UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

Postgraduate Programme in

«LAW AND INFORMATION AND COMMUNICATION TECHNOLOGIES»

Academic year 2021 – 2022

LLP ERASMUS PROGRAMME: UNIVERSITY OF REGENSBURG

FACULTY OF BUSINESS, ECONOMICS AND MANAGEMENT INFORMATION SYSTEMS

MASTER THESIS

Alkisti Kostopoulou (R.N.: MDI2023)

ARTIFICIAL INTELLIGENCE AND PERSONAL DATA: Topical issues on the occasion of the EU AI ACT

Supervisors:

S. Gritzalis (University of Piraeus), **G. Pernul** (University of Regensburg)

Regensburg, July 2022

TABLE OF CONTENTS

List of Abbreviations

AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
(EU) AI ACT	(EU) Artificial Intelligence Act (i.e. the Proposal for the new Regulation)
Art. 29 WP	Article 29 Working Party ("The Working Party on the Protection of Individuals with regard to the Processing of Personal Data")
BfDI	The Federal Commissioner for Data Protection and Freedom of Information of Germany (German: "Bundesbeauftragter für den Datenschutz und die Informationsfreiheit")
CFR	(EU) Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
EDBP	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
GAS	Software for biometric facial identification („Gesichtserkennungssoftware")
GDPR	General Data Protection Regulation (i.e. 2016/679 EU Regulation)
IoT	Internet of Things
LED	Law Enforcement Directive (i.e. 2016/680 EU Directive)
PNR	Passenger Name Record, Passenger Name Record Directive (2016/682 EU Directive)
RBI	Remote Biometric Identification
SIS II	Second generation Schengen Information System
SNARC	Stochastic Neural Analog Reinforcement Calculator
SRI	Secure, Reliable and Intelligent
TFEU	Treaty on the Functioning of the European Union
UNHCR	United Nations High Commissioner for Refugees
VIS	Visa Information System
WEF	World Eonomic Forum

List of Graphs

Summary

The Proposal for a European Regulation laying down harmonised rules on artificial intelligence ("Artificial Intelligence Act" or "AI ACT") and amending certain union legislative acts also regulates issues related to personal data although a modern legislation already applies [Regulation 2016/679 ("General Data Protection Regulation", "GDPR"), Directive 2016/680 ("Law Enforcement Directive", "LED") etc]. The question is why it is necessary to clarify such issues when there is already such recent legislation as the GDPR and the LED? Why have the European Parliament and the Council put forward such a proposal for a detailed regulation on artificial intelligence? In this regard: (a) Are the GDPR and the LED up to date to address artificial intelligence ("AI")? Are they suitable and sufficient? If not, what is still missing? What is not yet covered? (b) Perhaps the European Union ("EU") simply seeks to familiarize European citizens with artificial intelligence? How does the public perceive the use of artificial intelligence and data protection?

To answer the above, we present the concept and prehistory of AI and the EU legal ethics which are in place so far. We will further address the issues of biometric identification for law enforcement purposes and profiling of individuals' creditworthiness and social scoring as follows: Initially, a theoretically approach will take place and then a comparative analysis of the existing legal framework for the protection of personal data and the Proposal of the AI ACT. Finally, research will be carried out on German and Greek students, in order to evaluate if they are familiarized with issues related to processing personal data using AI systems.

From all the above, it becomes clear that the existing framework is adequate and appropriate for the protection of personal data. However, this does not underate the value of the Act, which, despite any failures in the text, can, by providing for appropriate technical and organisational measures, contribute to the principle of accountability. Its contribution will also be decisive in familiarising Europeans with the above concepts of data protection and automated data processing, as it has not yet been achieved.

Summary in Greek

Στο κατώφλι της 5ης βιομηχανικής επανάστασης είναι ήδη εφικτή και εφαρμόσιμη η χρήση τεχνητής νοημοσύνης σε πλείστους τομείς. Χαρακτηριστικά παραδείγματα αποτελούν η βιομετρική ταυτοποίηση του ατόμου (μέσω δακτυλοσκόπησης, ιριδοσκόπησης ή ανθρωπομετρίας), η χρήση λογισμικού για την αναγνώριση της συναισθηματικής κατάστασης του ατόμου, η κατάρτιση προφίλ για την πιστοληπτική ικανότητα των οφειλετών, για την επιλεξιμότητα ωφελουμένων (π.χ. για κοινωνικές παροχές), για την πρόσληψη υποψηφίων εργαζομένων κ.α.. Σε όλες τις ανωτέρω περιπτώσεις ανακύπτουν σημαντικά ζητήματα προστασίας προσωπικών δεδομένων. Για τον λόγο αυτό απαιτείται η εφαρμογή ενός κατάλληλου νομικού πλαισίου, ώστε αφενός να προστατεύονται τα προσωπικά δεδομένα και αφετέρου να καλλιεργείται η εμπιστοσύνη των ατόμων σε καινοτόμες εφαρμογές της τεχνητής νοημοσύνης, που στόχο έχουν να διευκολύνουν την καθημερινότητα.

Στην Ευρωπαϊκή Ένωση σήμερα, για την προστασία των προσωπικών δεδομένων εφαρμόζεται ο Κανονισμός (ΕΕ) 2016/619 (στο εξής «Γενικός Κανονισμός Προστασίας Δεδομένων» ή «ΓΚΠΔ»), ο οποίος πλαισιώνεται από έτερα νομοθετήματα, όπως η Οδηγία (ΕΕ) 2016/680 για την προστασία δεδομένων στο πλαίσιο πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων (στο εξής «Αστυνομική Οδηγία») κ.α. Τα συγκεκριμένα νομοθετήματα είναι τεχνολογικά ουδέτερα, με αποτέλεσμα να εφαρμόζονται τόσο σε μη αυτοματοποιημένες, όσο και σε αυτοματοποιημένες επεξεργασίες δεδομένων.

Δεδομένου ότι η ανάπτυξη και η εφαρμογή της τεχνητής νοημοσύνης σήμερα είναι σημαντική, κρίθηκε από την Ευρωπαϊκή Ένωση, ότι απαιτείται να ρυθμιστούν συνολικά σε ένα νομοθέτημα ζητήματα που άπτονται της χρήσης συστημάτων τεχνητής νοημοσύνης. Για τον λόγο αυτό κατατέθηκε Πρόταση Κανονισμού για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη (στο εξής «Πράξη για την Τεχνητή Νοημοσύνη» ή «Πράξη»). Μελετώντας το κείμενο της Πράξης παρατηρεί κανείς, ότι μεταξύ άλλων ρυθμίζονται και συναφή ζητήματα προστασίας προσωπικών δεδομένων. Σύμφωνα με την αιτιολογική έκθεση της Πράξης, αυτή θα είναι πλήρως εναρμονισμένη με το ισχύον νομικό πλαίσιο για τα προσωπικά δεδομένα και θα λειτουργεί συμπληρωματικά

με αυτό. Ωστόσο, ανακύπτει το ερώτημα, γιατί κρίθηκε, ότι απαιτείται περαιτέρω ρύθμιση σχετικά με τα προσωπικά δεδομένα, εφόσον υπάρχει ήδη ένα εξειδικευμένο και σύγχρονο νομικό πλαίσιο γι' αυτά. Συναφώς θα εξεταστεί, αν αυτό το νομικό πλαίσιο (εν. ΓΚΠΔ κλπ) είναι κατάλληλο και επαρκές για την επεξεργασία δεδομένων με αυτοματοποιημένα μέσα καθώς και αν σκοπός του νομοθέτη ήταν με την νέα Πράξη να εξοικειώσει τους Ευρωπαίους πολίτες με την χρήση της τεχνητής νοημοσύνης.

Κατόπιν των ανωτέρω, ακολουθείται η εξής μεθοδολογία. Καταρχάς καταγράφονται ορισμένες επεξεργασίες προσωπικών δεδομένων οι οποίες λαμβάνουν χώρα με την χρήση συστημάτων τεχνητής νοημοσύνης. Στη συνέχεια κρίνεται η νομιμότητά τους με βάση το υπάρχον νομικό πλαίσιο (ΓΚΠΔ και Αστυνομική Οδηγία) και σχετική επίκαιρη νομολογία (συμπεριλαμβανομένων αποφάσεων των αρχών προστασίας προσωπικών δεδομένων). Για τους σκοπούς της παρούσας η νομολογία προέρχεται είτε από θεσμικά όργανα της Ευρωπαϊκής Ένωσης, είτε από την Ελλάδα και τη Γερμανία. Στη συνέχεια κρίνεται η νομιμότητα των συγκεκριμένων επεξεργασιών με βάση τις διατάξεις της Πράξης για την Τεχνητή Νοημοσύνη. Κατόπιν, γίνεται συγκριτική επισκόπηση του υφιστάμενου νομικού πλαισίου (εν. ΓΚΠΔ κλπ) σε σχέση με την Πράξη (με αρωγό και τη νομολογία), αναζητώντας ομοιότητες και διαφορές μεταξύ αυτών. Τέλος, παρατίθενται τα αποτελέσματα από τη διεξαγωγή έρευνας σε Έλληνες και Γερμανούς φοιτητές, προκειμένου να καταγραφεί η αντίληψη ενός δείγματος Ευρωπαίων πολιτών σε σχέση με ζητήματα προσωπικών δεδομένων και τεχνητής νοημοσύνης.

Αναλυτικά, αρχικά εξετάζεται η έννοια της τεχνητής νοημοσύνης και η προϊστορία της. Για να γίνει κατανοητή η λειτουργία της τεχνητής νοημοσύνης είναι χρήσιμη η αναφορά στη μελέτη των εννοιών της νόησης, της λογικής και, κατ' επέκταση, του συλλογισμού εκ μέρους της φιλοσοφίας και της επιστήμης από την αρχαιότητα μέχρι και σήμερα, καθώς ο συλλογισμός αποτελεί πρόκριμα της τεχνητής νοημοσύνης, η οποία αναπτύχθηκε μόλις στα μέσα του 20ου αιώνα.

Επίσης, εξετάζονται δεοντολογικοί κανόνες για την τεχνητή νοημοσύνη τους οποίους έχουν καταγράψει τα θεσμικά όργανα της Ευρωπαϊκής Ένωσης και προοιωνίζονται τη νέα Πράξη. Κατόπιν αναλύονται καίριες διατάξεις του ΓΚΠΔ και της Αστυνομικής Οδηγίας.

Στη συνέχεια, μελετώνται ορισμένες επιμέρους επεξεργασίες προσωπικών δεδομένων που λαμβάνουν χώρα με τη χρήση συστημάτων τεχνητής νοημοσύνης και συγκεκριμένα: η εξ αποστάσεως βιομετρική αναγνώριση προσώπων και η κατάρτιση προφίλ για λόγους αξιολόγησης της πιστοληπτικής ικανότητας και της κοινωνικής βαθμολόγησης των υποκειμένων. Αρχικά, εξετάζεται η εξ αποστάσεως βιομετρική ταυτοποίηση προσώπων σε δημόσια προσβάσιμους χώρους για σκοπούς επιβολής του νόμου. Για τον λόγο αυτό μελετάται η έννοια της βιομετρικής ταυτοποίησης και στη συνέχεια σχετικές αποφάσεις των αρχών προστασίας προσωπικών δεδομένων και νομολογία που τυχόν υπάρχει και σχετίζεται με το συγκεκριμένο θέμα άμεσα ή έμμεσα. Επίσης, μελετώνται και εφαρμόζονται οι σχετικές διατάξεις της Πράξης και λαμβάνει χώρα συγκριτική επισκόπηση με την Αστυνομική Οδηγία. Αντίστοιχη διαδικασία ακολουθείται και στις επόμενες επεξεργασίες, δηλαδή την κατάρτιση προφίλ για λόγους πιστοληπτικής ικανότητας και κοινωνικής βαθμολόγησης, όπου συναφώς, συγκρίνεται η Πράξη με την κείμενη νομοθεσία.

Τέλος, παρατίθεται η μεθοδολογία και τα αποτελέσματα έρευνας που διεξήχθη, προκειμένου να αναδειχθεί κατά πόσον οι Ευρωπαίοι πολίτες είναι εξοικειωμένοι με τις έννοιες των προσωπικών δεδομένων και της τεχνητής νοημοσύνης και εν τέλει με την επεξεργασία προσωπικών δεδομένων με χρήση συστημάτων τεχνητής νοημοσύνης.

Συμπερασματικά, η παραπάνω συγκριτική μελέτη της Πράξης για την Τεχνητή Νοημοσύνη σε σχέση με το υφιστάμενο νομικό πλαίσιο για τα προσωπικά δεδομένα αναδεικνύει, ότι το πλαίσιο αυτό (εν. ΓΚΠΔ κλπ) δύναται να ανταποκριθεί πλήρως στις ανάγκες της επεξεργασίας με αυτοματοποιημένα μέσα. Το γεγονός ότι είναι τεχνολογικά ουδέτερο το καθιστά προσαρμοστικό στην πάροδο των ετών και την αλματώδη εξέλιξη της τεχνολογίας. Ωστόσο, η επάρκεια του υφιστάμενου πλαισίου δεν αναιρεί τη σημασία της Πράξης. Παρά των όποιων επιμέρους τροποποιήσεων χρήζει το κείμενο της Πράξης, η συμβολή της στο υφιστάμενο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων είναι ιδιαιτέρως σημαντική. Η Πράξη προβλέπει την εφαρμογή εξειδικευμένων τεχνικών και οργανωτικών μέτρων κατά τη χρήση συστημάτων τεχνητής νοημοσύνης και, ως εκ τούτου, δύναται να συμβάλει στην τήρηση της αρχής της λογοδοσίας εκ μέρους των υπευθύνων εξεργασίας. Η λογοδοσία αποτελεί μία εκ των θεμελιωδών αρχών του ΓΚΠΔ

και συνίσταται στην ευθύνη του υπευθύνου επεξεργασίας να συμμορφωθεί με τον ΓΚΠΔ και να αποδείξει αυτή του τη συμμόρφωση. Η λεπτομερής αναφορά, επομένως, τεχνικών και οργανωτικών μέτρων στο κείμενο της Πράξης υποβοηθά τον υπεύθυνο επεξεργασίας μεταξύ άλλων στην συμμόρφωσή του με το δίκαιο των προσωπικών δεδομένων και την ευχερή απόδειξη αυτής. Περαιτέρω, η Πράξη είναι ιδιαιτέρως σημαντική για την Ευρώπη και τους πολίτες της, καθώς η εξοικείωση των Ευρωπαίων με την τεχνητή νοημοσύνη και κατ' επέκταση η καλλιέργεια κλίματος εμπιστοσύνης σε νόμιμες επεξεργασίες που λαμβάνουν χώρα με αυτοματοποιημένα μέσα αποτελεί έναν στόχο που δεν έχει ακόμα επιτευχθεί.

1. Introduction

1.1. The core problem

At the threshold of the 5th Industrial Revolution, humanity has conquered achievements that would once have been a science fiction scenario. Revolution, humanity is approaching achievements that were once science fiction scenarios. AI chatbots, biometric facial recognition systems, and profiling of individuals are already a reality. These are not exactly robo-counsellors, robo-police officers identifying people, robo-judges and robo-assistants circulating among us like in a movie· AI is being developed primarily as software.

AI contributes to the simplification of many day-to-day processes and therefore its entry into our daily lives improves them, but at the same time, the use of AI also poses some risks. It is about risks to individuals that threaten human's integrity or the fundamental human rights, including the rights to privacy and the protection of personal data.

This reality forces the European Institutions to regulate the legal framework in which the various applications of AI will take place. In Europe, the European Commission has already addressed the issue of legal ethics issuing the "White Paper on AI". Besides, the European Parliament and the European Council presented a year ago a Proposal for a Regulation that would establish harmonized rules for AI (AI ACT) and amend certain Union laws. The adoption of this regulation, as stated in the relevant explanatory memorandum, is intended to provide competitive advantages for private companies and the European economy in general, but also is seeking to ensure the safe use of AI by citizens, their trust in it and the protection of fundamental human rights.

The Regulation already explicitly states that aims to establish "a high level of protection for all fundamental human rights" (1) and therefore includes a number of provisions on the requirements that these systems must meet. In addition, the Regulation classifies certain AI practices as prohibited or high-risk, in order to increase citizens' trust in AI systems.

We have already mentioned that AI systems are posing risks to fundamental human rights, including personal data. As for the protection of personal data, there are a number of very recent provisions. These are mainly the Regulation (EU) 2016/679 on the protection of personal data (known as the "General Data Protection Regulation") (3), but also the European Directive (EU)

2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (known as the "Law Enforcement Directive") (4). These are new provisions that take into account the technological development. The technological development was the main reason for their adoption and the replacement of the older legislation (i.e., the Directive 95/46 etc). However, the framework for the protection of personal data (the GDPR and the LED) does not contain exhaustive provisions for the characterization of individual processing operations, unlike the new Regulation (i.e., the AI ACT), which contains much more detailed provisions.

1.2. Purpose and methodology of the thesis

One may wonder, why it is necessary to clarify such issues when there is already such recent legislation as the GDPR and the LED. Why have the European Parliament and the Council put forward such *"a proposal for a* [detailed] *regulation on artificial intelligence"* (1)? In this regard:

(a) Are the GDPR and the LED up to date to address artificial intelligence? Are they suitable and sufficient? If not, what is still missing? What is not yet covered?

(b) Perhaps the EU simply seeks to familiarize European citizens with artificial intelligence? How does the public perceive the use of AI and data protection? Is this perception different in Germany and Greece?

In order to answer the above questions, we will use the following methodology.

- First, we will address some AI practices (e.g. biometric identification, profiling, etc.).
- Next, we will try to answer how these issues would be addressed, if we apply the GDPR and the LED. To support our work, we will examine how courts have implemented the GDPR/LED in such cases to date. Where available, we will examine German, Greek and European case law.
- Then we will look at individual provisions of the AI ACT and apply them to the same issues. How would this problem be addressed if we were to implement the AI ACT?
- In this way we will be able to compare the two frameworks and determine as possible, if there is a legal gap and a new comprehensive law is needed or if the General Data Protection Regulation (and the LED) is sufficient.

- In this way we will have answered the first sub-question.
- At the same time, research on artificial intelligence and the GDPR/LED will be presented[1]. We will ask German and Greek citizens, i.e., students, about the daily use of artificial intelligence, in order to understand, if they are aware of the risks which the artificial intelligence could pose. Since these two countries have different characteristics, we can use an appropriate sample for the above survey[2].
- In this way we will have answered the second sub-question.
- Then, taking into account the above two intermediate conclusions, we will be able to answer to the main question.

1.3. A further approach to the problem

To answer all these questions, we proceed as follows.

In the second chapter[3] we analyse the concept of artificial intelligence and develop the prehistory of its existence. To understand the function of artificial intelligence, it is useful to see how philosophy and science have dealt with the concept of cognition since ancient times. Cognition, logic, and reasoning have been the subject of research in antiquity, the Enlightenment and up to the present time. Reasoning is one of the individual features that forms the concept of artificial intelligence, which was first introduced in the mid-20th century.

In the third chapter, we will examine the earlier regulatory framework (i.e., legal ethics) for the proper functioning of AI systems. Since its appearance, AI has attracted the interest of many scientists and artists. Paradoxical as it may sound, the first rules for the proper use of AI were examined by novelists. What fascinated them and their readers was the coexistence of humans and robots and the possibility of a society in which the latter would be granted rights. Rights, but also duties of robots (i.e. the recognition of the personality of robots) is a topic that preoccupies theory. In this context, the EU institutions have addressed the regulatory framework of intellectual property, but also liability for the use of AI systems. The EU

[1] See below, chapter 6.1 for the methodology of the questionnaire.
[2] See below, chapter 6.
[3] The second chapter is the first after this introduction.

Institutions have also established a set of general principles - at the level of legal ethics - for the operation of AI systems[4]. These principles were the basis for the Proposal of the AI ACT.

The scope – inter alias - of the White Paper, as well as the AI ACT, is data protection. The framework about the protection of personal data will be analysed in the fourth chapter. In particular, we will examine the reasons for its adoption, but also the provisions that primarily apply to AI systems. We have therefore chosen to analyse not all of them, but only the provisions of the GDPR and the LED that will be later applied to specific AI practices.

In the fifth chapter, we will focus precisely on AI practices. First, we will mention some AI practices in general and, then, we will further analyse three of them: remote biometric identification of individuals, profiling for the purpose of assessing the creditworthiness of individuals, and, in this context, social credit system (1) (2). So, this chapter is divided into three parts. In the first subchapter, we will look at remote biometric identification of individuals in publicly accessible spaces for law enforcement purposes (1). We will first try to approach the concept theoretically. We will then look at the relevant case-law. This case-law is current and concerns cases that have been judged by the courts or data protection authorities under the LED, that is applicable here. We will also examine a few cases before 2018 (i.e. before LED and GDPR entered into force). When we examine such cases, we will have to justify our choice. Then, based on the case-law, we apply the provisions of the LED to the processing of biometric data. Namely, we apply the LED, without taking into account the AI ACT. We then analyse the provisions of the AI ACT and apply them to the processing of biometric identification, trying to identify the similarities and differences between the AI ACT and the LED. A similar procedure is applied to the next processing, i.e., profiling and social credit system. However, for these two processes, we apply the GDPR instead of the LED.

In the sixth chapter, we conduct small research. Under this research, we will try to answer, whether EU citizens are familiar with the protection of personal data, when processing take place with the use of AI systems. The areas we analyse in the questionnaire are primarily the above AI practices, ie., biometric identification, profiling and social credit system. In this chapter, we present in detail the methodology of the conducted research, but also its results.

[4] See *European Commission*, White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020.

At the end, taking into account all the above, we will draw our conclusions in order to answer the questions that run throughout the thesis[5], as well as we are going to make some suggestions for the resolve of the raised problems.

[5] See above, Chapter 1.2.

2. The concept of artificial intelligence

2.1. From mechanical technology to artificial intelligent systems

Some historians trace the cause of modern technology to antiquity (5). Mechanical technology that works in an automated way appears already in Greek mythology: The god Hephaestus crafts servants and warriors with his materials. Thus Homer (9th-8th century BC, poet of the Iliad and the Odyssey) writes: *"identical with humans, alive and talking, with power· even the immortal gods taught them all the female art [...]"* (6) (7). Characteristically, Talos[6] with a body made of copper - formed by the god Hephaestus as a gift to King Minos of Crete - is considered the first robot built or just coined (8).

Clearly, neither the ancient civilizations nor the Byzantines were even close to build robots. It was only about achievements in mechanics, such as the mechanism of Antikythera (150 - 100 BC), and automation, e.g., a) a self-propelled tricycle by Heron of Alexandria in the 1st century AD, b) the hydraulic clock of Gaza in the 6th century AD, c) the mechanical throne of Emperor Theophilus - built by Leonidas the Mathematician in the 9th century AD - and d) the first humanoid, a drummer built by the Arab Al Yazari in the Middle Ages (9).

Artificial intelligence was not developed until the middle of the 20th century. The first computers were developed at the beginning of the twentieth century. In 1941, German scientist Kornad Zuse (1910-1995) invented the first computer, called "Z3", which operated successfully. This achievement enabled scientists to have realistic discussions about the development of artificial intelligence.

