PRIVACY AND AI

PROTECTING INDIVIDUALS' RIGHTS IN THE AGE OF AI

FEDERICO MARENGO

PRIVACY AND AI

PROTECTING INDIVIDUALS IN THE AGE OF AI

FEDERICO MARENGO

Privacy and AI. Protecting Individuals in the Age of AI.

ISBN: 9798854287456 (printed edition)

First Edition: December 2023

CONTENTS

INTRODUCTION

Artificial intelligence (hereinafter AI) has brought many societal changes and is transforming the way to do business. AI systems are pushing the boundaries of machine capabilities, cutting down the time required to complete specific tasks, enabling the accomplishment of complex operations that exceed human capacity, and easing repetitive decision-making processes. In short, AI systems can provide a faster and cheaper method to solve everyday problems in various areas, for example, smart cities, fraud prevention, law enforcement, and autonomous driving. The opportunities offered by these technologies are countless. Yet, similar to what has happened with other innovations, AI solutions can have detrimental consequences for individuals and society. In particular, the processing of information using AI systems also entails risks to the rights and freedoms of individuals, such as the lack of respect for human autonomy, the production of material or moral harms, discrimination, and lack of transparency in the decision-making process.

Whereas these features reveal the potential of artificial intelligence to support most of the activities performed by individuals, it also triggers many crucial questions, in particular, regarding the adequacy and sufficiency of the EU legal framework on data protection to protect the rights and freedoms of individuals when their personal information is processed using AI systems.

This work attempts to discover the most critical challenges posed by the processing of personal data supported by AI systems, how the current European legal framework addresses these challenges, and it also proposes alternative pathways to better protect the rights of individuals without stifling innovation.

Since the entry into force of the General Data Protection Regulation (hereinafter GDPR) in 2018, there has been massive interest from researchers and industry stakeholders in data protection. The GDPR harmonised the regulatory landscape of data protection and introduced stringent requirements for the processing of personal data. Additionally, it is a technology-neutral regulation, which means that it was conceived to be flexible and adaptable to new technologies. It also included specific provisions concerning automated decision-making to provide more targeted protection against this particular way of processing.

When it comes to the interaction of AI and data protection, researchers dedicated much of their efforts to particular fields: the explainability of AI systems and the provisions concerning the right not to be subject to automated decisions established in the GDPR and also concerning the fairness of the decisions taken using AI systems.

Most reviewed materials provide highly detailed explanations about the legal concepts involved, present new interpretations, and offer recommendations about what should be done to improve individuals' general situation at the legislative level. However, there is in general a disconnection on how the legal concepts relate to operative aspects of data protection. For the adequate protection of individuals, the analysis cannot be only limited to legal texts and case law. It should also include non-binding documents such as guidelines, standards, and best practices that concretise and provide more detailed guidance on how the high-level principles stipulated in the laws and regulations governing the area should be translated into practical and operational requirements. This work attempts to bridge, on the one hand, the gap between the legislative and judicial interpretation and, on the other hand, the practical and operative aspects concerning the protection of personal data.

This work is structured in 5 chapters as follows. The first chapter, *Conceptualizing AI,* elaborates on the concept and importance of data, in particular personal data, for the development of AI systems and the conceptualization of artificial intelligence. The second chapter, *Data Protection Provisions Related to AI,* explains how personal data is protected in Europe. Starting with an overview of the fundamental legal texts that govern the area, it then assesses more in detail the relevant provisions of the GDPR that has a bearing with regard to the protection of personal data where the processing is made using AI systems. In particular, it elaborates on the impact of AI systems on the data protection principles and the lawful basis to process personal data. The third chapter, *Ensuring Individual Rights in AI,* provides an in-depth appraisal of the protection of individual rights by the GDPR when personal data is processed using AI systems. Whereas a large part of this chapter is devoted to the rights related to automated decision-making (together with its conceptualization, the exceptions and safeguards), the remaining rights listed by the GDPR are also evaluated. Particularly, rights derived from transparency obligations, the right to rectification, erasure, restriction, objection and portability are reviewed in the light of the challenges posed by the processing of personal data using AI systems. Furthermore, this chapter introduces the most important accountability mechanisms, which are also a crucial aspect regulated by the GDPR and essential to mitigating the risks posed by the processing of personal data using AI systems. The fourth chapter, *Overcoming the Limitations of the GDPR,* provides more details about the limitations of the current regime and explains how the weaknesses previously identified could be overcome. It focuses on two of the most important risks to the rights and freedoms of individuals: algorithmic transparency and fairness and discrimination. Finally, the fifth chapter, *Mechanisms to Further Mitigate the Risks Posed by AI Systems,* explores other measures to further reduce the risks presented by the use of AI systems to process personal data. In particular, it explores alternatives such as the creation of registers for AI systems, the introduction of the role of the AI ethical officer, the benefits of relying on standards on AI systems to fill legislative gaps, certifications, and codes of conduct for AI system operators, the provision of more powers to data protection authorities and the reliance on privacy by design measures to reduce the risks of AI systems.

