB379465E7F4A95B973A4977D#fn18

von Grafenstein, Max & Heumüller, Julie & Belgacem, Elias & Jakobi, Timo & Smiesko, Patrick. (2021). Effective Regulation through Design – Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection by Design Approach. SSRN Electronic Journal. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3945471

Yu Ronald and Gabriele Spina Alì, (2019), “What’s Inside the Black Box? AI Challenges for Lawyers and Researchers,” Legal Information Management 19, Available at https://www.researchgate.net/publication/332612588_What's_Inside_the_Black_Box_AI_Challenges_for_Lawyers_and_Researchers

Zarsky, Tal, (2017), Incompatible: The GDPR in the Age of Big Data, Seton Hall Law Review, Available at: https://ssrn.com/abstract=3022646

Zednik, (2018) Will Machine learning yield machine intelligence?, Available at: https://link.springer.com/content/pdf/10.1007/978-3-319-96448-5_23.pdf

Zednik, C., (2021), Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. Philos. Technol, Available at: https://doi.org/10.1007/s13347-019-00382-7

Appendix