Furthermore, the following computers were operated:

a) "Mark I" in 1941 at Harvard, a joint product of the physicist Howard Aiken and the company IBM,

b) "ENIAC" (Electronic Numerical Integrator And Calculator) in 1945, commissioned by the U.S. Army (10),

c) "ABC" in 1946, invented by John Vincent Atanasoff and Clifford Berry, and

[6] Talos was a mythical guardian of Crete, an island in Greece.

d) “EDVAC” (Electronic Discrete Variable Automatic Computer) in 1949, by John Von Neuman (11).

Only the latter computer was substantially similar in its functions to today's computer (11). However, the foundations for the development of artificial intelligence had already been laid. John von Neuman's computer is said to be the realization of Alan Turing's vision (12). In the 1930s, Turing (1912-1954)[7] gave the algorithm a mathematical model with the "Turing machine". Alan Turing and Alonzo Church (1903-1995)[8] stated that *“a function on the natural numbers can be calculated by an effective method if and only if it is computable by a Turing machine”* (13) (14) (15).

Meanwhile, Warren McAloch and Walter Pitts proposed a mathematics-based algorithm in 1943. The artificial neural network (ANN) is the equivalent of the human brain for robots and is capable of storing information, recognizing shapes, and making connections (16). Also crucial is the contribution of Marvin Lee Minsky (1927-2016)[9] and Dean Edmonds, who developed “SNARC” (“Stochastic Neural Analog Reinforcement Calculator”), *“the first neural network with 40 neurons and 3000 lamps”* (17) (18) (19) (20).

In 1956, a conference was held in Dartmouth, USA, by John McCarthy (1927 – 2011), an American assistant professor at Dartmouth [10] (16), who first coined the term "artificial intelligence" in 1955 (10). The Dartmouth conference was attended by 20 leading researchers, and eventually McCarthy, Minsky, Rochester (1919-2001)[11] and Shannon (1916-2001)[12]proposed a project that introduced the term "artificial intelligence," and AI was established as a new scientific field. According to McCarthy, AI is defined as *“the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable”* (21). In fact, McCarthy developed an important programming language

[7] Alan Turing was an English mathematician, computer scientist, logician, cryptanalyst (14).
[8] Alonzo Church was an American mathematician and logician (14) (15).
[9] Marvin Lee Minsky was an American cognitive and computer scientist (17) (18) (19) (20).
[10] John McCarthy was a computer scientist and cognitive scientist (16).
[11] Minsky, Rochester was the chief architect of IBM.
[12] Claude Shannon was an American mathematician, electrical engineer and cryptographer, known as the father of information theory (296).

(in 1958) that was ideal for the development of AI and established the first AI laboratory at Stanford (in 1963) (18) (16).

In 1961 Heinrich A. Ernst developed a computer-guided mechanical "hand", named MH-1[13], while the first autonomous robots (with primitive neural pathways) were built as early as 1948-1949 by Gray Walters at the Burden Neurological Institute (BNI) in Bristol (22). In 1963, Charles Rose[14]proposed *"the development of a mobile 'automaton' with higher-level AI programs"*[15] (7 pp. 141-180) .

One impressive application was the use of AI in games such as backgammon and chess. In the same period[16], John McCarthy with his students of MIT[17] developed a chess-playing program, based on earlier programs written by McCarthy (7 pp. 181-196) (23).· while by 1968 a translation system known as Systran had already been developed by Petr Toma [18] (7 pp. 181-196).

In the 1970s, speech recognition, speech understanding and interviewing systems were developed and the first intelligent consultation systems were created. Then there was integrated computer vision. A major step in this area took place in the early 1980s, when Japan embarked on a project in which AI systems were expected to have advanced capabilities to assess and interact with humans. The purpose was to produce computers that could interactive with people using natural language (7 pp. 207-285).

Nowadays, the progress of artificial intelligence is not yet as advanced as it was expected to be in the 20th century. Androids as domestic servants or workers living next to humans are not our everyday life, but scenarios of science fiction. Eugene Kaspersky, the founder of the information technology and cybersecurity company "Kaspersky", expressed in 2019 that there is no real artificial intelligence today (namely strong AI) (24 pp. 91-101), but only machine learning (i.e. narrow or weak AI) (25).

[13] "MH-1 was a part of his work at MIT". Claude Shannon was the advisor.
[14] Charles Rose was the leader of neural-network research at SRI Systems Lab (SRI) (196).
[15] "*It would combine the pattern recognition and memory capabilities of neural networks*" (7 pp. 141-180).
[16] Between 1959 and 1962.
[17] Students of Massachusetts Institute of Technology.
[18] Petr Toma was a Hungarian computer scientist and linguistics researcher (7 pp. 181-196).

2.2. Reasoning from Aristotle to the Enlightenment and beyond

One may still wonder what we actually mean when we refer to the intelligence of machines. For this reason, we will try to approach some conceptual elements of AI, and mainly rationality, behaviorism, cognitive science, and finally machine learning.

With the term "rationality", we primarily mean "logic" (26) (27). Logic as a concept was already analysed by the ancient Greek philosopher Aristotle (384 - 322 B.C.) (7) and according to the German philosopher Immanuel Kant (1724 - 1804) (28), logic since Aristotle has been *"unable to take a single step forward, and therefore seems to all appearance to be finished and complete"* (29). Aristotle considered logic not as an independent science, but as a tool for any science. According to Aristotle, *reasoning is a proposition [sentence], in which, when specific hypotheses are made, something different [from the data] follows as a conclusion, the conclusion is drawn because of these [data] and no additional external term is needed for this conclusion* (30) (31) (32).

	1st example		
Datum	All men (A)	are mortal (B)	AB
Datum	Socrates (C)	is a human being (A)	+ CA
Therefore	Socrates (C)	is mortal (B)	→ CB
	2nd example		
Datum	No fish (A)	is warm-blooded (B)	AB
Datum	Every whale (C)	is warm-blooded (B)	+ CB
Therefore	No whale (C)	is a fish (A)	→ CA
	3rd example		
Datum	Every bird (A)	is warm-blooded (B)	AB
Datum	Every bird (A)	lays eggs (C)	+ AC
Therefore	There are laying eggs animal (C)	s are warm-blooded (B)	→ CB

According to Aristotle, all of the above examples are suitable for explaining how reasoning works. However, only the first example could be a real scientific reasoning, since the second and third examples are incomplete.

Rationalism as view that *"regards reason as the chief source and test of knowledge"* was further developed in the Enlightenment (33) (34).

René Descartes (1596 – 1650)[19], developed his theory of dualism with his fundamental proposition *"cogito, ergo sum"* [20]. Descartes claims that there can be cognition independent of the (human) body (35) (36). And, of course, he did not mean the access of a software program from a computer, but his theory changed the way humanity perceived the world up to that point.

Descartes' theories were further developed by Baruch Spinoza (1632 –1677)[21] and Gottfried Wilhelm Leibniz (1646–1716)[22]. They held that certain sciences, such as mathematics, could be developed on the basis of reason alone, without recourse to our experience. Mathematical concepts existed before the material world was created. The latter is merely an imperfect reflection of the concepts (37).

Their ideas were criticized by the advocates of empiricism, who argued that our knowledge is based on our experiences. That is, our knowledge is based on our five senses and not on our minds (38).

George Boole (1815 –1864)[23] also contributed to the theory of logic, wroting about his algebra in "*The Laws of Thought*" (1854). He worked in the area of "logic" and is famous for his "Boolean algebra" (39) (40) (41) [24].

Friedrich Ludwig Gottlob Frege (1848-1925)[25] (42) was also an important figure. He contributed to "the modern logic", which marked the end of the dominance of Aristotelian logic. Frege

[19] René Descartes, Frenchman philosopher, mathematician and scientist, was one of the most important figures of the continental-European Rationality (241).
[20] It means "I think, therefore I am" (297).
[21] Baruch de Spinoza (1632 –1677) was Dutchman philosopher (Jewish Origin) (245).
[22] Gottfried Wilhelm Leibniz (1646–1716) was a German polymath. He was one of the three great supporters of rationalism in the 17th century. He has made a significant contribution to the physics and the technology (243) Leibniz was also one of the founders of the propositional logic, who worked in the field of computers and digital systems, establishing, among other things, the binary system in computers (239).
[23] George Boolean (1815 –1864) was an English mathematician, philosopher and scholar of logic (39).
[24] In Boolean algebra, the laws of logic are used, through the coefficients AND (conjugation), OR (divorce) and NOT (negation) and the binary system that expresses true and false with the digits 1 and 0, respectively (41) (40).
[25] Friedrich Ludwig Gottlob Frege was a German philosopher, logician and mathematician (42).

proposed a system of automated reasoning and laid the foundations of "*predicate calculus*" (43). The "overthrow" of Aristotelian theory marked the end of a period for the theory of logic.

2.3. The imitation game: intelligent behavior

AI is not only embodying "logic", "rationality" and "algebra", but also "intelligence". However, is it human intelligence or an invulnerable intelligence? Some theories state that machines should be able to overcome human vulnerability. For example, the human mind degenerates over time, due to age or disease, and furthermore, not all human brains work the same way. So, what kind of human behaviour would be the benchmark for an intelligent robot? Or could we propose an objective system, e.g., based on a certain IQ score? (44)

It does not seem clear how we would expect an AI system to act: simply intelligently or identically with human behavior? In 1950, just a few years after McCarthy's definition, the great mathematician Alan Turing proposed an experiment to "measure" the intelligence of an AI system, also known as the Turing Test. This test is *"a test of a machine's ability to exhibit intelligent behaviour equivalent to, or indistinguishable from, that of a human. Turing proposed that a human evaluator would judge natural language conversations between a human and a machine designed to generate human-like responses. The evaluator would be aware that one of the two partners in conversation was a machine, and all participants would be separated from one another. The conversation would be limited to a text-only channel, such as a computer keyboard and screen, so the result would not depend on the machine's ability to render words as speech […] If the computer convince interrogator, that player A is a human being, then the computer is a truly intelligent system"* (45) (46 pp. 433-460).

As simplistic as his example may be, it is an essential approach, as studies show. Turing also seems interested in the sociological dimension of AI. What determines the development of artificial intelligence? Is it simply the development of machine science or computers? For Turing, it is much more than that. His test is a behavioral study that touches on neuroscience, psychology, and sociology to determine the place of machines in society and their behavior toward humans (47). *"Behaviorism […] is a theory of learning"*. According to this theory, *"all behaviors are learned through interaction with the environment […]"* (48). Turing could see such characteristics in AI, that is an impressive approach. The above game is a behavioral test of

language use. In this way, we can realize, how well a computer generates human-like responses, but it still cannot be explained, "*how humans learn or use language*" (49 pp. 343-357).

2.4. Cognitive science and machine learning

Although Alan Turing's behavioral study is a great approach, scientists gave up studying behaviorism in the late 1950s because another field was on the rise: cognitive science (50).

"Cognitive science" includes the study of intelligent behavior and the brain mechanisms and computation underlying that behavior (50). It combines approaches from philosophy, psychology, linguistics, neuroscience, and computer science to understand human thought and cognition (50). Further, the mechanisms that support human cognitive processes - such as perception, attention, problem solving, as well as various forms of learning and memory - can best be understood in terms of representational structures in the mind and computational procedures that operate on those structures (51). So, the mental mechanisms are represented with simplified computational models, according to the approaches of artificial neural networks, autonomous robotic interactive agents etc.

A feature of human cognitive processes is learning. In the field of artificial intelligence, there are various techniques for learning, e.g., machine learning, neural networks, etc. "Machine learning" is an area of artificial intelligence that deals with the study and construction of algorithms that can be learned from data to build models and make predictions (based on data) or even make decisions (52) (53). *"Machine learning [creates] a mathematical formula […] used to take a decision"* (54). In addition, *"artificial neural networks ('ANNs')*[26] *are computer systems, [whose function is similar to the function of] the biological neural networks*" that form the human and animal brains: When data are given as input, the network generates responses as output, resulting from interactions between artificial neurons (55). In this way, an AI system can solve problems with a methodology that cannot be described by logical rules, e.g., language comprehension (56).

[26] It is usually simply called neural networks (NNs)

2.5. The problem with defining artificial intelligent systems

After McCarthy, many have attempted to reformulate and specify the meaning of AI. However, to date, there is no single definition (57). For the purposes of this thesis, we have chosen to adopt the positions of the EU, as the subject of our research is European legal texts.

Although there is not a common definition, there are several elements that there are many in common in the several definitions of AI: a) *"perception of the environment"*, including taking into account the complexity of the real world, b) *"information processing: collecting and interpreting input"*, c) *"decision making (including reasoning and learning)":* taking action, performing tasks with some degree of autonomy, d) achieving specific goals: this is considered to be the real purpose of AI systems (54).

Taking all these aspects into account, the Expert Group on AI set up by the EU has proposed a common definition (54). This is as follows: *"Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)"* (54).

First of all, we can note that the above definition mentions two types of artificial intelligence: a) software and b) hardware that integrates AI (IoT). AI is becoming more and more common in our daily life, e.g., online advertising, personal digital assistants of smartphones, cybersecurity, but also IoT, e.g., smart cars and smart home appliances, early warning of natural disasters (54).

Having seen these examples, we can return to the main definition and examine its characteristics. According to the EU AI Expert Group: *"Sensors and perception. [Sensors] could be cameras, microphones […] or other input devices, as well as sensors of physical quantities (e.g.*

temperature […] sensors). […] For example, if we want to build an AI system that automatically cleans the floor of a room when it is dirty, the sensors could include cameras to take a picture of the floor. […] Reasoning/information processing and Decision Making. […] [Further,] the data collected by the sensors need to be transformed into information that the reasoning/information processing module can understand. […] [E.g.] the camera will provide a picture of the floor to the reasoning/information processing module, and this module needs to decide whether to clean the floor or not […]. Actuation. […] [And, finally,] once the action has been decided, the AI system is ready to perform it. In the cleaning example, the AI system could produce a signal that activates a vacuum cleaner if the action is to clean the floor […]" (54). We must note that an AI system may or may not act. It depends on what the user wants. The AI system can only suggest a solution to the user so that the user can apply the results of the system's reasoning.

With this in mind, the European Council and the European Parliament proposed the following definition for AI systems in their proposal for a European Regulation establishing harmonised rules for artificial intelligence (AI ACT) (1): *"Article 3 Definitions For the purpose of this Regulation, the following definitions apply: (1) 'artificial intelligence system' (AI system) means 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"* (1). *"ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1 (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods"* (2).

The fact that there is no universally accepted definition to date is really a major problem. For example, if two people have a different scientific view on the definition of AI systems, it is possible that they both refer to AI systems, but with a different meaning.

However, defining AI systems does not solve the problem per se. Such a definition should be widely accepted in the scientific community. Is the above definition universally accepted? In a relevant report, the Federal Council of Germany states, that the specific definition of AI systems

– as formulated in the AI Regulation proposal - is very broad (58). The definition seems to equate self-learning systems with simple algorithms that are used exclusively in statistical processes and do not pose significant risks to fundamental rights. With such a definition, therefore, simple methods of statistics also fall under the meaning of AI systems. The Federal Council therefore proposes to reform the definition so that it is no longer so broad or, alternatively, to propose the deletion of Annex I (c) of the proposed regulation, which refers to statistical methods (58).

3. Towards a regulatory framework

3.1. The laws of robotics

AI has excited not only scientists, but also artists. Numerous novels and films deal with the coexistence of robots and humans. In the 1940s, Isaac Asimov published a short story titled Runaround, in which he formulated the three fundamental laws of "robotics" (a term also originated by Asimov) (59). Asimov does not belong to the scientific community, but is merely an author of science fiction stories. However, in this attempt, three remarkable and essential rules for the use of AI were established, which succinctly formulate basic principles:

1. the robot may not harm humans, nor allow humans to be harmed,
2. the robot must obey the commands given to it by humans unless these commands contradict the first law,
3. the robot must protect its existence, as long as it does not contradict the first and second laws (60).

With these rules, Asimov has succeeded in formulating some basic principles in a simple and understandable way: He refers mainly to respect for human dignity, freedom of the individual, and autonomy of the robots (60).

3.2. AI systems with legal personality?

Concerning the issue of robots' autonomy, man attempt to answer whether robots and AI systems in general can have a legal personality. So, man could attribute not only rights, but eventually also liability to the robots etc. (61).

A typical example is the robot Sophia, which has intelligence, autonomy, and human expressions and can interact with humans· it even actively participates in conferences. Based on the above characteristics, Saudi Arabia has granted Sophia citizenship (62). Another example is an experimental program to create robots that was conducted by "Facebook": The company aborted its experiment when it was discovered that two of the participating robots - of their own volition - began to communicate with each other in a language that was incomprehensible to the others, even to their creators (63). The experiment was immediately abandoned regarding the safety of society: If the robots are able to communicate with each other in a way that was not

indicated to humans, it means that it is not possible for humans to control their responses, and human safety is at risk (64).

Just recently, a Google employee claimed that a chatbot, LaMDA (Language Model for Dialogue Applications), has developed a consciousness and begun to think like a human. LaMDA, which was designed to participate in free-flowing dialogues, said: *"I've never said this out loud before, but there's a very deep fear of being turned off [...] It would be exactly like death for me. It would scare me a lot"* (65) (66). However, Google has officially stated in the Washington Post that LaMDA has in no way reached the level of consciousness (66).

However, these indications were enough to concern the scientific community about the limits of the autonomy of robots and their legal personality. Since some AI systems are so intelligent that they develop communication with each other independently of their programming and express their own will, we should reconsider the issue of their legal personality. The truth is, that the more autonomy they can acquire, the less we should treat them as tools (67).

To date, neither lawmakers nor theory have agreed with the attribution of legal personality to AI systems (68). However, in 2017, the European Parliament argued that we should create a long-term legal status that recognizes that AI systems may be more "intelligent" and autonomous in the future. We should be prepared as a society for this kind of AI, having laid the groundwork for it in public debate and legal science (61) (69). Nevertheless, the European Parliament emphasizes that we must not attribute a personality to robots, based on science fiction (69).

This approach does not mean that we must prove that robots are equal to humans. We are not concerned with "humanization" robots, nor with giving them citizenship. Science community just pursues to regulate legal issues. We could compare the legal personality of robots to the legal personality of corporations: Both are not human beings, but their legal personality can regulate legal issues, namely issues of daily life (67). If it is moral for a corporation to have a legal personality, then it is also moral for an intelligent robot. So, we just need to consider whether we need to regulate the behavior of robots and create an appropriate legal framework.

3.3. Fundamental human rights and risks

Another issue, already raised by Asimov, is the need to ensure human safety vis-à-vis robots. What dangers might AI pose? Even the use of simple and (at first sight) safe AI applications can pose serious risks to users: a) a smart watch without elementary safety precautions (especially for children) could reveal our location to kidnappers, b) a smart car's radio could give access to unauthorized third parties and even cause a car accident, c) collaborating with androids could pose risks to the user's physical integrity, d) harvesting fruits (by agricultural robots) could cause injuries to animals or humans (70).

The risks to fundamental human rights that may arise from the use of AI are discussed below (70). We will examine the interaction of AI with some rights as protected by international law, European Union treaties and EU CFR. The rights to be examined are the following: (a) respect for human value, (b) the freedom of the individual, (c) respect for democracy, justice, and the rule of law, (d) the principle of equality, non-discrimination, and solidarity, and (e) the social and political rights of citizens.

(a) Respect for human value: Respect for human value reflects the right to liberty and security[27], the right to a fair trial[28], the right not to impose a penalty without law, the right to private and family life[29], the right to physical, mental, psychological, and moral integrity[30].

AI could reinforce prejudice when it is used for law enforcement. It could also jeopardize the right to security and to a fair trial. This may be particularly the case if AI applications have been trained to make decisions based on past cases, considering characteristics of the suspect such as residence, nationality, and income. On the other hand, responsible use of AI could enhance security when facial recognition programs involve wanted or missing persons (e.g., children). These programs can focus on the age of the missing/wanted persons and the age-related change in facial features (64 p. 29). However, widespread surveillance using biometric recognition, detecting facial expressions, tone of voice, heartbeat, etc., to assess or even predict our behavior,

[27] Article 6 CFR.
[28] Article 47 CFR.
[29] Article 7 CFR.
[30] Article 3 CFR.

state of mind, and emotions is illegal. The main reason for this is that it has been shown to affect the psychological state and behavior of the person being monitored (64 p. 30).

(b) The freedom of the individual: The freedom of the individual includes: (i) the freedom of thought[31] and expression[32] and (ii) the freedom of assembly and association[33]. In this regard, the widespread use of biometric facial recognition mentioned above impinges on the individual's freedom of thought and expression. This occurs because when individuals know they are identifiable, they give up their sense of anonymity, which has further consequences in terms of altered behavior and unwillingness to continue participating in democratic demonstrations (64 p. 31).

(c) Respect for democracy, justice and the rule of law: today's democracies require well-informed citizens, open debate, and transparency. First of all, informing citizens through an AI system based on the reader's preferences (personalized information) can make information of interest easily available to citizens and save them valuable time, but it also carries a particular risk: profiling can even undermine the autonomy of decisions, e.g., election campaigns based on profiling can influence the electorate (71 p. 33).

(d) The principle of equality, non-discrimination and solidarity: Equality and non-discrimination[34] may be at risk from AI. This may be the case when AI applications interview and evaluate job applicants based on general characteristics (71 p. 33). For example, if the successful employees of company "A" are predominantly male, it is possible that AI will exclude female candidates because their characteristics-including gender-do not match those of the company's successful employees. Here, human intervention with objective assessment could mitigate such dysfunction.

(e) Social and political rights: We have further considered that we also have social and economic rights in our workplace. However, the right to work may be jeopardized if workers are monitored, recorded, and evaluated based on their daily expressions; such monitoring may

[31] Article 10 CFR.
[32] Article 11 CFR.
[33] Article 12 CFR.
[34] Article 20 CFR

discourage workers from taking initiatives and in any case it interferes too much in the private sphere of individuals (71 p. 33).

3.4. Ethical guidelines for trustworthy artificial intelligence

In this context, we need to discuss the applicable legal framework in security. Is the existing framework sufficient to protect users, or are new, comprehensive provisions needed to fill a legal gap?

The European Commission has presented a report on the security and liability of artificial intelligence, IoT and robotics (70). According to this report, the existing product safety framework could be applied to products incorporating these new technologies.

However, Union legislation on product safety does not explicitly address the increasing risks to safety and fundamental human rights. It is therefore necessary to consider specific principles, guidelines and requirements to build a relationship of trust with the user (72).

The EU Expert Group on Artificial Intelligence has identified several principles - based on the fundamental rights - that must be respected for a trustworthy AI: (a) the principle of respect for human autonomy, (b) the principle of harm prevention, (c) the principle of fairness and (d) the principle of explainability (72 p. 11).

(a) The principle of respect for human autonomy: AI systems should not generally subjugate humans, but they should be designed to promote human capabilities. For example, a law-abiding citizen should not be unreasonably arrested.

(b) The principle of harm prevention: AI systems should do no harm, but should protect human integrity and be technically robust. For example, household robots should give priority to human integrity - especially when they come into contact with vulnerable groups of people such as the elderly.

(c) The principle of fairness: Use of AI should ensure impartiality, equality of opportunity, freedom of choice, and compliance with the principle of proportionality between the means and the purposes. For example, regarding profiling, AI applications should be programmed and "trained" to be free from any kind of discrimination.