In addition, it includes two Annexes. Annex I *Machine Learning Algorithms* provides an overview of the most common algorithms used in machine learning (supervised learning). Then, Annex II includes an *AI Act Readiness Checklist* that allows companies to review the obligations that the AI Act draft (EU Commission 2021 version) imposes on different AI operators.

CONCEPTUALIZING AI

Introduction

Artificial intelligence will definitively reshape the world in which we live. Artificial Intelligence is the science of training machines to perform human tasks. It uses concepts from statistics, computer science and many other disciplines, to design algorithms that process data, make predictions, and help make decisions. It establishes basic parameters regarding the data and trains the machine to learn by itself by identifying patterns using many layers of processing.

Though the term Artificial Intelligence was forged in 1956 by Minsky and McCarthy, it was not until recently that it acquired its full significance. Discussions about the potentialities and fears around AI are not new, but technical features characterize and distinguish the current period. In particular, the surge in artificial intelligence is mainly due to the enormous increase in computational power and the access to huge amounts of data to train machine learning models. Recent technological developments have facilitated the transmission, processing and storage of huge amounts of information. The borderless nature of the Internet along with the vast volume of communications, create new regulatory issues for states, mainly regarding national security and data protection. These developments underpin the recent increase in machine learning capabilities and justify the wide public attention on the matter.

This chapter proceeds as follows. Firstly, it accounts for the importance of data and its free flow for the development of AI. It attempts to disentangle what is meant by ‘data’ and it pictures the importance of the free flow of information in the digital economy. Secondly, it assesses the intricacies of artificial intelligence. As there is no universally agreed definition of AI, it draws on the most common meaning of the term and the proposal made by the European Commission in the AI Regulation (hereinafter, AIA), as well as its foundations, capabilities and limitations. Thirdly, it reviews some algorithmic models that are covered under the umbrella term of AI. The purpose of this part is not to provide a complete understanding of the mathematical underpinning of the models. Instead, it leans on the assumption that there is a broad misunderstanding regarding the current methods comprising AI and it attempts to explain concisely the methods developers usually employ, leaving aside their mathematical foundations. For this purpose, the methods are classified according to their capacity to explain how they work and how they produce the results since it provides the groundwork to evaluate which methods could be more intelligible for users lacking specific technical background.

1.- The importance of data for the development of AI

1.1.- The concept of data

Throughout history, humans have kept the information they produced in diverse material means. Primitive societies painted walls to convey messages, and later written text was recorded on papyrus or paper. Technology allowed the digitalisation of information, which converted analogue into digital information. The process of digitalisation brought countless benefits to societies because digitalised information is easier to store, replicate and transmit. Data also changed the business environment in many ways. The most obvious outcomes of the digitalisation of the economy were the reduction of transaction and communication costs, the decrease in the time required to design, produce and deliver manufactured goods or provide services, and the creation of a whole new array of internet-enabled services.

Data can be defined as 'machine-readable encoded information'[1] or, more simply, as digitalised information. It is a recent discovery that data has an intrinsic capacity to generate wealth for the owner of the information and the society as a whole. In this sense, data was considered an asset in itself[2] or the new oil. Therefore, there is an understanding that data is a resource that has inherent or potential value and, as such, it deserves appropriate protection, in particular, when the data is deemed personal data.

The acknowledgement of data as a valuable asset, demands the identification of its fundamental features. Several characteristics serve to contrast data with traditional assets. First, data is a *non-tangible asset*, as opposed to corporeal or material goods. At the same time, it allows physical storage, highlighting a difference with the traditional notion of services. Second, it is *easily transferable and replicable*. People can move information across borders, either in one direction or simultaneously to many places, or duplicate it very quickly without cost. Third, its *value increases with aggregation*. Many benefits emerging from data-enabled applications, such as big data algorithms or personal

[1] Herbert Zech, 'Data as a Tradeable Commodity' in Alberto De Franceschi (ed), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution* (Intersentia 2016) 53.

[2] Paul M Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2055, 2094.

ANNEX II – AI ACT READINESS CHECKLIST

AI Act Readiness Checklist

On 21 April 2021, the EU Commission officially released the draft proposal for the Regulation of Artificial Intelligence (AIA).[293] The proposal sets out a comprehensive new legal framework for AI that aims at addressing a broad variety of challenges frequently associated with these technologies.

This readiness checklist rearranges the obligations imposed by the AIA draft on the operators of AI systems, taking into account **the EU Commission 2021 draft version.**[294] Amendments introduced by the Council or the Parliament are not included in this checklist.

Considering the provisions of the AIA draft proposal will give AI operators a competitive advantage, since they will be better placed to

[293] For simplicity, in this annex the AIA draft will be simply referenced as AIA.