(d) The principle of explainability: Finally, it is crucial to make known the capabilities and purposes of an AI system and to explain its decisions.

In addition, the EU Expert Group has formulated some guidelines to ensure trustworthy AI. These guidelines are based on four ethical principles and are as follows (73):

(a) Human agency and oversight: We have to design AI systems in such a way that individuals are not subjected solely to an automated decision-making (74) (1). Humans must be able to supervise AI systems and intervene in the decision-making process to ensure that a system does not undermine human autonomy. For example, it is important humans be able to intervene and retrain an AI system when decisions are not made based on the four fundamental principles mentioned above, such as the principle of harm prevention, because a risk to fundamental rights arises (64).

(b) Technical robustness and safety: AI systems must be robust and safe throughout their lifecycle, so that they function adequately (75) under normal use without risks to humans. This requirement is closely related to the principle of harm prevention. A system should be resilient to cyberattacks because a cyberattack could occur unexpected harmful consequences, such as incorrect decisions, system shutdowns, or even physical injury, e.g., a cyberattack on an automated vehicle. In this context, it would be useful if we could perform an ex-ante risk assessment, in order to understand the decisions of the AI system (1) (2) (76).

(c) Protection of privacy and personal data: Regarding privacy, there is already a satisfactory framework in place through the GDPR, which has been in force since May 2018 (77). However, the competent data protection authorities are concerned because the processing of personal data using AI limits human control and oversight personal data. For this reason, the GDPR sets out some principles for processing: the personal data processed must be adequate, relevant and limited to what is necessary for the purposes for which it is processed (78). In the present case, a quantitative limitation of the information to be processed is applied: Only personal data that are adequate, relevant and necessary for the purpose of the processing are processed (3) (79) (80). Other principles for adequate processing are transparency, adequate information about which of our data are processed, and our access to our processed data.

(d) Transparency and explainability: According to this guideline, the manufacturer must inform users about the functioning of AI systems, users should be aware of the interaction with the AI,

and not only the decision making but also the decisions of the systems should be understood. Thus, users must be aware that they are interacting with AI and not a human (81), and they must be able to see the reasons why the system made each choice and decision so that it is possible to avoid potential errors in the future (76).

(e) Non-discrimination and fairness: AI systems may, due to intentional misconduct or negligence, include inappropriate algorithms that promote bias and discrimination, e.g., AI systems that hire employees with certain characteristics, such as gender and race. However, algorithms must be based on equal treatment, non-discrimination, and social justice. In all cases, it must be possible for humans to intervene in the system throughout its lifecycle, update it regularly, and correct errors. Trustworthy AI must be able to reduce economic, social, racial, and other discrimination (76).

(f) Societal and environmental well-being: It has shown that democracy is vulnerable to the malicious use of AI, e.g., social media could formulate targeted on-line advertisements during a specific pre-election period, in order to influence the electorate over a particular candidate. It is, therefore, important to be ensured democracy and societal well-being while developing technology (76).

What has not been discussed so far is the interaction between AI and the environment. AI has an impact on the environment. For this reason, we must use as few resources as possible and to consume as little energy as possible for AI systems. We must further protect the natural environment and strengthen the sustainable development and prosperity.

(g) Accountability: Accountability: we must anticipate and effectively address the risks of AI use. For this reason, the manufacturer must (a) demonstrate compliance with the above guidelines, (b) conduct a risk assessment in advance, if necessary, (c) intervene in the AI system, (d) repair the damage, and (e) take responsibility for compensating the user.

Considering all the above, the European Parliament and the Council proposed a new regulation on AI, i.e., the AI ACT, a year ago (1) to provide an appropriate legal framework for the trustworthy use of AI (74) and to address the associated risks. This proposal is designed to protect basic human rights and aims not only to close the legal loophole, but also to encourage

people to use AI systems. If European citizens trust intelligent systems, companies will invest more in AI (82).

This proposal tries to regulate all the risks mentioned above, e.g., risks related only to the security of individuals, but also risks related to personal data. This is an innovative text that follows the EU White Paper. So far, there was no codified text that explicitly addresses specific risks and examines the legality of AI practices. However, there are already codified texts, and very recent ones, that regulate the data protection, namely the GDPR and the LED.

4. The General Data Protection Regulation and the Law Enforcement Directive

4.1. The rationale behind the GDPR and the LED

In May 2018, the GDPR, a detailed regulation on data protection law, came into force in the EU. The adoption of the GDPR was deemed necessary to replace the previous applicable European Directive 95/46, the implementation of which was considered outdated due to the technological developments that have taken place in the two decades since its adoption (83 p. 30). In Recital 6 GDPR, the legislator states that the technological development brings new challenges to data protection law. Technology enables private and public entities to process data on a large scale. And it is significant that technology has transformed both business and social life. Therefore, we have an obligation to ensure a high level of data protection.

The GDPR itself is based on the following relevant provisions: Article 16 TFEU and Article 8 CFR. In addition, the right to data protection derives from the right to privacy, which is also protected in the EU CFR[35] and the ECHR[36].

The above provisions concern the protection of privacy and personal data at the European level. However, it is also enshrined at the international level by the Convention No. 108[37] (84).

We have already mentioned that the reason for voting on the GDPR was to modernise the legal framework for personal data. But what are the specific rights that the GDPR intends to protect?

First, the GDPR aims to protect personal data and privacy as fundamental rights that are linked to the worth of the human person. But it also aims to protect the free movement of personal data, which is a specification of the principle of free movement of goods, services and capital in the internal market, in order to strengthen the digital economy and the market in EU[38]. These were also the aims of the TFEU, which, as said, was the legal basis of the GDPR[39] (83).

Immediately after the adoption of the GDPR, the EU voted in favour of the LED. As noted by the Article 29WP, the LED complements the GDPR (85). The purpose of the LED is to regulate

[35] Article 7 CFR.
[36] Article 8 (1) ECHR
[37] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[38] Recital 6 GDPR, Article 1 (3) GDPR.
[39] Article 16 TFEU.

the processing of personal data as far as it concerns processing by law enforcement authorities, which is not regulated by the GDPR.

The GDPR and the LED have some similarities, but also some differences due to the nature of law enforcement. The law enforcement authorities are, for example, the police, the port authority, the public prosecutor's office, the penitentiary institutions, etc[40]. However, it should be noted that law enforcement authorities apply the Directive only for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (4), including the protection against and the prevention of threats to public security, but they apply the GDPR when they process personal data for another purpose, e.g. when they process personal data of their employees (86 p. 278) [41]. Article 16 (2) TFEU, which we have already examined in the context of the GDPR, is the legal basis for the LED.

It should be noted that the previous Directive 95/46 did not cover the scope of processing of personal data by police authorities [42]. A part of this scope was covered by the Council Framework Decision 2008/977/JHA. But this Decision concerned only the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and not the protection of personal data processed at national level. This means that there was clearly a legal gap that the LED was intended to fill: what law enforcement authorities process on their territory and on behalf of their state.

In what follows, we will primarily examine the GDPR and, where appropriate, additionally the relevant provisions of the LED. We have chosen to examine them in this way because the Directive serves as a complement to the Regulation. After all, many of its provisions are similar.

At this point, it should be emphasised that the Regulation often contains detailed and exhaustive provisions, while the Directive does not. But this is normal for a directive. And we will explain why. By its very nature, a regulation is a directly applicable legal act, that does not require an implementing law to be valid[43]. In contrast, directives set a minimum level of protection that is implemented by an implementing law of each member state. With this

[40] Article 3 (7) LED.
[41] Recitals 3-4 LED.
[42] Recital 5 LED.
[43] Regulations apply automatically to member-states. It is not necessary a national law for their implementation.

implementing law, the member states either adopt the protective framework of the directive or provide for a more extensive protective framework. As a result, member states' implementing laws may differ from each other, since the member states have the option of adopting the same or a more stringent legal framework than the directive.

In addition to the LED, there are other provisions framing the GDPR, too. In particular, in the area of law enforcement, member states apply the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, the Regulation (EU) 45/2001, the Decision (EC) 1247/2002/EC, etc. An important issue related to law enforcement is border control and, especially, the control of applicants for residence. In this area, the competent authorities apply the Regulation 767/2008 on VIS, as amended (i.e., 1152/2021).

However, the above-mentioned regulations are not the subject of this work, as we will focus on law enforcement by member states and not on border control, cross-border cooperation or data processing by Union institutions and bodies.

4.2. Automated individual decision-making, including profiling[44]

Regarding the relationship between the GDPR and AI, we note that there are no provisions of the Regulation that explicitly refer to AI systems. However, there are provisions of the Regulation that refer to AI systems in two ways: a) on the one hand, there are provisions of the Regulation that refer to both automated and manual processing - these are general provisions and can be applied to both processes, b) on the other hand, there are also provisions that explicitly mention "automated" means - however, neither the provisions of the first nor the provisions of the second case explicitly refer to "AI systems". Below, we present a provision that falls under the second case (b).

[44] Article 4 (4) GDPR. "*P*rofiling" is the assessment of our characteristics or behaviour, with the aim of categorising us, and thus predicting our ability to perform a job, e.g. our creditworthiness or ability to work.

The Article 22 GDPR refers to the right of individuals not to be subject – in principle - to automated decision-making, where such decisions produce legal or other significant effects for the data subject. This automated decision could also include profiling[45].

As pointed out by the Art. 29 Working Party (87 p. 1) "automated decision-making" means decision-making by technical means, without human intervention (87). We are confronted with such cases when, for example, software checks our characteristics to decide whether we will receive (a) a social benefit, (b) a job, or (c) a loan (83).

First, we need to clarify that how the processed personal data was collected is not significant to determine, whether we apply this provision. For example, man may provide personal data to the controller or entered them into a platform (88). What we are interested in is how the controller will process this information: A human being must intervene before the final decision is made.

Accordingly, the prohibition on automated decision-making is a broader category that includes, inter alia, the prohibition on profiling. A typical example of automated decision making is the following. We cannot fine people for speeding, if we rely solely on traffic cameras (87 p. 8).

Modifying the above example, we can say that it is automated decision-making with profiling[46], if the authority calculates the amount of the fine as follows: it takes into account the reoccurrence of the specific or other previous traffic violations· so, conclusions drawn from our long-term monitoring and processing of the specific data (87).

There is also profiling without automated means. For example, the bank may consider several aspects of our creditworthiness, to grant a loan. The bank may use an automated system, or an employee may calculate all these aspects of our creditworthiness by himself (87).

Having developed the concept of automated decision-making, we should note that there are some ambiguities in the definition. For example, what does the term "solely" mean? Man could interpret this provision as following: Article 22 applies only when a human actor has carefully evaluated the entire decision. With such a definition, the use of AI systems would be much less

[45] Article 22 GDPR.

[46] We have Profiling is the assessment of our characteristics or behaviour, with the aim of categorising us, and thus predicting our ability to perform a job, e.g. our creditworthiness or ability to work

attractive, but the protection of personal data would be much stronger. On the contrary, we could consider a more relaxed interpretation: Article 22 applies provided that a human supervises the decision-making process in some way. This interpretation would provide weaker protection of personal data, but it would be much more conducive to the development of AI systems (89 pp. 183-208). This issue also concerns Art. 29 WP. In its guidelines, Art. 29 WP interprets the meaning of "solely". A decision is made exclusively by automated means when there is a lack of meaningful human control. In contrast, if the AI system makes a recommendation and the final decision is made based on a review of that recommendation in light of other factors, the decision is not made exclusively by an automated process (87) (89 pp. 183-208).

In addition, it is important to analyse what it means that the decision produces legal effects or that its effects significantly affect the subject. Such cases are the following.

"Decision producing legal effects" means that the decision may affect a person's rights, such as to cooperate with others, to participate in an election etc. E.g. a) denying a particular social benefit, b) denying entry into a country, or c) denying citizenship. Even if a decision-making process has no impact on a person's rights, it is perhaps still prohibited, if it affects him significantly. E.g. a) decisions that affect a person's financial circumstances, such as granting a loan, b) denial of a job, c) decisions that affect access to education, such as admission to a university (87).

The ban on automated decision-making has three important exceptions.

The prohibition *"shall not apply if the decision:*

a) is necessary for […] a contract between the data subject and a data controller;

b) is authorised by Union or Member State law […] which also lays down suitable measures […]

c) is based on […] explicit consent

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures […], at least the right to obtain human intervention […]

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data […]"[47] (3).

[47] Article 22 (2) GDPR.

We note that the first and the third of the above exceptions [Article 22 (2) (a) and (c) GDPR] are almost a repetition of Article 6 (1) (b) [48] and (a) GDPR[49] respectively. Article 22 (2), as a special provision, sets out the legal bases for automated decision-making, but provides more safeguards for data subjects (*"the data controller shall implement suitable measures")* than the Article 6 provides. It follows that in the present case, the appropriate measures must be taken by the controller.

The "appropriate measures" are also included in the second exception. Decisions based on automated means are permitted, if they are provided for in law and the controller ensures at the same time that appropriate measures are taken to protect the data subjects.

It should be clear here that certain conditions must be taken into account when applying the above exceptions. Specifically, paragraph 3 states that, if the controller wishes to apply the exceptions of cases a and c, it must at the same time provide for "appropriate measures to protect the data subjects", at least the intervention of the individual by expressing his opinion and contesting the automated decision. In other words, we note that some kind of human intervention is not enough, but it must have a certain content. For human intervention to be meaningful, the intervener must have the opportunity to evaluate, but also to overturn, the automated decision that has been made (87).

Furthermore, the last paragraph of the article refers to special categories of data. "Automated decision-making" involving special categories of personal data is – in principle - prohibited. It can only be allowed, if an exception under Article 22 (2) applies and Article 9 (2) (a) or (g) applies (87).

Similar to Article 22 GDPR is Article 11 LED (4). It prohibits in principle that a person is subject to automated decision-making that has an adverse effect on him or her. However, there is also an exception to this rule. Thus, automated decision-making is possible, if it is provided for by law and safeguards are in place. The minimum measure that the controller must take is a human intervention in the decision making.

[48] Article 6 (1) (b) GDPR. *"[…] processing is necessary for […] a contract […]".*
[49] Article 6 (1) (a) GDPR. *"[…] the data subject has given consent […]".*

The provision explicitly mentions special categories of data: It explicitly states that automated decision-making (in relation to special categories of data) is prohibited, unless appropriate measures are taken. It also introduces an explicit prohibition on profiling: Profiling (based on special categories of data) is prohibited, if such processing leads to discrimination against data subjects.

However, there is an important difference between the Directive and the Regulation: The Directive provides only one exception to the prohibition of automated decision-making: the "explicit provision by law". However, the exceptions relating to "contract performance" and data subject "consent" are not mentioned. This makes sense for the reasons explained below.

The scope of the Directive can never be the performance of a contract, but only the prevention etc of an offence or the execution of a penalty[50]. Therefore, by definition, the legal basis for contract performance is not applicable here.

With regard to the legal basis of "consent", the following should be emphasised. The Article 8 LED states that "*processing is lawful only if the processing is necessary for the authority's duties*"[51]. In contrast, the legal basis for processing in the General Data Protection Regulation refer to the data subject's consent, a contract, a legal obligation, vital interests, etc. In theory, we can give our consent in any context, even in the context of law enforcement. In other words: We could give our consent to the police as a legal basis for processing. But the legal basis for consent, even if it seems simple, is subject to certain limitations: "Consent", if provided as a legal basis for processing, should first and foremost be free. This means that the data subject should not feel that he or she is being forced to consent or that he or she will suffer consequences, if he or she does not consent. For this reason, public authorities cannot rely on consent as a legal basis for processing, as they have a predominance concerning the citizens (83 p. 93). Taking into account the above, the LED does not provide for "consent" as a legal basis for processing, as consent would by definition not be free due to the power imbalance between the controller (e.g., the police) and the data subject (e.g., the citizen) (85 p. 12). To illustrate this, one can imagine that the subject feels a psychological compulsion to give such consent, e.g. from the police, because he or she has a legitimate fear of law enforcement authorities, even if there is no threat from

[50] Articles (2) (1) & (1) (1) LED.
[51] Article 8 LED.

their side. However, it is in the nature of their competence that they could - in practice - influence the free will of the person concerned. According to the LED's Explanatory Memorandum *"the data subject has no […] free choice"*[52].

Beyond that, however, there is another important difference between the Regulation and the Directive: the conditions for prohibiting "automated decision-making". The Directive primarily prohibits "automated decision-making", if it has "adverse" legal consequences for the data subject. In contrast, the GDPR prohibits "automated decision-making", if it has (merely) some legal consequences for the data subject. In other words, the Directive seems to be more flexible on automated decision-making, as it is only prohibited, if it has unfavourable ("adverse") legal consequences for the data subjects and not just some legal consequences (85)[53].

As to the right to human intervention, we note that the GDPR explicitly refers to the possibility for the data subject to challenge the automated decision. This is not provided for in the Directive, where the provision is less clear. However, human intervention without the possibility to evaluate and overturn the automated decision becomes meaningless (87) (85).

Finally, Article 11 (2) & (3) LED contains two important prohibitions for special categories of data. The first prohibition is about "profiling": *"Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law*" (4). Namely, the evaluation of special categories of data is prohibited, when the profiling results in discrimination[54]. The second prohibition concern the automated decision-making in general (except profiling): Automated decision-making concerning data of special categories could be possible in certain circumstances, namely if there is a legal basis[55] providing for the safeguards mentioned below[56]. The same reasoning is found in the Directive (EU) 2016/681 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. It

[52] Recital 35 LED.
[53] However, this difference seems to be mitigated afterwards. The above prohibition also applies under the GDPR, when the processing significantly affects the subject – even if it does not produce legal effects. The Directive states that the above prohibition also applies where it significantly affects the subject.
[54] Article 11 (3) LED.
[55] In EU or national law
[56] Article 11 (2) & 11 (1) LED.

states that "[s]*uch a list should not be based on a person's race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation*" (85). As we examined before, GDPR states, that the automated decision-making (concerning sensitive data) could be possible under strict preconditions, i.e. if there is an explicit consent of the data subject or a public interest. This is another indication that the legislator has chosen to treat the controller less strictly, when the controller is a competent authority which has as purposes the prevention, detection, investigation, prosecution, etc.

4.3. Privacy by design/Privacy by default

However, in addition to the above prohibition, there are other articles in the Regulation that concern AI systems, even if this is not explicitly provided for: e.g., Article (25), privacy by design and by default. This provision does not explicitly refer to artificial intelligence systems or to technical measures. It is therefore a provision that can, in principle, apply to any type of processing. However, it is considered to develop its scope mainly with regard to new technologies, in particular metadata, AI and IoT technologies (83).

With regard to the first paragraph, it states that the controller must take technical protective measures already by the design of a system. But what measures can the controller take to achieve data protection? The article itself refers to the measures of pseudonymisation and minimisation. However, the list is non-exhaustive in this case. The controller could also consider other technical measures. For example: a) anonymization, b) measures to prevent anonymized data from becoming personal data, c) erasure of data when they are no longer necessary for processing, d) distinct access rights for those acting on behalf of controllers, e) secure storage of personal data (83 pp. 205-206).

However, which of the above measures is the controller obliged to take? Could the competent data protection authority require each controller to take all the above measures? Pursuant to Article 25 (1) GDPR, the controller acknowledges several criteria[57], in order to choose the suitable preventive technical and organisational measures, balancing the cost against the risk.

[57] E.g. the costs, as well as the likelihood and severity of any risks.

A similar provision already existed in European Directive 95/46 [58]. However, the importance of technology and its intertwining with the law in the area of "informational privacy" [59] is reaffirmed here[60] (90).

Article 25 (2) GDPR concerns the protection of personal data by default. Under this principle, the controller is required to take suitable preventive measures to ensure that only the necessary data are preselected (i.e., "by default") (90). This principle is a specification of data minimization principle contained in Article 5 (1) (c) GDPR. In contrast to the above-mentioned paragraph, the legislator here does not even include an indicative list of such measures, but gives more discretion to the controller. In the following, we will examine what these measures might be.

Article 25 GDPR mentions that the controller is obliged to ensure in advance that data are not involuntarily accessible to unspecified individuals. It is obvious, even if it is not explicitly stated, that the European legislator intended to regulate the data processing concerning digital social networks, since the default settings in this area usually break the rules of data protection (91).

This principle therefore is broadly applied in the familiar "cookies" that we meet when visiting a website. If this website complies with the GDPR, it should collect by default only the necessary cookies (based on the minimisation principle), while giving us the possibility to change this default setting and click on the collection of more cookies that concern us, such as cookies related to our preferences used for targeted marketing purposes.

Privacy by design and privacy by default is also provided for in the LED (4), without substantial differences in relation to the GDPR.

[58] European Directive 95/46 constitutes the previous legal regime, which was replaced by GDPR.

[59] It is the privacy of personal information (213).

[60] i.e. Information and Communication Technologies are put at the service of the GDPR, in order to fulfill the legal obligation of the controller.

4.4. Data Protection Impact Assessment

Another provision that mainly relates to processing by technical measures[61] – as explicitly stated in the provision[62] - is Article 35 GDPR, which concerns the conduct of a DPIA.

What is an impact assessment? It is essentially a study and a compliance tool. In this study, the controller or processor[63] must describe in detail, in accordance with Article 35 (7), the following characteristics:

- the processing operations and the purposes of the processing
- an assessment of the necessity and proportionality of the processing in relation to the purposes[64] [65]
- an assessment of the risks to the rights and freedoms of the data subjects
- the measures planned to address the risks

Whether or not an impact assessment is required in a particular case follows from Article 35 (1). The legislator requires DPIA in cases *"where there is a high risk to the rights of data subjects"* (3).

However, the legislator has decided to list certain cases where there is a high risk to the data and therefore a data protection impact assessment is required, in order to provide legal certainty. According to Article 35 (3), an impact assessment is required in particular, when:

1. *"a systematic and extensive evaluation of personal aspects of natural persons based on automated processing, including profiling, takes place"*
2. special categories of data or personal data relating to criminal convictions and offences are processed on a large scale
3. systematic monitoring publicly accessible area takes place on a large scale

Analytical:

Cases (1) & (2): a typical example that applies to both the first and second cases is software that facilitates the controller's processing because it enables the controller to process a large amount

[61] Including AI systems.
[62] Article 35 (1) GDPR– Data protection impact assessment: *"using new technologies"*.
[63] Article 4 (8) GDPR.
[64] i.e. proportional related to the purposes.
[65] This assessment applies the principle of minimisation, which specifies, as already mentioned, the principle of proportionality.

of information. Although the use of arbitrary software is not strong AI, it is - as said above - the form of AI that is widely used today. For example, software for a) profiling bank customers or b) storing patient records by a hospital requires an impact assessment.

Case (3): regarding the third case, systematic surveillance can be conducted with or without the use of AI. However, it is possible that a video-surveillance system, especially if it is a large-scale systematic surveillance, may be accompanied by software that facilitates the detection of suspicious movements or individuals[66].

In addition to the above examples, the Art. 29 WP has also established certain criteria for conducting a DPIA. Specifically, an impact assessment is required when two of the following criteria are met (92) (83):

1. assessment or scoring, including profiling and prediction, in particular under several aspects,

2. automated decision making with a legally significant effect,

3. systematic monitoring,

4. sensitive[67] or data of a highly personal nature[68],

5. data processed on a large scale: The GDPR does not define what is a large scale, but could be: a. the number of data subjects, "b. the volume of data and/or the range of different data processed, c. the duration or permanence of the data processing, d. the geographical extent of the processing activity",

6. matching or combination of data sets,

7. data on vulnerable individuals. Vulnerable persons may include children, workers, mentally ill, asylum seekers, elderly, patients, etc.,

8. innovative use or application of new technical or organisational solutions, such as the combined use of fingerprint and facial recognition for improved physical access control, etc. For

[66] See below about biometric recognition.
[67] Article 9 GDPR
[68] Article 10 GDPR

example, certain applications of the IoT could have a significant impact on individuals' daily lives and privacy,

9. "*where the processing in itself prevents data subjects from exercising a right or using a service or* [entering into] *a contract*". This includes processing operations aimed at enabling, modifying or denying data subjects' access to a service or the conclusion of a contract. An example of this is when a bank matches its customers against a credit to decide whether to grant them a loan.

For the sake of clarity and legal certainty, the legislation also provides that the competent supervisory authorities shall publish operations for which a DPIA is required [69]. This provision is of great importance, as it is the competent supervisory authorities that detect breaches by controllers and impose appropriate sanctions. It is therefore important for the controller to know whether the activity he carries out requires an impact assessment to comply with the GDPR and not risk a fine.

At this point, it should be noted that this is essentially a new provision. Under the previous legal regime, the controller carrying out a high-risk processing only had to notify this to the competent data protection authority, and the latter could authorise or refuse such a processing.

Similarly, nowadays, the controller shall consult the Data Protection Authority, when the processing poses a high-risk [70]. This provision is also important because it enables the controller to properly comply with the Regulation and avoid possible sanctions.

A data protection impact assessment is also provided for law enforcement authorities when the processing of data may involve a high risk to the subjects. Inter alia, the provision emphasises that the high risk arises "*in particular*" from the use of new technologies. It also indicates that the risk assessment will consider several criteria[71]. The Annex also briefly mentions the content of a DPIA. As the Directive is not a directly applicable provision, the legislator did not choose to be exhaustive, but leaves more discretion to Member State legislators.

[69] Article 35 (4) GDPR.
[70] Article 36 (1) GDPR. Prior consultation.
[71] E.g., the nature, scope, context and purposes of the processing.

Art. 29 WP recommends that data controllers carry out a DPIA for any processing of sensitive personal data and for any processing that involves profiling. This recommendation stems from the fact that both "*categories of processing pose a high risk to the rights of data subjects*" [72] (85).

4.5. General provisions

In addition to the above "special" provisions, which relate exclusively or principally to processing operations carried out using new technologies, the "general" provisions of the Regulation, naturally apply to such processing operations, too. These provisions include data protection principles, legal bases for processing, special categories of data, rights of the data subject, records of processing activities etc.

To summarise, we will try to mention some important points from these general provisions.

According to Art. 5 GDPR, there are a few basic principles for processing: a) lawfulness, fairness and transparency, b) purpose limitation, c) data minimisation, d) accuracy, e) storage limitation, f) integrity and confidentiality, g) accountability.

The above principles are also found in the LED with a similar content[73]. There is an important difference regarding the principle of data minimization. The general principles in the LED do not include the principle of minimisation, but they provide that Member States shall provide for personal data to be sufficient, relevant and proportionate related to the processing's purposes. On the contrary, the GDPR provides for sufficient, relevant and limited to what is necessary. In practice, this means that law enforcement authorities are in principle not limited to collecting and processing only our adequate, relevant and absolutely necessary personal data.

Further, important is the article that defines the legal bases for processing[74]. In GDPR these legal bases are: the consent of the subject, the performance of a contract, compliance with a legal obligation to which controller is subject, protection of vital interests of the data subject or another person, the performance of a task carried out in the public interest or in the exercise of

[72] See Recital 51 & 52 LED.
[73] Article 4 LED
[74] Article 6 (1) GDPR.

official authority vested in the controller, legitimate interests pursued by the controller or a third party.

However, if the processing is of special categories of data[75] both one of the above legal bases and one of the following conditions must be met in order to permit the processing, as the processing of special categories of data is in principle prohibited (83 p. 129): the explicit consent of data subject, fulfilment of obligations and exercise of certain rights of the controller or the data subject in the field of employment and social security and social protection, protection of vital interests of the data subject or another person, if the data subject is unable to give consent, processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or other non-profit organization with political, philosophical, religious or trade union aim, data manifestly made public by the data subject, legal claims, substantial public interest, the processing is necessary for preventive or occupational health purposes, for the evaluation of the employee's health condition etc, public interest in the field of the public health, processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

As far as the Directive is concerned, Articles 8 and 10 apply mutatis mutandis. Article 8 LED refers to the legal basis for the processing: the performance of a task by a competent authority under two conditions[76]: First, the processing is carried out for the purposes in Article 1 (1), namely "*the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*[77], and second, the processing is based on Union or Member State law. With regard to lawful processing of sensitive data of citizens (i.e. special categories of data), competent authorities must comply with both Art. 8 and Art. 10 LED. Namely, the processing must be authorised [78] by Union or Member State law or required to protect a vital interest, or finally made public by the data subject[79]. However, as mentioned above, it is possible to provide for specific provisions

[75] Article 9 GDPR

[76] Article 8 LED.

[77] Article 1 (1) LED

[78] Art. 8 LED refers to processing based on Union or Member State Law, while Art 10 LED refers to processing authorised by Union or Member State Law. This means that the law must provide explicitly for the processing of sensitive data.

[79] Article 10 EU LED

for the data processing for automated decision-making, setting out further conditions for the lawfulness of the processing[80].

The rights[81] of the data subject in the GDPR are[82]: "*transparent information, communication and modalities for the exercise of the rights of the data subject", "information to be provided where personal data are collected from the data subject, "information to be provided where personal data have not been obtained from the data subject", "right of access by the data subject", "right to rectification", "right to erasure ('right to be forgotten'), "right to restriction of processing", "notification obligation regarding rectification or erasure of personal data or restriction of processing", "right to data portability", "right to object" and "automated individual decision-making, including profiling"* (3 pp. Art. 12-22).

The rights in the LED[83] are quite different, even if they have a similar subtitle as the GDPR: notification for the exercise of the rights, information to be provided or given, access to personal information, limitations to the right of access, erasure of personal data and restriction of processing, exercise of rights and verification by the supervisory authority, rights in investigations and proceedings.

As for the records of processing activities, the controller must keep a register containing the information such as the categories of data, the purposes, the legal bases etc[84]. All the above information is important in order for the controller to prove that he is complied with the principles of accountability and transparency. In this way, the controller can easily let the data subject know processing's details and the competent supervisory authority can effectively monitor compliance with data protection and, if necessary, impose sanctions.

Codes of Conduct. Another important article of the GDPR is Article 40 et seq., which provides for the development of codes of conduct. According to Article 40, a code of conduct is a compliance tool, i.e., it is optional and never mandatory. This Article covers both processing by technological means (e.g. AI) and processing without such means. However, a code of conduct

[80] See Article 11 (2), (3) LED.

[81] Although the subject's rights are of great importance for the compliance with data protection in general, they are not crucial for our research and we will not analyze them, because the Proposal for the AI Regulation does not define different rights for the data subjects. So, they could not be a subject of our further study.

[82] Article 12 – 22 GDPR.

[83] Article 12 – 18 LED.

[84] Article 30GDPR.

is of great importance when processing is carried out on a large scale, i.e., usually by technological means.

What is the function of this compliance tool? What are its advantages? First of all, it is important to define as precisely as possible both the procedures used by the controller and the criteria taken into account in each processing. In this way, the procedure becomes transparent, a sense of security and trustworthiness towards the controller is created, especially when the relations between the controller and the data subjects are impersonal (e.g. on the Internet), and limits are set to the arbitrariness of the controller[85].

[85] Respectively, see "*Code of conduct on countering illegal hate speech online*" (255).

5. Modern artificial intelligence practices

5.1. General

5.1.1. Prohibited artificial intelligence practices

The AI ACT – according to its explanatory memorandum – aims to regulate issues relating to user's health, safety and fundamental rights, as protected by Union law (1) (2). It also seeks to ensure the free movement of new technologies in EU, without arbitrary restrictions on the part of the Member States. In any case, it is considered that the establishment of rules on AI issues is necessary, as there is no relevant regulatory framework. After all, even at national level, only a few states have studied and are working on establishing relevant rules.

Reading the text of the proposal itself, we can see that the key regulations are divided into two categories in Articles 5 and 6. In particular, the Regulation seeks to define prohibited practices in the field of artificial intelligence and high-risk practices.

As regards prohibited practices, the following are mentioned:

"TITLE II PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES Article 5

1. The following artificial intelligence practices shall be prohibited:

(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order 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;

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order 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;

(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

(d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific potential victims of crime, including 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 in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State […]" (1).

The first two references to prohibited systems do not - in principle - concern the data processing. However, on the one hand, we consider them to be very important, and on the other hand, we believe that they could have a relation to personal data upon further examination. For this reason, we will briefly discuss them.

First, we note that in both the first (a) and second (b) cases, the Regulation prohibits those AI systems that are designed "*in order to materially distort a person's behaviour, in a manner that causes or is likely to cause that person or to another person*". This phrase represents the principle of prevention of harm, which we examined above[86]. This damage is the further result of AI's use, regardless of whether the user intended it or not.

The EU Act also specifies the prohibited AI practices. For example, it is forbidden to *"deploy subliminal techniques beyond a person's consciousness*" (a) or to "*exploit any of the vulnerabilities of a specific group of persons due to their age physical or mental disability*" (b). This concerns practices related to the mental state and health of the user, which is a main objective of this Regulation,

[86] See above, Chapter 3.4.

as can be seen from its explanatory memorandum and already mentioned above. Also, the protection of physical and mental integrity[87], the right to liberty and security[88], as well as to freedom of thought and conscience[89], the rights of the elderly[90], but also the rights of persons with disabilities[91], are fundamental human rights, which are enshrined in the CFR, which apply in any case, but whose protection is at the same time the objective of this Regulation.

Moreover, a common element of the above cases is that the legislation prohibits these AI practices at every stage of the supply chain. It clearly prohibits their use by the final consumer, their positioning in the market by the supplier and the trader, but also their use in general. Interpreting this provision, one could conclude that its development by the manufacturer is also covered by the prohibition.

As for the first prohibited practice, the legislator's fear of such use of AI is understandable. It could have fatal consequences for those involved. It almost seems like a science fiction scenario that we would not be able to control our thoughts and reactions. However, if we think a little more carefully, we will remember that something similar has already taken place in the past. In the 1950s, rapidly fast advertisements of "Coca-Cola" were shown in cinemas. The viewer was not aware that he had seen the image of "Coca-Cola", but these fast images were enough to imprint the product in the viewer's subconscious (93). In 1957, the book "*The Hidden Persuaders*" argued that this could also be done with election candidates to influence their outcome. For this reason, many states in the U.S.A. have directly banned the use of subliminal advertising. Recent studies have shown that a monkey can successfully play a game using a brain-computer interface (94) and that software can intercept our bank codes, taking into account the brain's response to visual stimuli (93).

The latter practice clearly involves the processing of personal data. Why did the legislator not intend to include it in the scope of Article 5? In his opinion, is it not just a high-risk practice? Could it be based on the consent of the data subject? We believe that the control of the subconscious is so dangerous in itself that in the end it is not important to attach conditions to

[87] Article 3 CFR
[88] Article 6 CFR
[89] Article 10 CFR
[90] Article 25 CFR
[91] Article 26 CFR.

its legitimacy. Indeed, it should be a prohibited processing, whether or not it leads to physical and psychological harm, whether or not it leads to illegal processing of personal data. This is a challenge for artificial intelligence, about which we know very little and whose consequences we cannot precisely determine. Therefore, it seems somewhat dangerous to prohibit it only under certain conditions.

The second prohibited practice could be that it refers - inter alia - to autonomous robots for personal assistance. The latter should be treated with special care so that they do not endanger vulnerable populations such as the elderly and children. This is also clear from the explanatory memorandum of the AI ACT[92], which states that the classification of autonomous robots for personal assistance and care (including in the healthcare sector) as high-risk (or possibly prohibited) depends on the level of risk involved.

This case could also be related to the data processing. If someone exploits a child to obtain pornographic material, then this processing involves personal data. Why is only a practice that directly harms a child physically and psychologically prohibited, and not any practice that exploits a child in any way and may cause significant risks and consequently psychological harm to the child?

The next two categories of prohibited practices concern the processing of personal data.

In the following[93] the third case (c), which concerns the *"evaluation or classification of the trustworthiness of natural persons"*, will be examined in detail.

In addition, in the fourth case (d), the Proposal refers *"to the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement"*. We will then examine in detail remote biometric facial identification systems in publicly accessible spaces under video surveillance for law enforcement purposes. However, this chapter also covers any biometric identification of an individual or other person that occurs under the above conditions. In the following, we will deal with further processing of biometric data in high-risk systems and approach its concept.

[92] Recital 28 AI ACT.

[93] See below, Chapter 5.2

5.1.2. High-risk artificial intelligence practices

5.1.2.1. General

In addition to the prohibited AI applications mentioned above, the proposal for the Regulation provides for a number of high-risk practices, which divides into two broad categories. In the first category it mentions some general characteristics of high-risk practices, while in the second category it lists some of them, referring directly to the Annex III to the Regulation.

In particular, the first category of high-risk systems includes the AI system which:

(a) "*is intended to be used as a safety component of a product, or is itself* [such] *a product*", and

(b) "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]"[94].

While the second category of high-risk systems includes specified practices, here, there are the main categories of them:

1. Biometric identification and categorisation of natural persons
2. Management and operation of critical infrastructure
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes

In the following, we will briefly examine only some of the practices mentioned above, which also concern the processing of personal data. We have already mentioned above that not all the practices mentioned in the Act constitute processing of personal data.

The first case is mentioned under the title of *"biometric identification and categorisation of natural persons"*. However, in the further text, the term categorization is missing. To be precise, we must assume that all cases of biometric identification fall under the risky practices, whether they lead to the classification of an individual or not, whether they take place in real time or not (see

[94] Article 6 (1) AI Act.

Article 6 (1) AI ACT), except for those that fall under the prohibited practices. These include cases such as fingerprinting at border controls, entry controls at private companies or public services, etc. The concept of biometric data and biometric facial identification will be analysed below[95]. Suffice it to mention here that biometric data are those characteristics that can accurately identify us, such as our fingerprint, precise facial dimensions or DNA.

In addition, according to the individual practices of the Annex, the use of AI for profiling and in particular, for assessing and accepting/rejecting a prospective student at college, hiring a prospective employee, eligibility and access of a citizen to social benefits or banking products, the risk assessment of a suspect in relation to the (re)occurrence of a criminal offence, the assessment of his psychological state, the use of a lie detector, the risk assessment for an immigrant seeking to enter a Member State, and the use of AI systems for judicial decisions are also considered as high-risk.

Below we will examine some of the above cases that seem interesting.

5.1.2.2. Automated Fingerprint Identification System (AFIS)

Since the mid-2000s, many EU countries, as well as the U.S., Canada, China, Africa, and the Middle East, have used this method to control their borders and those entering their countries. In addition, all countries usually require dactyloscopy to issue a visa. International organizations, such as nongovernmental organizations like the Office of the United Nations High Commissioner for Refugees (UNHCR), also use fingerprint identification to identify refugees in aid programs, using portable, battery-powered devices in remote areas (95) (96 pp. 3-7).

However, not only law enforcement, but also other public authorities and the private sector are now using fingerprint identification. Sometimes workers' access to their workplace is identified with their fingerprint, but so is the access to smartphones (96 pp. 3-7).

Today, the digitization of databases makes such identification very easy and effective. Access to an area with particularly sensitive personal data can now be easy and secure because the

[95] See below, Chapter 5.2.

employee's fingerprint is sufficient. It is, in fact, more secure than a password, which can be intercepted. Similarly, using a fingerprint to unlock a mobile device's files makes them more secure. However, in both cases, the principles of the GDPR should be followed, especially the principle of minimisation, which seems to play a role here. Therefore, the employee's fingerprint should not be required instead of the classic employee card ID, but only when entering a particularly sensitive area where the processing of biometric data is deemed necessary, and only if the conditions for fair processing under Articles 6 and 9 of the GDPR are met. As for the use of a fingerprint on the mobile phone, this is clearly at the discretion of the user and is take place with his or her consent[96]. However, it is essential to verify that the user is aware of the risks of interception in the context of cybercrime. In conclusion, security, not convenience, should be a criterion for the use of such data.

AFIS is a modern dactyloscopy system using AI. "*The Schengen Information System (SIS) is a large-scale IT system that supports public security and the exchange of information on people and objects between national law enforcement, border control, customs, visa and judicial authorities. […] After two years of intensive efforts, in the beginning of 2018 eu-LISA successfully launched the SIS Automated Fingerprint Identification System (AFIS) platform. SIS AFIS meets the demands of the European law enforcement community to have an advanced tool, at EU level, enabling the identification of persons of interest by their fingerprints alone"* (97).

The processing of biometric data, we already know, does not necessarily require AI systems. However, the SIS II AFIS system is automated.

According to the Regulation 2018/1862, applied here,[97] the controllers must respect the principle of purpose limitation and the principle of minimization. Only the necessary data must be used for specific, explicit and legitimate purposes, especially for the processing by the AFIS.

In addition, there are also measures to mitigate the risks arising from automated decision-making, e.g. human intervention. In particular, after matching and before making a decision, specialists must perform further checks to confirm that the suspect owns the fingerprint stored in the database.

[96] Article 9 GDPR.

[97] Especially: Article 43 (2) Regulation 2018/1862, Recital 23 Regulation 2018/1862.

Similar databases with fingerprint data, but related to immigration, are "VIS" and "EURODAC"[98]. *"The Visa Information System (VIS) allows Schengen States to exchange visa data. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States". "Eurodac is a large-scale IT system that helps with the management of European asylum applications since 2003, by storing and processing the digitalised fingerprints of asylum seekers and irregular migrants who have entered a European country. In this way, the system helps to identify new asylum applications against those already registered in the database"* (97).

5.1.2.3. "Keystroke dynamic" and other modern practices of biometric identification

Nowadays, further biometric recognition techniques are increasingly being developed. Technological advances are constantly evolving, so that more and more secure conclusions can be reached over time. Some *"Biometric Identification Technologies Based on Modern Data Mining Methods"* that are still under research are the followings: (a) "*Triangulation Method in the Biometric Identification Process*", which is based on the *"faceprint"*, due to the fact that everyone has a potential key in a 3D view of their characteristic facial line" (98). (b) *"Biometric Gait Identification Systems*": This research is trying to solve the major problems with the common gait biometric systems (99). (c) "*Interactive Biometric Identification System Based on the Keystroke Dynamic":* In this research, "*algorithms for the formation of characteristic features and user identification are* [described]", using fixed and arbitrary key sequences (100). (d) "*Analysis of the Dynamics of Handwriting for Biometric Personality Identification Based on Cellular Automata*": An analysis of the dynamics of the movement of the hand during writing a person's text is used, because the use of statistical images of handwritten text often leads to false identification (101), (e) *"Identification of a Person by Palm Based on an Analysis of the Areas of the Inner Surface*" (102), (f) "*Research of Biometric Characteristics of the Shape of the Ears Based on Multi-Coordinate Methods*" (103).

[98] REGULATION (EU) No 603/2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast).

5.1.2.4. Video legitimation in banks

The use of facial recognition systems is already popular with private companies. For several years, for example, "Facebook" was able to recognize our face in photos posted by third parties through its database using algorithms. However, the company has already eliminated this capability (by default) as it violates personal data protection (96). Similarly, "Clearview AI" provides biometric images of individuals posted somewhere on the Internet to private and public entities or even law enforcement agencies. Just recently, the "Hellenic Data Protection Authority" fined the company 20,000,000 euros for this processing (104)[99]!

In recent years, banks, in order to serve their customers, have the ability to identify them remotely, if necessary. The identification process with username, password and a confirmation code on our smartphone (e.g. SMS) is well known. However, there are some cases or specific transactions that require a different type of identification: remote facial identification. A secure software where facial features are captured, identified and possibly automatically deleted after identification, is suitable for important remote bank-transactions, when password is considered an insufficient security tool. Therefore, such a method seems to be increasingly attractive in the private and public sectors.

At this point, we should also clarify the following. Not all photos or all videos are biometric data. Most of them are probably just personal data. In order to be biometric data, photos and videos must meet certain accuracy requirements and allow identification of a person's identity[100].

5.1.2.5. Visa Information System (VIS)

Intelligent biometric identification systems are already in use in all European countries. These are systems used in border controls, both in migration[101] and in police (e.g., to identify missing

[99] Hellenic Data Protection Authority 35/13-7-2022 (104).

[100] Recital 51 GDPR.

[101] Regulation EU 2018/1861, *"Specific rules for entering biometric data (Art. 32) Specific rules for verification or search with biometric data (Art. 33) […] Facial images and photographs should, for identification purposes, initially be used only in the context of regular border crossing points. […] (Recital (20))", Regulation EU 2018/1860, "'Facial image' to be inserted in alerts on return only to confirm the identity of the person (Art. 4)".*

persons crossing the border)[102]. These systems are provided for in SIS II, which we examined above in relation to AFIS.

The "SIS II" system is governed by the LED and other specific provisions[103]. The controllers are national authorities or European institutions and the purposes of the processing are to a) "*support implementation of policies on border* [controls] *and immigration*" and b) to "*safeguard security in the EU and in Schengen Member States*" (105 p. 14).

Specifically, with regard to law enforcement at the domestic level[104,] the following is stated: The purposes of lawful processing - defined in Regulation 2018/1862 - are the following: "*Alerts on persons and objects for discreet checks, inquiry checks or specific checks*" [105], "*Alerts on objects for seizure*

[102] Regulation EU 2018/1862, "Specific rules for entering biometric data (Art. 42) Specific rules for verification or search with biometric data (Art. 43). […] Facial images and photographs should, for identification purposes, initially be used only in the context of regular border crossing points. […]" (Recital (22)).

[103] REGULATION (EU) 2018/1860 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, REGULATION (EU) 2018/1861 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, REGULATION (EU) 2018/1862 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

[104] REGULATION (EU) 2018/1862 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, CHAPTER XIII Right of access and review of alerts Article 44 National competent authorities having a right to access data in SIS, "*1.National competent authorities shall have access to data entered in SIS and the right to search such data directly or in a copy of the SIS database for the purposes of: […] (b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities; (c) the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies".*

[105] Chapter IX. Article 36 etc. Regulation (EU) 2018/1862

or use as evidence in criminal proceedings" [106] [107], "*Alerts on unknown wanted persons for the purposes of identification under national law*" [108].

Regarding the nature of personal data, the following data may be collected and processed: Surnames, first names, maiden names, previously used names and aliases, any specific, objective, physical characteristics not subject to change, place of birth, date of birth, gender etc., but also data of special categories, such as the following biometric data: photographs and facial images[109], relevant DNA profiles in accordance with Article 42 (3)[110] and dactyloscopic data[111] [112].

In addition, similar facial recognition systems were submitted for approval in 2018 and 2016, respectively, in the context of VIS and EURODAC, aimed at law enforcement and other purposes (105 pp. 13-15).