[294] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM/2021/206 final

TABLE B – AI PROVIDERS

1.- PROHIBITED AI PRACTICES	
1.1.- Ensure that you do NOT place on the market or put into service or use an AIS that:	
- deploys subliminal techniques beyond a person's consciousness to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm (art. 5(1)(a) AIA)	☐
- exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm (art. 5(1)(b) AIA)	☐
- evaluates or classifies the trustworthiness of persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics (art. 5(1)(c) AIA): - by public authorities or on their behalf; - with the social score leading to detrimental or unfavourable treatment of certain persons or whole groups thereof: - (i) in social contexts which are unrelated to the contexts in which the data was originally generated or collected; and/or - (ii) that is unjustified or disproportionate to their social behaviour or its gravity	☐
- carries out 'real-time' remote biometric identification (RBI) systems in publicly accessible spaces for the purpose of law enforcement (art. 5(1)(d) AIA)	☐
1.2.- You can use of real time remote biometric identification on public spaces for law enforcement purposes ONLY if:	
- the use is strictly necessary for one of the following objectives: - (i) the targeted search for specific potential victims of crime or missing children; - (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; - (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable by a detention order for a maximum period of at least three years (art. 5(1)(d) AIA)	☐
- you considered the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system (art. 5(2)(a) AIA)	☐
- you considered the consequences of the use of the system for the rights of all persons concerned (art. 5(2)(b) AIA)	☐

- you implemented safeguards, particularly concerning the temporal, geographic and personal limitations (art. 5(2) in fine AIA)	☐
- you ensured a procedure to request for any individual use a prior authorisation granted by a judicial or an independent administrative authority (art. 5(3) or (4) AIA)	☐

If your AIS performs any of the above-mentioned actions and it is not covered by the exceptions concerning real time remote biometric identification, you are liable to the highest fines the AIA establishes: up to EUR 30M or 6% or the total annual global turnover.

2.- HIGH RISK AI SYSTEMS (HRAIS)	
2.1.- Identification of HRAIS	
Complete either 2.1.1 or 2.1.2 as appropriate	
2.1.1.- Safety Components	
Evaluate whether your AIS	
(a) is intended to be used as a safety component of a product, or is itself a product, covered by the EU harmonisation legislation listed in Annex II; AND (b) the product whose safety component is the AIS, or the AIS itself, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II (art. (6)(1) AIA)	☐
2.1.2.- HRAIS listed in art. 6(2) AIA and Annex III AIA	
Evaluate whether your AIS is intended to be used:	
- for the 'real-time' and 'post' RBI of persons (point 1(a) Annex III AIA)	☐
- as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity (point 2(a) Annex III AIA)	☐
- for determining access or assigning persons to educational and vocational training institutions (point 3(a) Annex III AIA)	☐
- for assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions (point 3(b) Annex III AIA)	☐
- for recruitment or selection of persons, e.g., advertising vacancies, filtering applications, evaluating candidates in interviews or tests (point 4(a) Annex III AIA)	☐
- for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behaviour of persons in such relationships (point 4(b) Annex III AIA)	☐
- by public authorities or on behalf of public authorities to evaluate the eligibility of persons for public assistance benefits and services, and to	☐

grant, reduce, revoke, or reclaim such benefits and services (point 5(a) Annex III AIA)	
- to evaluate the creditworthiness of persons or establish their credit score, except where AIS are used by small scale providers for themselves (point 5(b) Annex III AIA)	☐
- to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid (point 5(c) Annex III AIA)	☐
- to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts (point 8(a) Annex III AIA)	☐
- for any other purpose that the Commission has included according to Art. 7 AIA	☐
Evaluate whether your AIS is intended to be used by law enforcement authorities:	
- for making individual risk assessments of persons to assess the risk of a person for offending or the risk for potential victims of criminal offences (point 6(a) Annex III AIA)	☐
- as polygraphs and similar tools or to detect the emotional state of a person (point 6(b) Annex III AIA)	☐
- to detect deep fakes as referred to in article 52(3) AIA (point 6(c) Annex III AIA)	☐
- for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences (point 6(d) Annex III AIA)	☐
- for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling or assessing personality traits and characteristics or past criminal behaviour of persons or groups (point 6(e) Annex III AIA)	☐
- for profiling of persons in the course of detection, investigation or prosecution of criminal offences (point 6(f) Annex III AIA)	☐
- for crime analytics (point 6(g) Annex III AIA)	☐
Evaluate whether your AIS is intended to be used by competent public authorities in migration, asylum and border control management:	
- as polygraphs and similar tools or to detect the emotional state of a person (point 7(a) Annex III AIA)	☐
- to assess any risks posed by a person who intends to enter or has entered into the territory of a MS (point 7(b) Annex III AIA)	☐
- for the verification of the authenticity of travel documents and supporting documentation of persons and detect non-authentic documents (point 7(c) Annex III AIA)	☐
- for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the applicant (point 7(d) Annex III AIA)	☐

If your AI system is intended for one or more of the purposes listed in 2.1.1 or 2.1.2, you must complete the table below.