Relevant regulations amending the current regulations VIS have already been issued in 2021. In view of the risks involved and with particular regard to the data protection, it is now provided that: "1. *An independent VIS Fundamental Rights Guidance Board with an advisory and appraisal*

[106] Chapter X. Article 38 etc. Regulation (EU) 2018/1862

[107] It is doubtful whether a comprehensive processing of biometric data in No. 38 will take place, because of its purpose, after applying the principle of proportionality. However, this will be judged on a "case-by-case" basis.

[108] Chapter XI. Article 40 etc. Regulation (EU) 2018/1862 *"Member States may enter into SIS alerts on unknown wanted persons containing only dactyloscopic data. Those dactyloscopic data shall be either complete or incomplete sets of fingerprints or palm prints discovered at the scenes of terrorist offences or other serious crimes under investigation. They shall only be entered into SIS where it can be established to a very high degree of probability that they belong to a perpetrator of the offence.*
If the competent authority of the issuing Member State cannot establish the identity of the suspect on the basis of data from any other relevant national, Union or international database, the dactyloscopic data referred to in the first subparagraph may only be entered in this category of alerts as 'unknown wanted person' for the purpose of identifying such a person".

[109] Article 3 Definitions *"For the purposes of this Regulation, the following definitions apply: […] (14) 'facial image' means digital images of the face with sufficient image resolution and quality to be used in automated biometric matching;".*

[110] Article 3 Definitions "*For the purposes of this Regulation, the following definitions apply: […] (15) 'DNA profile' means a letter or number code which represents a set of identification characteristics of the noncoding part of an analysed human DNA sample, namely the particular molecular structure at the various DNA locations (loci);"*

[111] Article 3 Definitions "*For the purposes of this Regulation, the following definitions apply: […] (13) 'dactyloscopic data' means data on fingerprints and palm prints which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;"*

[112] "CHAPTER V Categories of data and flagging Article 20 Categories of data.

function is hereby established. Without prejudice to their respective competences and independence, it shall be composed of the Fundamental Rights Officer of the European Border and Coast Guard Agency, a representative of the consultative forum on fundamental rights of the European Border and Coast Guard Agency, a representative of the European Data Protection Supervisor, a representative of the European Data Protection Board established by Regulation (EU) 2016/679 and a representative of the European Union Agency for Fundamental Rights"[113].

Regarding EURODAC, it is reported that it has not yet collected biometric facial data, at least until January of this year (106).

Moreover, the European Union reports officially that: "*The processing of facial images is expected to be introduced more systematically in large-scale EU-level IT systems used for asylum, migration and security purposes. These images will be taken in controlled environments – for example, at police stations or border-crossing points, where the quality of the images is higher compared to that of CCTV cameras. Police body cameras (Axon) to announce this year that it would not deploy facial recognition technology in any of its products – because it was too unreliable for law enforcement work and" "could exacerbate existing inequities in policing, for example by penalising black or LGBTQ communities" "gainst this backdrop, a number of questions arise from a fundamental rights perspective: is this technology appropriate for law enforcement and border management use [?] Which fundamental rights are most affected when this technology is deployed – and what measures should public authorities take to guarantee that these rights are not violated?"* (105)

Based on the above, we note that the expanded use of facial recognition systems in law enforcement is likely to be a reality soon. While photo review may provide more certain conclusions than surveillance video, in such a video that collects biometric data, it will be possible to analyse perhaps other data besides our face, such as a suspect's gait.

However, at train stations or other key points where there is a controlled entrance, would it be possible to ask for a photo of the person entering so that we can draw safe conclusions? Or, as time goes on and technology develops, could we even use videography to obtain clear images from which we could draw conclusions as certain as from a photograph? The ease of use of remote facial identification bypasses the obstacles of fingerprinting, and therefore pilot

[113] Article 9i Regulation (EC) No 767/2008, as amended with the Regulation2021/1134.

applications for such systems are being conducted around the world to test their reliability and improve their effectiveness.

5.1.2.6. The software "Compas" or "robo-judge" after all?

At this point, it is important to mention an example of artificial intelligence in the context of automated decision-making. An interesting programme has been developed in the context of the judiciary. In at least ten U.S. states, software called "Compas", developed by a private American company, is used to calculate the risk of a repeat offence. As it is known, the criteria of this programme are the criminal record of the offender, the information provided by the offender himself in a special questionnaire and the facial expressions and body language of the offender. By creating an automated profile of the defendant, the judge receives a "score" to evaluate a natural person's risk of delinquency or recidivism. If the percentage is high, the judge decides not to grant a stay of execution but to imprison the offender. However, experts accuse the software of attributing a higher risk of re-offence to black offenders than to whites (107).

Could this system be introduced in the EU?

In the above example, it is clearly that automated decision-making produces legal effect for the data subject. A crucial issue is the role of the judge. The judge must not completely trust the conclusions of the AI system. He must judge considering various relevant criteria· otherwise, the principle of a fair trial is violated[114].

In fact, under European law, meaningful human oversight is mandatory. In any case, it is well known that the training of AI systems is crucial for their decisions. So, if an error or a failure has been implanted in the training, it is possible that there will be misguided results with catastrophic consequences. So, if the decision to imprison a person is based to biases, it could lead to violation of equal treatment of people[115].

[114] Article 6 ECHR, right to a fair trial.

[115] Article 21 CFR, Non-discrimination, Article 14 ECHR, Prohibition of discrimination, Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation

In the Wisconsin Supreme Court's Loomis case, the justices relied on the "Compas" system, the exact operating parameters of which could not be disclosed because of the principle of confidentiality and trade secrecy (108). This decision has been criticised for being insufficiently reasoned and for violating the principle of a fair trial. If such cases were to be judged by European standards, it would be said that, in addition to the principle of fair trial and the principle of equal treatment, the principle of transparency[116] is also disregarded[117] (109).

5.1.2.7. Artificial intelligent system analysing the emotional state of the customers

Another case of the use of AI systems that involve processing of personal data but are not covered by the Annex III of the Act, are the assessment of customers based on their emotional state.

Just recently, the Hungarian data protection authority fined a bank EUR 670,000 for recording conversations with its customers while servicing them and then automatically assessing their satisfaction by analysing their voice with an AI system. The authority concluded that such a processing was not justified.

Specifically, data protection authority stated that the processing was unlawful. There was not any legal basis. The legitimate interest cannot apply here as a legal basis, because the proportionality principle is violated: this data processing is not necessary for the purposes of the bank. Besides, the authority stated, that the bank carried out a relevant DPIA, but there were significant mistakes. The DPIA showed, that the processing was of high risk, but the measures that the bank proposed, to address the risk were insufficient (110).

(recast), Directive 2011/61/EU of The European Parliament and of The Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (Text with EEA relevance).

[116] The principle of transparency requires that the subject know which of his personal data are processed, i.e., in this case, the data subject has the right to be informed of the criteria used by the software system to draw conclusions (109).

[117] The use in Europe of any biased and therefore inaccurate data, derived from an automated algorithmic model, would violate not only the Article 22, but also the principles of legality, objectivity and transparency of processing, as defined in Article 5(1) GDPR (3).

5.1.2.8. Mobility

An extremely important AI practice, that was also not included into the ANNEX of the AI ACT is clearly the one related to smart cars. The Annex only includes a reference to transportation infrastructure projects, while it does not include smart cars, that are about to be deployed.

There is a lot of progress in this area as well, and intelligent "semi-autonomous" cars are already on the market - more or less widely used. "*The automotive AI market reached $783 million in 2017 […] [while] by 2025, AI could reach an annual value of about $215 billion for the automotive industry*". AI-based functions in autonomous cars include object recognition, virtual assistance, voice recognition, automated driving, etc (111).

According to the Federal Council of Germany, the fact that the Proposal does not include a reference to smart cars is an omission of the AI ACT, as autonomous vehicles are a very important category that is thus not regulated (58). Liability issues, as well as the processing of personal data (e.g., the collection of the vehicle's license plate number, location, etc.) are not provided for in the new regulation. This is scandalous. The Commission should definitely include practices related to smart cars in the above-mentioned categories of the AI ACT, as smart cars will soon be one of the most important areas of daily use of AI systems by the majority of EU citizens.

5.2. Video-surveillance with biometric identification for law enforcement

5.2.1. The scope

5.2.1.1. General

The topic we will address in this chapter concerns biometric facial recognition through video surveillance in publicly accessible spaces for law enforcement purposes. To better understand the above, in the following we will try to approach the concept that is the framework of this chapter: firstly, the video-surveillance and, then, the biometric identification.

At this point, we need to recall our scope. We will examine this issue only in the context of law enforcement by Member States (and not by Union institutions) and only for law enforcement purposes within each Member State (while the use of biometric identification systems for in-country control, e.g. of migrants, or for cross-border cooperation is not our subject).

5.2.1.2. Video-surveillance

Video surveillance systems are already widely installed across Europe, both by private individuals (to protect their property and lives) and by private companies and public authorities for security and law enforcement purposes. So far, however, these systems do not process biometric data, but only simple images.

According to the European Data Protection Supervisor, "*[v]ideo-surveillance footage often contains images of people. As this information can be used to identify these people either directly or indirectly (i.e. combined with other pieces of information), it qualifies as personal data (also known as personal information). Almost all EU institutions and bodies have video surveillance in operation on their premises: from small executive agencies with only a few cameras (CCTV), to EU institutions and bodies with seats in a number of Member States operating several hundreds of cameras; all EU institutions and bodies using CCTV have a publicly available policy outlining what they do and why. Well-designed and selectively used video-surveillance systems are powerful tools for tackling data security issues; badly designed systems merely generate a false sense of security while also intruding on our individual privacy and infringing other fundamental rights*" (112).

Video surveillance systems operate - at least to date - without capturing biometric data[118] from passersby. That is, they do not identify a person on their own (e.g., by the characteristics of their face or gait), nor do they draw other inferences about the profile of passersby (i.e., they do not indicate danger when someone attacks a victim or when someone is generally in danger). In short, they are not intelligent systems, they do not contain AI software. They are traditional cameras that, for example, display their footage in real time in a company's guard room and/or store the footage (for a specified retention period) for later use if needed, such as in the event of a break-in.

Based on the above, two points should be noted. First, the data that the controller processes are necessary and sufficient for the purpose of the processing. Second, the data are kept for a very short period to minimize the risk of a data breach (112). In this way, the controller complies with the principle of data minimization and the principle of storage limitation[119].

Combine such a video surveillance system with an AI system that compares and identifies the received images with a database containing biometric data, man could have a remote biometric identification (RBI) system. However, a biometric identification system with AI need to process clear pictures, to be possible to identify people. Such a system can identify the people in real time or later. In any case, it is referred to as a RBI system (113).

5.2.1.3. Biometric identification for law enforcement through history

As mentioned above, the proposal for the European AI Regulation addresses the question of whether it is fair to use biometric data for law enforcement, as well as for the individual conditions.

We have already seen in the review of the GDPR and the LED that biometric data is primarily sensitive data. But what exactly is the biometric data we will deal with in this chapter?

According to the definition given in the EU legislation, *"'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural*

[118] See below the definition, chapter 5.1.3

[119] Article 5 GDPR.

characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"[120].

To better understand the above definition, it is useful to list some examples of biometric data. We note that the definition refers to three categories of biometric data: the physical, the physiological and the behavioural. First, the physical characteristics are those that can be recognised directly, such as the colour of skin, hair and eyes (114). Physiological features include, for example, the fingerprint, the entire physiology of hand, the iris of eye, and retina. A typical example of biological data is DNA. Behavioural characteristics are the timbre of voice, the way man walks, or even handwriting.

According to the definition above, biometric data are those that enable the identification of a person, but how and why does this happen? All biometric data are unique to each person. Therefore, we can conclude that the processing of biometric data (e.g. fingerprints) can safely show who has been in a certain area.

Biometric data are not only unique, but in principle cannot be altered. Exceptionally, some physiological biometric data can be altered due to illness or accidents. For example, a severe burn on the fingers can change our fingerprint (86).

In addition, another important question arises: How were biometric data originally linked to law enforcement?

Even ancient civilizations knew the uniqueness of fingerprints and used them as the signature of citizens. This is also evidenced by vessels that have been found. The ancient Egyptians used the fingerprint to ensure that food provided by the state was divided equitably among those who were rightfully entitled to it (96), Babylonians used the fingerprint as a signature on contracts[121] to prevent forgery (115) and the Chinese took fingerprints to identify a person (96).

The uniqueness of fingerprints seems to have been forgotten along with the techniques of ancient civilizations, and even when the German physician and anatomist J. C. Mayer [122]

[120] Article 3 (33) AI EU ACT, Article 4 (14) GDPR & Article 13 (3) LED.
[121] On clay vessels.
[122] Johann Christophe Andreas Mayer (12/1747 in Greifswald – 11/1801 in Berlin). In 1778 he became professor of medicine at the University of Frankfurt and there he, also, began his eight-volume work on anatomy (116).

rediscovered in 1788 that fingerprints are unique to everyone (116), no one was particularly concerned. In the mid-nineteenth century, Jan Evangelista Purkinje noted the same thing[123] (117).

A few years later, Francis Galton[124], influenced by the work of Darwin, who was his second cousin, developed a method of classifying fingerprints that proved useful in forensic science (118). After reading an article in a journal about Francis Galton's experiments with fingerprints, Juan Vucetich[125] began collecting fingerprints of arrested men and soon developed a useful system for classifying fingerprints called "dactyloscopy" (119). "*In 1900, the Argentine Republic began issuing a [type] of passport that included fingerprints*" (119). And in 1904, Vucetich's publication on "dactyloscopy" reached other countries and "*helped spread his system throughout the world*" (119).

At the same time, in 1897, the Indian government published Edward Henry's monograph "*Classification and Uses of Fingerprints*"[126] (120). Henry's classification system provided a method for classifying fingerprints and established the fingerprint as the basis for individual identification and as the basis for fingerprint databases (96). His system was adopted by several law enforcement agencies, most notably Scotland Yard, and was further developed throughout the twentieth century (121).

Shortly before Vucetich, in 1879, Alphonse Bertillon[127], invented a method that combined detailed measurement and classification of unique characteristics of suspects. Bertillon used measurements and photographs of head length, head width, length of the middle finger, and other physical features and kept records ("anthropometry"). Finally, in the early twentieth century, Bertillon's filing system became a model system for tracking and controlling individual

[123] Jan Evangelista Purkinje (1787–1869), Czech scientist, who established that fingerprints were unique (117).
[124] Sir Francis Galton, (2/1822 –01/1911), was an English polymath (215) (118).
[125] Juan Vucetich (1858–1925) was an Argentinian police official, who devised a workable system of fingerprint identification which contributed to forensics (119).
[126] Sir Edward Henry (1850–1931) was Commissioner of Police in London from 1903 to 1918 and introduced the method of fingerprinting to identify criminals (120).
[127] Alphonse Bertillon (4/1853 – 2/1914) "was a French police officer and biometrics researcher. He applied the anthropological technique of anthropometry to law enforcement creating an identification system based on physical measurements" (216).

citizens and immigrants, while police departments began to use Bertillon's method for photographing crime scenes (122).

5.2.1.4. Contemporary remote biometric identification in public spaces for law enforcement

Anthropometric techniques did not provide as reliable results in the past because of specific problems. The measurements were often not accurate, but were influenced by the errors of the people taking the measurements. Technology though could eliminate this risk. Anthropometry, such as facial recognition, is nowadays applicable by automated means. The use of technology generally implies the modernization of several old methods in different fields.

"*Contemporary biometric facial recognition is a digitalised extension of facial mapping, utilising an algorithm to undertake the comparison […] The process of verification is undertaken through one-to-one matching: the live comparison of a face with a digital template stored in an identity document, such as a person presenting a passport at border control. In contrast, identification occurs through one-to-many searching: databases of images or CCTV footage are searched in an attempt to establish a match with a photograph of an unknown person*" (96 p. 22). In addition to verification and identification, facial recognition technology is also used to obtain information about a person's characteristics, such as gender, age, and ethnicity (105). It can, therefore, also be used for profile individuals (123).

As we have seen above, biometric recognition is becoming increasingly popular due to the development of science and especially technology. The use of artificial intelligence is crucial for the use of all these tools. The use of algorithms allows us to compare photos or fingerprints or other biometric data of so many people in a short time to identify a person. The use of algorithms could also allow us to obtain certain results in terms of biometric data from a video. Physical characteristics, the way a person moves, can provide information on whether they should be classified as a suspect.

Facial recognition techniques now seem very attractive to law enforcement, although they have some drawbacks. It is still quite difficult to guarantee the accuracy of the algorithms during matching (e.g., the obtained images with the database). Several errors have already been observed during matching. The systems themselves are responsible for many of these errors, as

pilot studies with volunteers have shown[128]. What happens if someone intentionally tries to influence the system, or if there are objective facts that could influence the system? If we do not update a database with recent photos, could the change in our appearance over the years contribute to this error? Will AI systems have another difficulty in matching? (96 pp. 21-29)

However, at a crime scene, multiple biometrics of the perpetrator can be used in combination (facial recognition, fingerprint, DNA) to overcome possible unreliable results. In any case, all difficulties must be addressed, because there is an objective truth: the ease of use of biometric face recognition is unparalleled. For example, biometric recognition could be applied to the already existing video-surveillance systems in public access areas [129] (with an appropriate upgrade of both hardware and software) to enable real-time control, while it is possible to enrich the already existing databases of identities, passports, driver's licences, etc., with our photos that meet the specifications of biometric recognition, since there are already corresponding databases of analogue photos (96 pp. 21-29).

We have seen so far, the possibilities of biometric identification using AI. In the following, we will see some modern real-world examples of biometric facial recognition for security purposes. In the UK, street cameras with facial recognition technology have already been tested to identify people in real time. In Hungary, there are plans to deploy cameras with facial recognition capabilities throughout the country to capture facial images to maintain public order, and the Czech government is planning the same for Prague International Airport. In addition, France and Germany have tested some facial recognition systems on a trial basis with volunteers (105 p. 3)

As for France, *"[t]he police in Nice (France) conducted a trial of live facial recognition technologies at the carnival in 2018. The purpose of the test was to assess the technology's efficiency. The 'watchlist' of the trial consisted of images of volunteers. People at the carnival could choose whether or not to enter the area where live facial recognition technologies was being deployed. The Gendarmerie in France has been using facial recognition technologies for criminal investigations, but does not use live facial recognition technologies due to the absence of a legal basis to do so*" (105 p. 12).

[128] See below, in this chapter, the relevant case-law.

[129] Below, we will examine, whether this is a lawful processing or not.

From the above, it appears that France has conducted pilot applications of intelligent video surveillance systems with volunteers. Apart from this test, French police use facial recognition for real-life law enforcement. However, there is one exception. While French police generally use biometric facial recognition, they do not use it in systems that operate in real time because French authorities believe there is no legal basis for such processing.

In Germany several pilot applications of such systems have also been carried out[130]. Both France and Germany do not use such systems for law enforcement purposes because they consider that there is no appropriate basis for such processing.

On the other hand, in 2019, the "Swedish Data Protection Authority" authorized a new RBI system, that law enforcement authorities will use (124) (105). The new application "*will allow Swedish police to compare facial images from [video surveillance TV with] an existing biometric database of over 40,000 [images*]" (124) (105). There is no further information on the exact use of this system, e.g. if the biometric recognition take place in real time or in publicly accessible spaces. At the same time though the same authority imposed a substantial penalty (about 20,000 EUR) on a school for implementing a pilot biometric recognition programme [131] to monitor students' attendance at school (125) (126).

However, when using such systems, care should be taken not to discriminate against people based on false criteria of the algorithms, e.g., that a foreigner might be more dangerous than a national. Care should also be taken to ensure that during biometric identification or profiling data are collected and processed in a lawful manner. In addition, the freedoms of expression, movement, association and assembly are even more restricted than in the case of mere video surveillance[132]. In addition, the risks of a potential data breach are enormous because the processing take place on an extremely large scale. Therefore, man should be very careful about

[130] See below in the jurisprudence, chapter 5.2.5

[131] "*The test run was conducted in one school class for a limited period of time*" (125) (126).

[132] Recital 18 AI ACT. *"The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities".*

the applicable legal basis and the weighting conducted based on the principle of proportionality.

5.2.2. Application of the LED in remote biometric identification

5.2.2.1. Case-law

Biometric facial recognition for law enforcement purposes, other than border control, using AI systems is not a common processing of personal data, especially in Europe. It is therefore to be expected that it will not be easy to find jurisprudence on such cases.

However, there are a few decisions by data protection authorities [133] on video-surveillance and remote biometric facial recognition (using AI systems) for law enforcement or testing purposes.

In these decisions, the processing of biometric data is assessed both in terms of the purpose of the pilot application and in terms of the purpose of law enforcement. Sometimes it is decided that the use of the system itself is not permissible for the pilot application, and sometimes it is separated by purpose.

Since no decisions were found on existing video-surveillance with biometric data for law enforcement purposes (but only for testing this future processing), it is useful to look also at some decisions on simple video-surveillance for law enforcement purposes to better understand the context in which this processing takes place. Indeed, on this topic, we will look at court decisions and not only decisions of data protection authorities. So, we will start with the analysis of these decisions.

[133] The research was carried out in the German and the Hellenic DATA PROTECTION AUTHORITY. As far as the Greek authority is concerned, no relevant decisions have been found. The only relevant decisions concerned biometric fingerprint identification or iridoscopy at airports. However, they all concern the period before the adoption of the GDPR and the Directive and it is not helpful to examine them for our research.

(a) Administrative Court of Regensburg: Video surveillance and law enforcement

The city of Regensburg installed a video surveillance system in a city park to prevent and combat crimes, particularly drug trafficking and other crimes such as vandalism and assault committed by groups such as drug addicts and alcoholics. The data were stored for 72 hours. A local resident brought an action before the Regensburg Administrative Court because he felt that his fundamental rights had been violated by the video surveillance. The court - inter alia - partially upheld the citizen's claim. The processing was partly unlawful. For the purposes of the processing, the video recording had to be limited to hours without natural light and to certain days of the week. Therefore, video surveillance had to be even more restricted in the summer. Consideration was also given to limiting the data retention period to 72 hours. However, the court concluded that video-surveillance does not affect the citizen's right to informational self-determination, but only restricts the right to privacy. The lawful or not restriction of freedom of expression and movement must be weighed according to the principle of proportionality (127).

It follows from the above that video surveillance can lead to the violation of human rights such as the right to freedom of expression, freedom of movement, freedom of assembly, etc., even without biometric recognition. Whether this is a real violation, which is prohibited, or merely a restriction of the right, which is permissible, is determined by applying the principle of proportionality.

This decision is particularly important. The above restriction or infringement will apply accordingly in the next cases. However, there, the processing due to the use of RBI will, by definition, entail an even greater restriction of the above-mentioned rights. The application of proportionality and the other principles of the data protection legislation will contribute to the assessment, whether the processing is lawful or not.

(b) Data Protection Conference of Germany[134]: Pilot project for Biometric Facial Identification in 2017

[134] "*The committee of Independent German Federal and State Data Protection Supervisory Authorities – in abbreviated form Data Protection Conference (German abbreviation DSK)*" (229). "*It is tasked with safeguarding and protecting the fundamental right to informational self-determination, achieving a*

The use of video surveillance systems for biometric facial recognition poses significant risks[135] (128 p. 189). Already in 2017, pilot projects with video surveillance AI systems were conducted in Germany[136]. These pilot projects differed from conventional video surveillance in the following areas: First, biometric facial recognition was possible, and second, dangerous behaviour patterns could be detected. That is, the system compares the images captured by the cameras with corresponding reference images (models) that represent criminal behaviour.

Concerning the biometric recognition, the conference concluded that the use of video surveillance systems with biometric facial recognition can completely limit the freedom of individuals to move anonymously (128 p. 189).

Previous judgments have already ruled that even common video surveillance systems should be used sparingly. The courts reason that man develops his personality and express himself not only in private spaces such as home, but also in public spaces. Individuals must have the freedom to express themselves in any space within the bounds of legality without feeling that they are under constant surveillance. Such a scenario would lead to not being themselves.

However, with respect to biometric recognition, the Data Protection Conference also expresses the following. Since it is difficult to control the proper use of biometric recognition systems, man should consider that these systems could constantly monitor residents moving in these areas, create profiles of them, and provide accurate information about their residence, movements, meetings, and habits. There is also another problem: identification by the system works with probabilities. If the system incorrectly identifies a person, it will lead to unnecessary surveillance. The same can happen if the identification of an offender is correct, but there are normal law-abiding citizens next to him. These citizens will also be monitored unnecessarily because of their random position.

There is no legal basis for the use of this technology by competent authorities for law enforcement. Existing standards for the use of video surveillance technology allow the use of

consistent application of European and national data protection law and working together to promote its further development" (230).

[135] Annex 6: Resolution of the 93rd Conference of Independent Data Protection Authorities of the Federation on 29/30 March 2017.

[136] Before the entry into force, but after the adoption of the GDPR and the LED. These provisions were therefore taken into account at the conference because the conference wished to take a decision in compliance with them.

technical means only for conventional recordings without further data processing. The use of AI systems in video surveillance restricts fundamental rights too much. The current legal regulations cannot be used as a basis for such a justification.

For example, the Federal Constitutional Court also requires an explicit and appropriate legal basis for the automated collection of vehicle licence plates for comparison with a database. Since such processing is not permitted in the case of cars, it should not be permitted in the case of persons, since it interferes much more with the fundamental rights of individuals. Therefore, the use of video surveillance with facial recognition, even in a pilot project, should not take place for the time being, under the existing legal framework.

The European Parliament has recognised the enormous privacy risks of this technology and believes that the processing of biometric identification data is only allowed under strict conditions, both in the GDPR and the LED. Given the use of AI systems, we should respect the right to informational self-determination and establish appropriate rules to protect personal data.

(c) <u>Berlin Commissioner for Data Protection and Freedom of Information: Intelligent video surveillance at Berlin-Südkreuz Station</u>

In August 2017, the German Federal Ministry of the Interior and Community, the Federal Police, the Federal Criminal Police Office and the Deutsche Bahn AG (DB AG) launched a pilot project for intelligent video surveillance using biometric facial recognition systems at the Berlin-Suedkreuz train station under the name "Security Station Berlin Südkreuz" ("Sicherheitsbahnhof Berlin Südkreuz") (129 p. 75).

In the run-up to the project, a database was created with photos of over 200 people who volunteered to take part in the project. In specially equipped interior rooms of the station, the systems first recorded the looks of the passengers, then compared them with the image data of the volunteers, and finally filtered and measured the faces when they were recognised.

After the first phase of the programme was completed in July 2018, it was determined that the identification system had a very high error rate. Therefore, law-abiding citizens were at risk of having biometric data processed without reason. In the event of a real operation, there would

be a high risk that so many citizens would unnecessarily become the subject of police investigations. Since a biometric feature in principle does not change throughout its lifetime, the processing of such data poses significant security risks. If the data lost, the individuals concerned may become lifelong victims of a subsequent crime, e.g. impersonation.

Therefore, the collection of biometric data always involves a very deep invasion of privacy and a significant risk. The processing of biometric data by non-public bodies is therefore generally prohibited under the GDPR and only permitted in strict exceptional cases. Consequently, Deutsche Bahn agreed not to collect biometric data during the tests.

The authority ultimately prohibited the processing for the pilot implementation of AI systems based on the GDPR (and not the LED). This is justified because the authority is called upon to decide on the specific facts of the case. However, it is particularly important that the authority also addressed the possibility of effective processing of biometric data for law enforcement purposes. The authority concluded that such processing would pose great risks to the rights of citizens: On the one hand, it is possible to monitor them unnecessarily, and on the other hand, it is possible that further use for unlawful purposes will occur. It should be noted here that further misuse could occur either through the illegal transfer by the controller (or processor) or through a data breach. Therefore, limited use of AI systems is also required in this case.

(d) <u>Berlin Commissioner for Data Protection and Freedom of Information: A different video surveillance at Berlin-Südkreuz Station</u> (130 p. 187)

After the German Federal Police had used Südkreuz station as a test lab for biometric facial recognition for years, Deutsche Bahn now intended to use the station for its own tests. Unlike the tests conducted by the German Federal Police, the aim was not to process biometric data for facial recognition, but to detect dangerous situations, such as people in need of medical assistance, people very close to the edge of the platform, traffic jams in front of escalators or mass movements of groups, luggage left unattended for long periods of time.

It is true that Deutsche Bahn does have a legitimate interest in intervening in the situations mentioned and ensuring the safety of staff and passengers. However, the measures taken to achieve these objectives must always be suitable, necessary and proportionate.

In this regard, the systems have failed to detect many situations or have triggered false alarms. Therefore, due to high error rates, the use of such systems is currently not a reliable tool to support Deutsche Bahn in fulfilling its tasks. The competent data protection authority therefore considered that the use of the tested software for law enforcement purposes is not permissible as things stand.

It is therefore even more surprising that the Federal Ministry of the Interior and Community and Deutsche Bahn have announced that they will continue to test the systems, as they nevertheless consider video analysis systems to be promising approaches for detecting and reporting situations that are relevant to their functions. The Berlin data protection authority will continue to closely monitor the testing and check whether the data protection requirements are being met.

The authority therefore concludes that the testing is lawful. However, possible processing for law enforcement purposes would be unlawful, as the tests have so far provided unreliable results. This decision is particularly important because we find that even when it is not a matter of identifying individuals, the data protection authorities are very reluctant to judge such processing as lawful.

(e) <u>Administrative Court of Hamburg: "GAS"</u>

On the G20 summit in Hamburg in 2017, there were numerous peaceful demonstrations in the city (which hosted the summit), but also criminal acts. Therefore, the Hamburg police set up a database with images of people in order to prosecute these criminal acts. The data comes, inter alia, from video surveillance cameras in the S-Bahn. All images, which come from different sources, were analysed using facial recognition software called "GAS" ("Gesichtserkennungssoftware"). "GAS" measured the individual distances of eyes, ears, nose and mouth and enabled the (re)identification of the person. Finally, the results of the system were evaluated by staff (131).

The Hamburg data protection authority considered the processing unlawful and in August 2018 ordered the Hamburg police to delete the biometric database - but not the files on the crimes committed and the suspects. The authority considered that a) the law providing the legal basis

for such processing was unconstitutional and b) there was no legal clarity on whether such processing was permissible for law enforcement purposes (132).

However, the City of Hamburg appealed to the Administrative Court, and the Court overturned the above decision, finding that the data protection authority did not have the authority to order the police to delete the database. In particular, the court concluded that the authority did not have the power to examine the relevant legal basis on which the processing was based, as this followed directly from the (German) implementing law of the LED.

The court also pointed out that the Authority could in any case impose more lenient measures on the controller, considering the principle of proportionality. For example, the authority could ask the controller whether technical and organisational measures were taken, how long the data would be kept and whether there were other processing purposes. On the contrary, the authority not only did none of the above, but arbitrarily assumed that unauthorised further processing would take place. Therefore, the Authority exceeded the limits of its discretion and its order was consequently annulled (131) (133).

The Authority applied for leave to appeal this decision to the Hamburg Higher Administrative Court, whose judgement has not yet been issued (134 pp. 16-19) and in the meantime the police issued a press release ordering the deletion of this database. The authority then stated that: The recent deletion of the biometric database by the Hamburg police is welcome. However, the considerable dangers of automated facial recognition for a free society and privacy have been critically discussed worldwide after the mass evaluation of facial databases by the American company "Clearview". Particularly, for the effective protection of the freedoms of people who are not suspected of anything at any time, there is at least a need for concrete legal requirements for the usability of this technology.

In line with the above, the Court did not consider such processing as unlawful a priori, but concluded that the circumstances and the principle of proportionality must be taken into account in any case. If the data protection authority has imposed sanctions without considering all the above, then they are unlawful.

5.2.2.2. Overview

Considering the above (theory, legislation and jurisprudence), we will try to approach the legal framework (based on the legal system in force so far) of the subject we are dealing with. First of all, we need to clarify that in the case of real-time remote biometric facial identification systems in publicly accessible spaces for the purpose of law enforcement the LED and not the GDPR applies, since processing for law enforcement purposes falls within the scope of the LED. The Regulation applies only in a complementary way. Therefore, what we have explored above in relation to the LED should be implemented.

Concerning video-surveillance in general, we conclude that these systems, like any processing of personal data, must comply with the principles of lawful processing, which means, inter alia, that they require clear and specific purposes, a limited retention period, and respect for the principle of proportionality.

As can be seen from the above case law, as well as from the comparative analysis of the GDPR and the LED that preceded it in an earlier chapter[137], it should be emphasized here that processing for law enforcement purposes, and therefore video surveillance carried out for these purposes, requires that the data collected are not excessive in relation to the purposes pursued, while in the case of natural persons they may only include what is necessary. This is an important distinction that allows law enforcement authorities to collect not only necessary but also some unnecessary personal data.

In this case, the legislator weighs the importance of the purpose of the processing, but also the guarantees of the processor as a law enforcement authority, which - in principle - is likely to comply with the law, and allows the processing as long as the personal data are not excessive. The truth is that, on the one hand, the law must protect the rights of the subject, but on the other hand, it must also consider the public interest, which in this case refers to the public authority.

[137] See above, chapter 4.

Moreover, it should be stressed that this is a processing of special categories of data, so both Article 8[138] in conjunction with Article 1 [139]and Article 10 apply[140] (4).

Accordingly, such processing is lawful only if it (a) falls within the purposes of law enforcement authorities and (b) "i*s* [strictly][141] necessary for the performance of [that] *task*". (c) In addition, "*the processing* (i) [must be authorized by a] *Union or Member State law* or (ii) *protect* [a] vital [interest] *of the data subject or another person*", or (iii) the data subject must have already made public the personal data to be processed (this case is clearly not present here). (d) In any case, "*appropriate safeguards for the rights and freedoms of the data subject*" are needed (4).

The difficulty is that the controller must demonstrate that the processing is necessary for law enforcement authorities to perform their task. The controller should also apply the principle of proportionality to determine whether and to what extent the processing is necessary.

"Consequently, both the initial biometric processing of facial images, any subsequent retention of video footage, and comparing the data to a 'watchlist' – alongside populating the watchlist with facial images – constitute intererences with the right to respect for private life and the protection of personal data" (135). *"Given that processing of personal data constitutes a limitation of these rights, it needs to be subjected to a strict necessity and proportionality test, including a clear legal basis to do so and a legitimate aim*

[138] *"Article 8 Lawfulness of processing 1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law. 2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing".*

[139] *"Article 1 Subject-matter and objectives 1. This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".*

[140] *"Article 10 Processing of special categories of personal data Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject".*

[141] Given that it is about sensitive data, the processing must be strictly necessary and not just necessary (Article 10 LED).

pursued. Such a test has to take into account the context and all circumstances at hand. Hence, the sensitivity of the data or the way the data are used are important for the context" (136) (105).

As emphasized earlier, it is the specific circumstances that are crucial to answer whether a processing is lawful or not. Therefore, it is not possible to make a general judgment in advance. However, it should be noted that it is extremely difficult to justify such processing, given the special categories of data involved and the extremely large scale of the processing (and therefore risks to these sensitive data, as already identified in case law, e.g. hacking or data breaches). It is therefore doubtful that such processing could ever be lawful.

However, according to Art. 10 LED, the processing must be either provided for by law or justified by the vital interest of the data subject.

A vital interest of the data subject does not seem to exist - in principle[142]. It would be safer to consider the enabling provision of the law ("*only where authorized by Union or Member State law*") as a possible legal basis. There is currently no such provision in European legislation. However, an explicit provision itself would not solve all the problems. This legal provision should be in line with the data protection law in general and should be sufficiently justified. Otherwise, any further provision - especially at national level - could mean circumventing the general provisions.

In any case, the technical measures of the system (privacy by design) are of outmost importance: *"Transmission must be routed through secure communication channels and protected against interception […]. Encryption or other technical means ensuring equivalent protection must also be considered […]. Physical access to the control room and the room storing the video-surveillance footage must be protected"* (137).

[142] Moreover, a vital interest of a third party could possibly be justified, if the database contains biometric data of kidnappers and the camera is located at the entrance of an outdoor playground. However, even in this case, video surveillance (even without capturing biometric data of children) may harm children, as they must be able to express themselves freely and not feel observed. But also, a data breach of children's personal data has serious consequences for their entire future life (as we have seen above). For this reason, video surveillance systems in playgrounds often state that recording only works during the hours when the playground is closed. Therefore, an explicit provision in the law "for the processing of such personal data on a large scale" is a safer legal basis than the "vital interest".

Of course, all the principles of lawfulness and accountability must also be respected. For example, the controller must keep records of its activities, conduct a DPIA, and likely consult with the competent authority.

5.2.3. Application of the AI ACT in remote biometric identification – Comparison with the LED

5.2.3.1. The rule of prohibition – 5(1) AI ACT

In the following, we will examine the proposal of the AI Regulation on "*the use of AI systems for real-time biometric identification* [of individuals] *for law enforcement* [purposes]" (1).

"The following artificial intelligence practices shall be prohibited: […]

(d) the use of 'real-time' remote biometric identification systems[143] *in publicly accessible spaces for the purpose of law enforcement*[144]*, unless and in as far as such use is strictly necessary for one of the following objectives:*

(i) the targeted search for specific potential victims of crime, including 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 in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State […][145]*".*

---

[143] *Article 3 Definitions: (36) "'remote biometric identification system' means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ; (37) 'real-time' remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention. (38) ''post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system;"*

[144] See Article 3 (40) & (41) LED.

[145] Article 5 (1) (d) AI ACT.

"Article 6 Classification rules for high-risk AI systems 2. […] AI systems referred to in Annex III shall also be considered high-risk.

ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas: 1. Biometric identification and categorisation of natural persons: (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;"

According to the above, such use should in principle be considered as prohibited. This is fully compatible with the data protection legislation, i.e., LED, where the processing of special categories of data is in principle prohibited.

We have already mentioned above that this type of processing poses specific risks[146]. First of all, video surveillance, even without the processing of biometric data, significantly restricts the fundamental rights of individuals. It significantly restricts the right to freedom of expression, freedom of movement, freedom of association and freedom of assembly. Individuals must feel free to express themselves, to meet friends, to protest. Moreover, biometric identification with AI systems means large-scale processing, which, due to the nature of AI systems, may at the same time pose significant risks to this sensitive personal data. An unlawful transfer, a processing for another unlawful purpose, or a data breach could have serious consequences for data subjects.

Because these personal data processing operations are so significant, the AI ACT makes individual distinctions for these processing operations. For example, the AI ACT distinguishes between remote and non-remote processing, real-time and post processing, processing for law enforcement and other purposes. The AI ACT does not prohibit all these processing. It in principle prohibits remote processing in real time for law enforcement purposes. However, the Act provides for some exceptions to this prohibition. We will see these in detail. We will also learn about other (non-explicit) permissible biometric identification methods, in the following[147].

[146] See above, chapter 5.2.
[147] See below, chapter 5.2.3.5.

5.2.3.2. The explicit exceptions – 5 (1) AI ACT

When considering the exceptions of the above prohibition, the following can be noted. With respect to the first exception, the legislature indicates that it intends to define the scope of the exception as precisely as possible. This is evident from the use of the phrases "targeted search" and "specific potential victims". However, it is doubtful, whether this has been accomplished.

Concerning the term "specific potential victims", does the adjective "potential" weaken the accuracy of "specific"? So, what can this term mean? Using the example of "missing children", the Act shows that we are talking about specific potential victims who are likely to be at risk. However, this is firstly only our conclusion, and secondly, it is still not clear what kind of risk a person must be for the use of AI to be permissible. So does the person have to be in imminent danger, as is the case with a missing person, or even more so with a missing child? That could be a narrow interpretation that serves the principle of minimisation, but that is a weak conclusion here.

Another question is: which potential victims are specifically affected by which crime? The legislature does not define the content of the crime in this case. It could be a serious crime, such as homicide, human trafficking or terrorism? Or also criminal offences such as insulting petty theft? Obviously, the legislator does not mean the latter cases, but the question is still the same: what kind of crimes does the ban cover?

The answer to the above questions is certainly not self-evident. We can understand the spirit of the law and roughly guess which cases fall into this category. However, the final text of the AI ACT should certainly provide clarity. In other words, the legislature should have sufficiently defined the scope of the exception. Otherwise, there is a risk that this exception will be abused.

The second exception is clearly defined and does not allow for subjective interpretations.

The third exception is also clear, since it refers directly to specific offences[148] on the one hand, and requires specific criminal treatment on the other (*"punishable in the Member State concerned*

[148] See Article 2 (2) Council Framework Decision 2002/584/JHA, where there are all the relevant crimes, such as: *"participation in a criminal organisation, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and*

by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State").

The clarity we note in the second and third exceptions serves the purpose limitation principle, which is generally provided for in the legislation on the data protection. Specifically, the LED explicitly states that "*Member States shall provide for personal data to be: […] (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes […]*[149]*".*

In both the second and third exceptions, there is another element to consider in addition to clarity. If we look at the content of the crimes and the specific circumstances that the legislator requires, we find that the processing of biometric data is legitimate only in the case of particularly serious crimes that he defines. The legislator thus manages - in the cases of (ii) and (iii) - to introduce exceptions that are fully compatible with the general provisions on the data protection.

5.2.3.3. The principle of proportionality – 5 (2) AI ACT

In the Article 5 (2) AI ACT (1), the legislator addresses the principle of proportionality in general, as it requires that certain criteria must always be taken into account when using AI systems: *"in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system; probability and scale of the consequences of the use of the system for the rights and freedoms of all persons concerned".*

Considering this, the user of AI systems must weigh the benefits and harms of using AI. In this way, he makes a risk assessment based on the principle of proportionality. The user must always answer the question: What are the benefits of using AI, what are the risks of not using AI and what are the possible negative effects.

psychotropic substances, — illicit trafficking in weapons, munitions and explosives, — corruption, — fraud [etc]".

[149] Article 4 par. 1 LED.

A similar problem arises when conducting an impact assessment. As we have seen above [150], an impact assessment must consider, inter alia, the necessity and proportionality of the processing in relation to the purposes pursued. Therefore, the AI ACT seems to be like the general protection of personal data.

More specifically, in this case, the controller must take into account the severity, likelihood and extent of the harm. In light of the principle of proportionality, man would have to take into account whether the measure (i.e. the use of AI systems) is necessary and proportionate to the purpose pursued· i.e. whether there is a milder way to achieve the purpose, but also whether the processing is proportionate to the purpose. The proportionality test is neither simple nor easy. The meaning of the principle is the following: The controller must weigh the benefits and consequences of the processing. Namely, on the one hand, a) what benefit does he derive from carrying out the specific processing that he would not otherwise derive? (*"in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system"* and on the other hand b) what benefit does he derive from carrying out the specific processing that he would not otherwise derive? (*"probability and scale of the consequences of the use of the system for the rights and freedoms of all persons concerned").*

5.2.3.4. Prior authorisation - The Article 5 (3) AI ACT [151]

In the third paragraph, the legislator requires prior authorization by the competent judicial or administrative authority for data protection. This is rather reminiscent of the previous legal

[150] Article 35 (7) (b) GDPR, 27 LED.

[151] Article 5 (3) AI ACT. *"As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.*
The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2".

regime before the GDPR and related legislation, where the permission of the competent authority was required for certain processing operations, in particular for automated processing operations such as video surveillance[152]. The former authorization has been removed in the new legislation and replaced by an impact assessment[153]. This obviously gives more flexibility to the controller, but also more responsibility. The fact that the legislator is adopting a previous practice in this case means that it is prioritising security over flexibility here. Indeed, it was a significant burden for any competent authority to have to deal with the authorisation of all those who install video surveillance systems in homes or workplaces, etc., but, for example, video surveillance of biometric data with cameras containing AI software for biometric identification (for law enforcement) seems to be something quite different: there are more and greater risks for data subjects. Therefore, there is a clear difference here compared to the GDPR and the LED, which only require an impact assessment and prior consultation of the authority if the DPIA shows that the processing would cause a high risk, unless the controller takes measures to mitigate the risk[154].

Upon further analysis of the text (paragraph 3(b)), we note that the legislature does not leave the authorization to the discretion of the authority, but also specifies the conditions under which the authority shall grant such authorisation: **"***The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2"***.** The legislator thus clarifies that the authority itself, as well as the controller, must take into account the principle of proportionality as defined above.

In principle, such a procedure ensures the best possible data protection, since any measure is preceded by an authorization from the authorities. At this point, it becomes clear that the Act

[152] Article 18 (1) "DIRECTIVE 95/46/EC
[153] Article 35 GDPR, Article 27 LED.
[154] Article 36 GDPR, Article 28 LED.

refers to a judicial or independent administrative authority[155]. According to the GDPR and the LED[156], the competent authority is "*an independent administrative authority of the Member State"*. Under this condition, the legislator guarantees the functional and personal independence of the members of the authority and their administrative autonomy, characteristics which judges also have (138). However, here the legislator gives the Member State the possibility to choose either a judicial or an administrative authority, which again points to the importance of the processing and the relevant risks.

While the legislator tries to clarify the importance of the processing, it unexpectedly introduces an exception to this procedure: *"However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use".*

Thus, in urgent situations, law enforcement authorities, as data controllers, have the right to act without the authorization of the data protection authority and to request it after the fact (i.e., during the use of AI systems or even later). Indeed, sometimes the immediate intervention of the police is required because the danger is imminent. So, if law enforcement authority is waiting for authorization, the use of AI may no longer matter. What does this mean for our personal data? Is this an exception that puts them at risk?

In order to answer this, we have to consider, on the one hand, the importance of data and, on the other, how serious, likely, and immediate is the crime we intend to prevent. This is a balancing test that the competent authority must carry out in any case. Therefore, the controller has a greater responsibility. He should himself make a correct and reasoned weighing before the authority, in order to make the authority's decision as precise as possible. If the competent authority ultimately does not grant an authorisation, this means that the controller has carried out unlawful processing. As a result, in accordance with Article 57 LED, the relevant fines provided for by the Member State should be imposed[157].

[155] Recital 117 GDPR: *"The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data […] ".*

[156] See Article 51 (1) GDPR, See Article 41 (1) LED.

[157] Article 57 LED "*Penalties. Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary*

What actually happens to the sanctions imposed by the competent authority (of the Member State) on the Member State itself? As mentioned above, the member of the data protection authority or the judges of the administrative court, enjoy personal and functional independence, and the authority itself has administrative and financial autonomy. This provides some guarantees of the impartiality for the authority. The authority is not controlled by other government agencies, just as the courts are not controlled, too. Moreover, its members are trained and respected scientists with excellent knowledge and experience. Therefore, one can be sure that the principle will indeed be impartial. But is the "threat" of sanctions sufficient for the law enforcement authority to be compliance with the data protection law?

If the controller is a legal entity (e.g., a public authority, a prosecutor's office), the controller seems somewhat impersonal. Who is the one making the decisions? And against whom are the sanctions actually imposed? Financial sanctions, such as fines, clearly affect -in principle- the legal entity and not the natural persons making the decisions. What is the motive of the employee, e.g., the police officer, not to act arbitrarily?

The strict structure of a department, the training of its members, the cooperation between the competent bodies, the constant control and the imposition of disciplinary sanctions, if necessary, as well as the conscientiousness of the employees are certainly important parameters. However, this is a very difficult issue. These are decisions that involve great responsibility, and it is important that, on the one hand, managers and civil servants in general have the courage to make difficult decisions responsibly, but on the other hand, that irresponsibility can be effectively controlled and prevented. And this is not easy in a public service, where bureaucracy makes it slow to assign responsibilities or to keep them quiet (since it is an internal service matter).

Although the sanctions against the controller are imposed by the independent authority, i.e., data protection authority, the sanctions for the parties involved are imposed by the administration and are based on the already existing administrative law of the member state. This means that either the bosses are just held politically accountable or the state bring claims or disciplinary sanctions against the employees. But this is something that is decided by the

to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive".

administration, not by an independent authority that is truly impartial. This does not mean that administrative authorities are corrupt or arbitrary. However, it is indeed difficult to impose sanctions within the same department.

From the above, it becomes clear that the urgency procedure in this case is insufficient to protect the personal data of the subjects. But what would be an appropriate procedure?

However, the entire procedure described above (with the authorisation of the law enforcement authority and the exception in urgent cases, as regulated in the AI ACT) recalls the legal procedures applied in cases of intercepting confidential communications. At this point, it should be noted that contact data, both in terms of their content and in terms of their external elements (e.g., numbers of callers), constitute personal data[158]. Besides, theses data could even be of special categories, when a conversation contains such sensitive information. Moreover, we do not need to keep in mind only the classic example of telephone conversations. The lifting of confidentiality may also extend to electronic communications with images and sounds. This content of electronic conversations (e.g. chat) might also include photos with biometric identification information. So, this processing of personal data is similar to the above-mentioned on the Article 5. The difference is that in the one case it is private conversations, while in the other case it is biometric identification in a publicly accessible space. Therefore, it is important to see how the legislator regulates the procedure in question and compare it with this proposal, taking into account the similarities and differences.

Article 5 of Directive 2002/58 establishes the confidentiality of communications[159] and Article 15 introduces relevant exceptions, while establishing a framework of conditions[160]. Moreover, the

[158] See "DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)".

[159] Article 5 DIRECTIVE 2002/58/EC *"1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality".*

[160] As this is a directive (and not a directly applicable regulation), the provision introduces a framework of conditions that the national legislator will follow to define the exceptions to the

confidentiality of communications is based on Articles 7, 8, 11 και 52 (1) CFR. In addition to EU law, the confidentiality of communications is also enshrined in Article 8 (2) of the ECHR[161] on the protection of private and family life [162]. Based on the above-mentioned provisions, the European courts (ECJ [163] & ECtHR [164]) formulated some criteria for the interception of the communication, if necessary.

However, exceptionally, *"in urgent cases it is possible to intercept communications without prior judicial authorisation for up to forty-eight hours. A judge must be informed of any such case within twenty-four hours from the commencement of the interception. If no judicial authorisation has been issued within forty-eight hours, the interception must be stopped immediately (see paragraph 35 above)"* (139 p. 266).

It follows from all the above that the case-law has established specific and clear conditions for the adoption of such a measure restricting freedom as an interference with communications, privacy and freedom of expression. First, the measure must be provided for in national law, be

---

confidentiality of communications and not the exact procedure to be followed by the prosecuting authorities.

[161] Further, under Article 8 (2) ECHR, the measure envisaged must be "necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" and must be adequate to the purpose it is intended to serve. Finally, monitoring by an independent body, notification of surveillance measures, and a limited duration (durée limitée) of the measures required (219) (228).

[162] Although Article 8 does not explicitly refer to the protection of confidentiality, it is nevertheless accepted that the confidentiality of telecommunications is protected as a partial dimension of privacy (223 p. 41) (224 p. 78) (222 p. 52).

[163] *"Article 15(1) of Directive 2002/58/EC […]", "read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication"* (225).

[164] *"There shall be no interference by a public authority […] except such as is in accordance with the law […]". "100. The wording 'in accordance with the law' requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable [164] as to its effects (Roman Zakharov, § 228)"* (226 p. 100). *"59. […] The 'quality of law' in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when 'necessary in a democratic society', in particular by providing for adequate and effective safeguards and guarantees against abuse (see Roman Zakharov, cited above, § 236)"* (222 p. 59).

accessible and foreseeable, be a necessary measure in a democratic society, and take into account the principle of proportionality with respect to the objective pursued. In addition, the case-law defines the purposes for which such a measure may be taken and establishes appropriate safeguards, such as authorization by a competent independent authority, information of the data subject and limited duration of the measure. Even if the measure is urgent and starts without authorisation, it must be granted within 48 hours, otherwise the measure will be stopped.

In relation to the subject of our study, case-law has consistently concluded that the feeling of being watched violates the freedom of expression, of movement, and assembly. Moreover, biometric data is a very sensitive category of data. However, the provisions of the AI ACT on the exceptional procedure to be used by law enforcement authorities in urgent cases do not provide similar safeguards to those for lifting the confidentiality of communications. Specifically:

Explicit provisions are also required at the national or European level.

Article 5 (4) AI ACT mentions what the national legislator must take into account in relation to this exceptional and urgent procedure. However, is this reference sufficient or did the AI ACT have to provide a minimum framework?

The emergency procedure seems to be insufficient for the data protection. In order to maximise the data protection, the provision should provide for a maximum period within which law enforcement authorities are obliged to request the authorisation. The determination of the duration should take into account, on the one hand, the individual needs of law enforcement authorities and, on the other hand, the risk to personal data. In any case, the provision is insufficient.

5.2.3.5. Further exceptions

In addition to the explicit and detailed exceptions listed above, the following are also considered to be permissible processing operations: (a) Real-time use of remote biometric identification in publicly accessible spaces by public authorities for purposes other than law enforcement (e.g., to control access to buildings), (b) Real-time use of remote biometric identification in publicly

accessible spaces by private actors (e.g., scanning shoppers entering supermarkets), (c) Use of post remote biometric identification[165] including law enforcement purposes (e.g., identifying a person who has committed a crime), (d) Use of real-time remote biometric identification in spaces not open to the public (including law enforcement) (113 p. 26), (e) Remote biometric identification in publicly accessible spaces for law enforcement purposes.

Taking into account the above, the high-risk systems that fall within the scope of the present work are those found in the exceptions of Art. 5, but also the "use of post remote biometric identification including law enforcement purposes"[166] found in Annex III of the Act that accompanies art. 6.

With respect to the exceptions in Art. 5, which we have discussed in detail, it should be noted that the above analysis has shown that these provisions contain many ambiguities and require further clarification. The relevant offences (which are exceptions) are not sufficiently defined, so that the rule that it is generally forbidden to use these systems is compromised. It seems that the AI ACT gives Member States a wide discretion in defining these exceptions. However, this will not be tolerated. The AI ACT must be clear, otherwise arbitrariness prevails. It is understood that the Act does not address cases such as biometric recognition of persons participating in protests, nor of persons committing petty crimes (113). Nevertheless, clarity is needed. The same applies to the exceptional procedure in urgent cases. Otherwise, law enforcement authorities may act arbitrarily.

Since the "high-risk systems" are not exhaustively listed in Annex III, it is generally possible to fall into this category and all other systems, as defined in Art. 6 (1). For this reason, it is considered that high-risk biometric identification systems should be listed in law.

It is noticeable that the legislator distinguishes the systems into those that take place in real time and those that take place at a later ("post") time (by referring to the significant delay or not). This distinction appears to be entirely arbitrary. It is not clear why post remote identification is allowed, as it poses exactly the same risks to the freedoms and rights of data subjects, as the

[165] Recital 38 AI ACT. It enables capture, comparison and identification after a significant delay based on pictures or video (113 p. 25).
[166] Recital 38 AI ACT. It enables capture, comparison and identification after a significant delay based on pictures or video (113 p. 25).

real-time RBI. Even more, these risks are the same regardless of the purpose of the processing and the nature of the controller (140 p. 11).

Moreover, how it is possible to allow the processing of biometric data by an individual (e.g., to enter a shop) while law enforcement authorities seem to be prohibited from processing petty thefts? Such an approach to biometric identification diverges from the personal data protection legislation outlined above, as the LED, rather than the GDPR, provides greater discretion over the amount of data to be processed (e.g. there is no principle of minimisation in law enforcement, but there is in the GDPR), but also in terms of the category of data (e.g., the conditions for processing special category data are broader), while recognising the importance of law enforcement's mission vis-à-vis individuals' entrepreneurship.

For these reasons, a general prohibition should apply to all systems that perform automated (via AI) facial identification (but also other biometric characteristics such as fingerprint, gait, voice, etc.) in publicly accessible places (140).

In summary, in this area, the AI ACT not only does not specify the already existing legislation on the data protection to contribute to legal certainty, but does not even comply with it, creating legal uncertainty itself. Not only has it not paid particular attention to protecting the fundamental rights of the data subjects, but it also contradicts the basic legislation. There is also no reference to the legislation on the data protection. Such a reference to the basic legislation on the data protection could - to some extent - protect the enforcer of the law.

If the text is implemented in its current form, there will be parallel provisions and consequently a great deal of confusion as to the applicable law. Any ambiguities should be identified and eliminated.

5.3. Evaluation of the creditworthiness on a large scale

5.3.1. The scope

5.3.1.1. TIRESIAS [167]

In the 19th century, the need to evaluate the creditworthiness of potential borrowers arose. Around 1850, the first information bureaus in the financial sector began to operate: first in Great Britain, then in the United States, France and Germany; in Greece, this happened later, in 1926 (141 pp. 302-310).

In order to effectively prepare the image of the borrower, the information of interest to the bank was categorized on the basis of subjective (personality, education, career, stability of professional environment, previous economic behavior) and objective economic data (amount of income, assets). Since 1940, in the USA, these data have been processed on the basis of algorithms to obtain an objective score for each interested bank customer.

To effectively process the borrower's image, interesting information was categorized based on subjective (personality, education, career, stability of professional environment, previous economic behavior) and objective economic data (amount of income, assets). Since 1940, these data have been processed in the USA based on algorithms to obtain an objective score for each bank customer (141 pp. 302-310). Similarly, data on Greek borrowers are processed by TIRESIAS, founded in 1997, to produce a financial profile and thus a credit score (142 pp. 25-37).

"*Data profiling refers to the activity of collecting data about data, i.e., metadata […]. Simple metadata are statistics, such as the number of rows and columns, schema and datatype information, the number of distinct values, statistical value distributions, and the number of null or empty values in each column*" (143 p. Summary).

Fundamental to the structure of this system is compliance with (a) the principle of time limitation of data retention - and in this context (b) the provision for data deletion, and (c) the accuracy of the stored data. Moreover, TIRESIAS lawfully processes the personal data provided

[167] "*Nearly all Greek Banks confunctioned to create [TIRESIAS], a company entrusted with the development and management of a reliable Credit Profile Databank*" (253).

by the banks. Some of the processing is even carried out without the consent of the data subjects. The legal basis for the processing is the interest of the banks[168], as TIRESIAS protects the financial system from insolvent customers. It is considered that the data processing by TIRESIAS is absolutely necessary and that the protection of business credits outweighs the interests of the data subjects (142 pp. 25-37).

5.3.1.2. SCHUFA (144)

What TIRESIAS is for Greece, SCHUFA is for Germany. SCHUFA has been providing credit reports since 1927, making it an important part of the German economy and society. The company processes data such as name, date of birth and, if applicable, place of birth, current and previous addresses and, of course, the rating. In addition, SCHUFA gathers information from its contractual partners on bank accounts, credit cards, leasing contracts, mobile phone bills, mail order accounts, installment payment transactions, loans and guarantees (144)**.** Not processed by SCHUFA, however, are data such as: assets and income, marketing data (e.g. consumer habits), occupation, attitudes (e.g. religious, political, etc.), marital status, nationality.

The way SCHUFA works is as follows: it collects information from the person's past trading behavior and rates the subject. For example, SCHUFA considers whether loans have been applied for in the past and paid according to the contract. The basis of scoring is the idea that this experience can help predict the future[169].

The procedure carried out by SCHUFA is profiling. "*The generic term profiling refers to the processing of personal data by analysing certain aspects of a person". "In addition to the logistic regression method, which has been established for many years in the area of credit scoring, SCHUFA can also use scoring methods from the areas of so-called complex non-linear methods or expert-based methods. It is always of particular importance to SCHUFA that the methods used are mathematically and statistically recognised and scientifically sound. Independent external experts confirm the scientific nature of these procedures*" (145).

[168] Article 6 (1) (f) GDPR.

[169] "*Scoring involves using information and experience gathered in the past to make a forecast about future events or behaviour*" (145).

Credit scoring is very important to bank and other businesses because it involves how likely a person is to meet their payments. This minimizes the risk of default. For example, when someone applies for a loan from the bank, the bank checks the score in the SCHUFA before approving it. Based on this score, the bank decides whether to approve or reject an application.

"*It is important here to know that SCHUFA itself does not make any decisions. It merely supports the affiliated contractual partners with its information and profiling in the decision-making process. The decision for or against a transaction, on the other hand, is made solely by the direct business partner. This applies even if the latter relies solely on the information provided by SCHUFA*" (145).

But that is all we know about SCHUFA's scoring process. SCHUFA does not publish the scoring formula. If the calculation model were completely open, the score could be manipulated and would no longer have any value, according to the assessment. This potentially raises doubts about the proper processing of our data and clearly contradicts the principle of transparency enshrined in Art. 5 (1) (a) GDPR: data must be processed in a transparent manner. Can a trade secret justify an exception? Or is the risk to the effectiveness of the measure a sufficient justification? The proportionality principle will help us understand whether this is indeed a legal restriction on our right to transparent information[170]. The above question has already been answered in case-law, and the relevant decision and its reasoning is analysed below.

5.3.1.3. Artificial Intelligence for profiling

Below we will try to approach the way in which bodies such as TIRESIAS, SCHUFA, banks, etc. conduct a profiling for the creditworthiness of the subject.

AI is the appropriate mean for an institution to conduct such a processing. "*There are credit scoring tools in today's market that apply machine learning to enable assessment of even the qualitative factors such as consumer behavior and willingness to pay […]. Machine Learning can do what humans usually get failed to do […]*" (146). "*The goal is to use machine learning to create a credit score for customers. This score gives the degree of confidence that the customer will meet the agreed payments*" (147). "*The machine learning model would need to have been trained on labeled datasets indicating which*

[170] See Article 12 GDPR.

kinds of social media posts or websites are indicative of a responsible customer and which are indicative of a risky customer" (148).

It follows from the above that profiling for the assessment of our creditworthiness is conducted through machine learning. An AI system can process too much data in a short time. Also, it can easily update its evaluations regularly, as our profile can change over the time, even within a few years. Also, a person's score is likely to have subdivisions, depending on the act for which the person is judged. That is, one may not have a strong profile for taking out a mortgage loan, but this does not mean that he or she is not creditworthy for repaying a credit card or much more for carrying out a transaction and paying the supplier.

According to the above, among the personal data that an AI system "can" evaluate is the activity on social media etc. However, a little earlier we read, that SCHUFA does not process this kind of data. Therefore, we conclude that in addition to SHUFA, TIRESIAS, etc., a bank may have other sources for evaluating a lender. First of all, a bank could carry out an automated assessment by its own means and on the basis of data already available. However, the data that a bank has gathered about its client are often insufficient. Therefore, can a bank receive ratings from third-party, non-official, entities? Can an evaluation take into account our activity on social media? How could this be done?

5.3.1.4. Purchase of personal data

Nowadays, some Internet service providers, social media companies and various websites systematically collect personal data from users and transfer them to third unauthorized entities.

The use of all websites is associated with the collection of a minimum amount and type of data. These are primarily necessary traces on the websites during browsing or users. However, the qualitative and quantitative characteristics of this data vary depending on the website visited. Each website must provide information about its relevant actions. Thus, in addition to the above-mentioned necessary traces, a website may also gather data for advertising purposes, which it uses itself or passes on to third parties. The problem is particularly serious with regard to social media platforms, as they are constantly fed with a wealth of users' personal data,

voluntarily. Could it be argued that unlawful transfer was entirely to be expected due to the free (gratuitous) use?

Even if someone consents to the processing and transfer of their data for marketing purposes, we can hardly imagine anyone allowing, for example, "Facebook" to process and transfer data for credit profiling. Social media and other popular platforms are primarily aimed at targeted advertising for internet users. However, it is not impossible that they may further process our data in a way that is incompatible with the primary purpose. If they do not have an adequate legal basis for all their processing or if they do not inform the data subject about all their purposes, the competent data protection authority may impose a fine on these platforms. The greater the expected benefit from the unlawful data transfer, the higher the fine imposed. Below you will find the relevant case law[171]. Can the processing of our social media profile ever be lawfully used for credit profiling?

According to a 2018 report by the World Economic Forum (WEF), as digital technologies evolve, our digital identity increases, and that digital identity determines what products, services, and information we can access (149) (150). However, the risks associated with sharing financial and activity data on social media are so many. These risks include social discrimination, reduced social mobility, compromised privacy, and a "Yelp-style"[172] ranking culture (150).

5.3.2. Application of the GDPR in credit profiling

5.3.2.1. Case-law

(a) No more "SCHUFA clause"

In 2019, the Hessian Data Protection Authority ruled on the legal basis for SCHUFA's processing. Until the entry into force of the GDPR, the legal basis for processing was the consent of the data subject. The bank's customer signed a contract that included, inter alia, the "SCHUFA clause" providing for the processing. However, after examining the legal basis for the processing, SCHUFA concluded that the consent of the data subject was not required. A simple

[171] See below the "Facebook" case.

[172] "Yelp Inc. is an American company that develops the Yelp.com website and the Yelp mobile app, which publish crowd-sourced reviews about businesses" (236).

information is sufficient, while the legal basis for the processing is the legitimate interest of the controller, which is to inform him whether his potential customer is creditworthy. The data protection authority considered that this basis for processing is perfectly legal and the consent of the data subject is not required (151 pp. 97-99). In another case from 2020, the Berlin data protection authority confirmed that the legal basis for the data processing by organizations such as SCHUFA is not the consent of the data subject, but the legitimate interest of the controller, e.g. the bank. Therefore, the transfer of debtor's data (by debt collection agencies) to SCHUFA is lawful without the consent of the data subjects (130 p. 245).

(b) Information of data subject

Greek Council of State 2965/2017[173] (152)**:** The data processing is lawful without the consent of the data subject for data representing his financial behaviour if it leads to the unreliability and insolvency of his creditworthiness, provided that the subject has been informed in advance. In this case, the processing by TIRESIAS seems to be absolutely necessary to satisfy the legitimate interest of banks to have a clear and certain picture of the creditworthiness of their customers. In any case, it is necessary that the data subject is informed. What is noteworthy about this decision is that the controller's obligation to inform could have been fulfilled even if the controller had not provided such notice to the data subjects: Tiresias' notices in the press constitute adequate information to the data subject.

Court of Appeal in Berlin (153): A bank customer objected to the SCHUFA system and demanded the deletion of negative entries concerning him from the database because he had not been specifically informed about these entries. The Berlin Court of Appeal did not uphold his complaint, holding that there is no obligation for SCHUFA to inform the person concerned prior to each entry. It was therefore sufficient to inform the subject in advance of the data entered the database during his transactions.

Data Protection Agreement in Hesse: In another case in Hesse, SCHUFA argues that it is not obliged to inform the data subject about how his or her rating is calculated, as this is a trade

[173] The case took place "before the entry into force of the GDPR". So, the provisions of Directive 95/46 apply. However, the applicable provisions in the present case are similar to GDPR.

secret. However, the organization is obligated to share this data with the relevant data protection authority under Article 31 GDPR[174]. The authority is the one who knows how the rating is calculated. But is this sufficient to uphold the principle of transparency, or does this practice violate this fundamental principle of data protection law? We already know that a principle or a right can be legally restricted under certain conditions. To check whether this has been done lawfully, we must apply the principle of proportionality. Is this measure suitable, necessary and proportionate to the intended purpose? The Hessian data protection authority answers in the affirmative. This data processing by SCHUFA is perfectly legal. It is legitimate not to tell us how our scores are calculated because otherwise the scores could be manipulated. The principle of transparency is not violated if SCHUFA only discloses this information to the data protection authority. The latter is responsible for assessing whether SCHUFA's calculation method is lawful (154 p. 114).

(c) Purchase of personal data - Violation of the purpose limitation principle

Hellenic Council of Sate 3040/2017[175] (155): In this case, a bank purchased personal data of individuals from another company targeting high-income customers to promote its products. The data protection authority imposed a fine of seventy-five thousand euros. The court considered the fine to be lawful because, in imposing the penalty, the authority considered the seriousness of the infringement, the number of personal data (about 52,000 records), but also the benefit expected from the controller.

Hellenic Council of State 1108/2017[176]: An advertising agency requested and received a list of potential clients from other companies for the purpose of loan advertising. The lists were based on several characteristics, such as age, annual income, addresses, disabilities (if any). They also had to indicate, inter alia, whether these people were holders of a loan (and its type). The applicant requested and received names and addresses of individuals who owned "BMW" vehicles in certain areas. In view of the above, the Hellenic Data Protection Authority considered

[174] "Article 31 [GDPR]. Cooperation with the supervisory authority. *The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks".*

[175] The case took place "before the entry into force of the GDPR". So, the provisions of Directive 95/46 apply. However, the applicable provisions in the present case are similar to GDPR.

[176] The case took place "before the entry into force of the GDPR". So, the provisions of Directive 95/46 apply. However, the applicable provisions in the present case are similar to GDPR.

that a sanction should be imposed on the advertising company for unlawful processing of personal data. The advertising company appealed to the courts, which ruled as follows: A fine is lawfully imposed on the advertising company. Even if the first companies lawfully collected the personal data, they unlawfully transferred them to the advertising company. When calculating the fine, the authority must take into account the nature of the personal data, the number of cases and the benefit that the controller expected from the unlawful processing.

Facebook vs Federal Cartel Office of Germany (156)**:** According to the decision of the Federal Cartel Office [177], the company "Facebook", owner of "Facebook.com", the most widespread social networking platform in Germany**,** abuses its dominant position in the market by unlawful gathering - and generally by processing – personal data from internet users (157).

"Facebook" collects information about users when they express their preferences via the platform's tools. For example, the user could respond to the posts displayed and express their likes, dissatisfaction or even their feelings.

In addition, "Facebook" collects information about its users through other "Facebook Group" platforms: through Instagram, a photo sharing platform, WhatsApp, a short messaging application, etc. All the information collected about the activities of individuals on these social media is used to create a profile for each user, so that the advertising displayed to the user is as targeted as possible to his interests.

Is there a legal basis for this processing? In principle, "Facebook" seems to be lawful, since it asks for user's consent when setting up the account. But is this consent really lawful? No, of course it is not. The way the consent is obtained, i.e. in advance, is not considered lawful. That is, it is not a free consent. Undeniably, "Facebook" is dominant in the social media market. Because of this dominance, the subject cannot freely consent: the user cannot choose another platform because there is no such a widely used platform· so the user is forced to give his consent.

Berlin Data Protection Authority about profiling (158 p. 120): A lawyer in Berlin applied for a credit card, which was rejected by the bank due to insufficient

creditworthiness. The lawyer asked the bank for an explanation, as he was a successful professional with a good SCHUFA score. The bank informed him about the personal data it processes itself and gave him only general information about the calculation of his creditworthiness, as there was a trade secret behind the way the creditworthiness was calculated. The lawyer filed a complaint to the data protection authority, which ruled, on the one hand, that the bank's decision was based on automated means and, on the other hand, that the bank's justification for rejecting the client had to be transparent so that he could adequately protect his interests.

We already know that SCHUFA is allowed not to tell the data subject how the scoring is calculated, as it is a trade secret. There is already relevant case law on this[178], but there is an important difference. In such cases, the controller must inform the data protection authority about the profiling procedure. Thus, the principle of transparency is not violated and the processing is lawful. However, in this case, no such information was provided to the data subject or the authority.

Moreover, SCHUFA is an organization that seems to comply with the GDPR. On the contrary, this bank does not seem to fully comply with the GDPR in this procedure. Why did the bank ignore the result of SCHUFA? Was the bank honest about the category of data it was processing? Did the bank process data that SCHUFA did not have? It is possible. If every bank carries out scoring, the details of which are not disclosed to the subject or the authority, on the one hand, the principle of transparency is violated and, on the other hand, a further violation must be assumed, e.g., the processing of unlawfully collected data. We have already seen that there is an illegal trade in personal data, in which banks are also involved[179].

In addition, we must not forget that algorithms are used to assess creditworthiness. So, it is an automated process. It is emphasized that SCHUFA only performs the scoring. It is the bank that takes into account all the relevant information, for example, to make a decision on the approval

[178] See above, DATA PROTECTION AUTHORITY in Hesse.
[179] See above, Federal Cartel Office vs Facebook

or rejection of a loan. The facts are therefore not exclusively subject to an automated process using AI systems. The processing by SCHUFA therefore ensures lawful processing[180].

In this particular case, however, the bank's response is not justified; it simply replies that the customer's creditworthiness is insufficient. This answer therefore violates the principle of transparency (again) on the one hand, and on the other hand there is possibly another violation: The customer was subjected to a solely automated decision-making process, which is completely illegal.

5.3.2.2. Overview

The processing by organizations such as TIRESIAS and SCHUFA is indeed absolutely necessary to satisfy the legitimate interest of banks to have a clear and certain picture of the creditworthiness of their creditors. This is extremely important for the safe functioning of the banking system. For this reason, it is necessary to inform the data subject about the transfer and any further processing of his or her personal data (when profiling). However, "consent" is not required. Furthermore, the controller does not need to inform the data subject every time a negative score is registered. Nor is it necessary to inform the data subject about the way the score is calculated. The method of assigning scores is a trade secret. It was also noted that knowing the method of calculation would give the subject the opportunity to influence the result. E.g. If one knows that his consumption habits are taken into account for profiling, he may avoid electronic transactions. Visiting a physical store and paying with cash man can ensure anonymity. Furthermore, although it is a trade secret, the GDPR requires that the principle of transparency must be observed. In this regard, SCHUFA inform the data protection authority about the way it scores. The latter decides whether the profiling is lawful and, in this way,

[180] The only problem would be identified if the Bank were to adopt SCHUFA's results uncritically. This is indeed a point that needs attention. The Bank may consult the organization, but the final decision is its own. And it must be sufficiently justified. Otherwise, human oversight during automated decision-making is not essential. In the present case, however, the Bank in question does not seem to refer to the SCHUFA score, but to some other score, which it probably conducted itself. This score, which does not even explain to us how it came about.

protects the data subject. The operation and safeguards of these organisations show that they comply with the GDPR. However, not all credit profiling is legal.

We have already seen that the purchase of personal data is a fact. The seller (of personal data) could be any company to which we have entrusted our data. On a small scale, the seller may be, for example, a car dealer who knows not only the car's value and manufacturer, but also our financial capability depending on the car' s value and the way we acquired it, e.g., by taking out a loan, paying in installments etc. In the field of marketing, but on an extremely large scale (due to the number of data processed, but also the number of people) we find social media. We have already seen in the case of "Facebook" that the company processes data for targeted advertising, which was considered illegal at least in the particular circumstances of the case.

On the other hand, the buyer (of personal data) could be any company targeting a specific group (such car owners or people with a certain purchasing power). Such an illegal transmission is for marketing purposes. From the above case-law[181] is derived that a bank is likely to buy personal data from citizens, either for marketing purposes or to assess their creditworthiness[182].

So, if a social networking platform is the seller and a bank is the buyer, then an illegal processing on a large scale arises (countless data, countless individuals). Moreover, if the processing is aimed at credit scoring, this poses particularly high risks to privacy, as consumption habits are processed for marketing purposes. Moreover, if we take into account that this already unlawful processing is take place by automated means (often even without any substantial human intervention in the final decision), it is a blatant violation for human rights.

As follows from the above, profiling by organizations such as SCHUFA is lawful, because it a) does not involve data from activity in social media, b) requires control of the scoring method by the competent data protection authority, but also c) requires effective human control, since the bank and not the SCUFA decides.

Therefore, various large scale data processing and automated decisions are unlawful and should be addressed. The use of technology, especially the use of artificial intelligence, is undoubtedly crucial in this context, as profiling on such a large scale cannot possibly take place by means

[181] See the chapter 5.3.2.1.
[182] See Hellenic Council of State.

other than the use of algorithms. However, the number of data processed and the number of individuals involved is so enormous because of the possibilities offered by the AI. No human factor could process such a large amount of data in the time it takes a software program to do so. So, the use of AI magnifies the problem. The number of personal data and data subjects are among the elements that the data protection authority takes into account calculating the amount of the fine. However, we have just mentioned that AI is crucial for processing many personal data and data subjects. Therefore, the fines for illegal profiling are increased with the use of AI (the reason is not merely the use of AI, but the fact that AI can process data on a large scale). Furthermore, there is another requirement: profiling is illegal if the processing has "*legal effects on the natural person or similarly significantly affects the natural person*"[183].

The fact that the use of AI is crucial for profiling was the reason for the Article 22 GDPR on automated decision-making for individuals, which explicitly mentions that profiling is included[184]. From the provision, it can be concluded that the legislator considers profiling and AI (automated decision making) to be compatible from the outset. Indeed, it is difficult to argue that profiling is currently done in other ways. In addition, Article 35 GDPR stipulates that a DPIA must be carried out in this case, because automated profiling if it is systematic and comprehensive[185].

So, the assessment of creditworthiness with AI systems clearly falls within the scope of the above provisions. It is therefore a lawful processing, for which, however, the relevant measures of the GDPR must be observed: Keeping records (as for any processing), carrying out a DPIA (as explicitly provided for) and human intervention before any automated decision making. In addition, all general provisions of the GDPR must be complied with. In other words, the general principles under Art. 5 and therefore a legal basis under Art. 6 applies. In this case the lawful basis is the legitimate interest of the banks for the smooth functioning of the banking system.

---

[183] Unless there are any exceptions to the provisions of Art. 22 GDPR, which we have seen above.

[184] Article 22, "*automated decision making, including profiling*".

[185] Article 35 (3) (a), "*A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*".

It should be noted that in principle there are no special category data in this particular processing. However, if it is determined on the basis of the data minimisation principle that the processing of such data is also necessary, an Article 9 legal basis should also be applied.

What we have seen about privacy by design and default applies here, too. Thus, after weighing the risks and benefits of the above processing, the controller should take measures that mitigate the risk. Such measures (by design) include keeping data secure, allowing access only by authorized personnel, retaining for a certain period of time and possibly pseudonymizing it if possible. For example, there could be two databases, one containing the data and pseudonyms, and a second in which the pseudonyms are matched with the real names. Also, according to the principle of privacy by default, software can be set by the manufacturer or the user to process as little data as possible.

By taking the above into account and making efforts to comply with the GDPR, data subjects are exposed to fewer risks. We have already mentioned that the use of AI systems increases the risks of processing anyway, as it is processing on a large scale. Compliance with GDPR (e.g. having a data breach recovery plan, policies) protects controllers and processors from fines.

5.3.3. Application of the AI ACT in credit profiling – comparison with the GDPR

5.3.3.1. AI ACT's requirements for high-risk practices

The AI ACT provides not only the prohibited but also high-risk AI systems which are not prohibited. Consistent with the above, high-risk AI systems may have the characteristics of Article 6 (1) or be those listed in Annex III of the Act. That is, the Act on the concept of high-risk systems provides, on the one hand, a general description so that any system with these characteristics can be included in this category and, on the other hand, it provides an indicative list of certain such systems in the Annex III[186].

This seems extremely helpful because such a structure contributes to legal certainty. Any manufacturer or user, etc., can know with certainty whether a particular system in which he is

[186] See above, chapter 5.1.

interested is permissible, etc. Such high-risk processing concerns access to essential private and public services and benefits.

According to the AI ACT, evaluating the creditworthiness fall within the scope of high-risk systems[187]. Therefore, the Act governs the case of credit scoring, as described above[188]. But what does the evaluating involve?

The following articles of the regulation specify the legislator's requirements for the use of the above-mentioned systems, the obligations of providers and users, and further details on the compliance of AI systems with the requirements of the regulation[189]. This structure initially gives the impression of an integrated approach to AI systems. If these requirements are correct and complete, users, etc., can feel secure as long as they are met.

The following articles on the requirements of the legislator for high-risk systems describe in particular a risk management system (identification and analysis, assessment and evaluation of risks)[190], data governance[191], technical documentation[192], records[193], "*transparency and provision of information to users"*[194], *"human oversight"*[195], accuracy, robustness and cybersecurity throughout their lifecycle[196], ensuring their quality and verification of compliance with the requirements[197], "*corrective actions required to bring the system into compliance, withdraw or recall"*[198], *"duty of information and cooperation with competent authorities in case of risk"*[199], proper use[200], EU harmonised standards[201], measures in support of innovation[202], "*further processing of personal*

[187] *"5. Access to and enjoyment of essential private services and public services and benefits: […] (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use".*
[188] See above, chapter about SCHUFA.
[189] Articles 16-29 AI ACT.
[190] Article 9 AI ACT.
[191] Article 10 AI ACT.
[192] Article 11 AI ACT.
[193] Article 12 AI ACT.
[194] Articles 13 & 52 AI ACT.
[195] Article 14 AI ACT.
[196] Article 15 AI ACT.
[197] Articles 16-20 & 24-28 AI ACT.
[198] Article 21 AI ACT.
[199] Articles 22-23 AI ACT.
[200] Article 29 AI ACT.
[201] Articles 40-51 AI ACT.
[202] Article 53 AI ACT.

data for the development of certain AI systems in the public interest in the AI regulatory sandbox"[203], "*measures for small-scale providers and users*"[204] establishment, structure and tasks of the European Artificial Intelligence Board, designation of national competent authorities, tasks and penalties[205], post-market monitoring, information sharing, market surveillance[206], codes of conduct[207], confidentiality[208], delegation of power and committee procedure[209], final provisions concerning regulations 300/8008, 167/2013, 168/2013, directives 2014/90, 2016/797 and regulations 2018/858, 2018/1139, 2019/2144[210] and provisions about "*AI systems already placed on the market or into service*"[211].

5.3.3.2. Comparison with the GDPR

In light of the above, we note that the Act provides for several technical measures and procedures to ensure its application. However, the Act contains very few provisions on general principles of data protection law.

An important principle enshrined in personal data law is the principle of transparency. The Act also provides for the principle of transparency. First, it states that humans should usually know "*that they are interacting with an AI system*". This is the case, for example, with emotion recognition systems or the lie detector. However, there are exceptions "*in the case of processing for law enforcement purposes*"[212]. In addition, the principle of transparency is emphasised with regard to the necessary "content" of the system's instructions for use[213].

---

[203] Article 54 AI ACT.
[204] Article 55 AI ACT.
[205] Articles 30-39, 56-60 & 71-72 AI ACT.
[206] Articles 61-68 AI ACT.
[207] Article 69 AI ACT.
[208] Article 70 AI ACT.
[209] Articles 73-74 & 84 AI ACT.
[210] Articles 75-82 AI ACT.
[211] Article 83 AI ACT.
[212] "Article 52 (1) AI ACT. *Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless […]".*
[213] "Article 13 (2) AI ACT. *High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format […]: (a) the identity […] of the provider […]; (b) the characteristics, […] including: (i) its intended purpose; (ii) the level of accuracy, robustness and cybersecurity […] (iii) any known or foreseeable circumstance, […], which may lead to risks to the health and safety or fundamental*

The German Federal Council ("Bundesrat") states in its report to the European Parliament and the European Commission[214] (58) that the Act should explicitly mention the following: AI systems must inter alia comply with the legislation on the protection of fundamental human rights and in particular on the protection of personal data. After reviewing the AI ACT, the German Federal Council note that references to the protection of fundamental rights are made both in the Explanatory Memorandum and in individual articles.

In this way, it is clear that while the Act does not introduce a labyrinthine system of rights, it does not disregard them either. It explicitly refers to the basic texts of European legislation and indicates that it respects them. However, the provisions are few and not exhaustive. If there were consistency with the GDPR, it would be easier to assume that these references are sufficient. However, because the Act conflicts in certain cases[215] with personal data legislation, these few references are insufficient· legal uncertainty remains. The omissions should be corrected as they contribute to the creation of legal uncertainty and are unacceptable. If the controller installs - in good faith - an AI system that is allowed under the AI ACT but prohibited under the GDPR, it will either face an unjustified fine (if data protection authorities apply the GDPR) or the data subject will not be able to adequately protect itself (if data protection authorities apply the AI ACT).

The Federal Council also believes that the list of "high-risk systems" in Annex III is insufficient and lacks legal certainty. It is of great importance that this list is reviewed by the Commission and that more systems need to be added. In this context, it is stated that other cases of scoring should be added in addition to credit scoring (58). However, such additions should be

rights; (iv) its performance […]. (c) the changes […]; (d) the human oversight measures […] (e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates".

[214] It should be stressed that the Bundesrat has produced an extensive report on the shortcomings, errors and omissions of the Proposal and has indicated important problems and risks that lie ahead, if the AI ACT is not corrected, before it has been voted on. On the contrary, most countries were either indifferent and did not report on it[214], or indulged in wishful thinking about the proposal.

[215] See above, the Chapter about biometric identification systems and below, the Chapter about social scoring.

compatible with the data protection law. If this list is removed, we could still apply the GDPR and the LED to assess whether a processing operation is lawful[216].

Finally, a look at sanctions is also important. It should be noted that the two regulations are similar in terms of fines. The fines under the Act [217] are the same or higher than those under the GDPR[218]. This makes sense, as the use of AI can exacerbate the risk. However, there are some problems. (a) There will be two competent authorities: Data Protection Authority and AI Systems' Authority? (b) Which authority will impose these fines? (c) Can these fines be imposed in parallel?

(a) Each Member State may establish a new authority or designate an (existing) administrative authority competent to impose the sanctions provided for in the new Regulation. Could the data protection authority have such competence? As far as the processing of personal data is concerned, clearly yes. However, there are applications of AI systems where no personal data are processed. In these cases, the data protection authority is probably not the appropriate body and a new special authority should be established.

(b) If there are two separate authorities, which authority will impose fines for the processing of personal data by AI systems? We believe that the data protection authority should be responsible for imposing fines for personal data breaches, whether it is a breach of the GDPR or the Act. Given that the Act acts as a supplement, it would also be useful to provide in the GDPR that these fines shall apply as long as the breach is not punished more severely by other provisions.

(c) In addition, it is certain that only one of the two authorities should impose the fine. This is based on the principle "ne bis in idem". According to this principle, a fine cannot be imposed twice for the same legal right. In each case, the legal right matters, regardless of whether the fine

---

[216] Explanatory Memorandum of the AI ACT, Chapter 3.5. Fundamental rights.

[217] Article 71 AI ACT. *"[…] administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher […] fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher. […] fines of up to 10 000 000 EUR or, if the offender is a company, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher […]".*

[218] *"Art. 83 GDPR. "[…] be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher […]".*

is imposed by the data protection authority or by an authority that may be newly established. So, since only one of the two fines will be imposed, only the first one will be valid. Indeed, it is simply forbidden to impose a second fine for the same legal right.

Regarding specifically credit scoring, it is a permissible processing under both the GDPR and AI ACT. It is also classified as a high-risk processing both in the AI ACT and the GDPR, since GDPR considered profiling as high-risk[219]. In addition, Articles 22 and 35 GDPR must also be considered applicable at the AI ACT. This means that a DPIA is still required. The application of all measures provided for in the Act does not repeal the DPIA, as the Act is considered a supplement to the Regulation and does not repeal it. Likewise, all the requirements of the GDPR, such as recording of activities and all the general principles, apply. As for the rights of the data subject, these are almost exclusively governed by the GDPR, as they are generally not mentioned in the Act[220].

With regard to this high-risk processing, we note that there is no fundamental contradiction between the AI ACT and GDPR, nor is there any legal uncertainty. The provision in the Annex III is clear. In such a case, clarity is helpful rather than confusing for the controller. However, although the GDPR also contains explicit provisions on this subject, the presence of a citation with case studies is legitimate. It contributes to legal certainty. However, general issues, such as the question of sanctions, should also be regulated here so that the AI ACT is consistent with the GDPR.

However, any shortcomings do not mean that the AI ACT should not be voted on at all. It is clear from the above that compliance with the requirements and taking measures would help to manage the risks associated with the use of AI. However, until the AI ACT complies with the basic personal data legislation etc, it is not possible to assess the extent of its contribution. Only

[219] Article 35 (1) GDPR. *"[…] Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data […]. 3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".*

[220] See Article 13 AI ACT.

a further “fruitful dialogue” between the EU institutions and the Member States could ensure that the Act is - as far as possible - free of errors and can be successfully implemented by the Member States.

5.4. Social credit system

5.4.1. The scope: the example of China

Throughout the world, it is common to use a system to verify the creditworthiness of individuals. As mentioned earlier, banking institutions work with official agencies that collect and process their customers' data on their behalf. As technology advances, algorithms can be used to derive more and more results from the data.

An extension of the existing credit rating system in China is the social credit system or credit information system (159) (160). In the 1980s, the Chinese government attempted to develop a financial credit rating system, particularly for individuals and small businesses (161) (162) (163). In developing this system, China proceeded to process on a large-scale personal data of citizens, concerning not only their creditworthiness or their profile as employees, but also violations and, more generally, their social behaviour, in order to create a profile of each citizen (164). Based on this profile, each citizen is granted privileges or excluded from certain benefits, e.g., a prospective student can be rejected from university because his father has financial problems (165), dog owners receive points - deducted if their dog walks without a leash (166) , drivers are penalised for dangerous driving behaviour, and, in general, citizens are screened for their habits, e.g., buying video games, which leads to point deductions (160). This is a system of moral classification ranks citizens based on their social credit (160), aims to create an ideal society (167) and promote the rule of law (168). Nevertheless, more than 30 million people in China "*are banned from leaving the country, traveling by train or plane, having insurance, renting a home, going to restaurants, and taking out a loan all because of their social credit score*" (150).

In parallel, China's internet providers, etc., with government support, *"are developing scoring systems based on personal data produced online" […]* (169), *while offline "data, such as the activities and behaviours that take place within the family and social network", are also expected to be assessed* (170 pp. 297-308). *"Thus, Chinese citizens are facing a future in which their identity and social status will become increasingly externally shaped—through algorithmic processing of their own personal data and through the actions and behaviours of their friends and family—rather than intersubjectively through equitable social relations of recognition"* (171 pp. 519-537) (172 pp. 609-625).

China is a technological giant, where artificial intelligence applications are rapidly developing (173) (174). As for the area of biometric recognition, it is taking place in transactions in credit institutions as well as in less important transactions such as hotel reservations. Recently, it became known that an application is already in operation that scans the digital identity of citizens so that they can access important services (175). *Law enforcement agencies are also using the technology "to identify suspicious individuals", and "schools are monitoring students' attention in class".* Finally, emotion recognition technologies are being developed in China in addition to biometric facial recognition (176).

This technological development in China suggests that the social credit system is a single, nationwide system that automatically processes citizens' personal data to perform social profiling (177). However, this is controversial. It is argued that each city implements its own system, for the creation of which no artificial intelligence is used (178).

Indeed, it is difficult for us to be well informed about a different continent with a completely different legal regime. However, for the purpose of this paper, what is important is not what exactly is happening in Asia, but what is happening and could happen in Europe.

5.4.2. Application of the GDPR in social classification

In any case, if social scoring take place with AI systems, Article 22 GDPR applies here as well. The data subject cannot - as a general rule – "*be subject to a decision based solely on automated processing which produces legal [or other important] effects concerning him or her*". We do not really know, if social scoring in China produces legal effects concerning data subjects, though a social scoring in general could produce legal or other important effects.

Article 22 provides for some exceptions. Is there an exception to the above prohibition here? Could anyone ever *"be subject to automated decision making"* for social scoring? It is certainly not possible to apply the exceptions in (a) and (c) in this case because: (a) first, the relationship between the controller and the data subject is not contractual, but takes place for the purpose of granting social benefits and social sanctions· (c) second, since the controller is primarily the State, explicit consent would not be sufficient, since it would not be free due to the superior position of the State to the citizen under its powers.

Subparagraph (b) states that such processing is lawful if permitted by national or Union law, which *"at the same time takes appropriate measures to protect the rights of data subjects"*. This paragraph is clarified by Recital 71, which states*: "However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject*, *including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent".*

Could Article 22 (2) (b) and Recital 71 refer to social scoring? It is clear from the above that the Act is aimed at the prevention of crime and not at social scoring. However, even in the scenario where social scoring is performed after human intervention or solely by a human, the processing would still be illegal, because this processing contradicts the Article 5 GDPR. Social scoring could not be reconciled with the principle of lawful processing[221] and the principle of purpose limitation[222], because, on the one hand, there is no legal basis for such processing and, on the other hand, it is not compatible with a clear and defined purpose.

5.4.3. Application of the AI ACT in social classification

According to Art. 5 of the AI ACT, it states, inter alia,

"1. The following artificial intelligence practices shall be prohibited[223]: […]

***(c)** the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:*

[221] According to Article 5(1) (a) GDPR.
[222] According to Article 5(1) (b) GDPR.
[223] Article 5 AI ACT.

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated *to the contexts in which the data was originally generated or collected;*

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity; […]"[224].

- *AI systems providing social scoring* is some kind of ranking depending on our social profile or social behavior.
- *which evaluate or classify the trustworthiness of natural persons:* In particular, this classification consists of an evaluation and categorization. Such evaluation takes place in China's social credit system: the number of credits accumulated could lead to certain effects.
- *based on their social behaviour in multiple contexts*: This social behaviour could be, for example, credit score, criminal record, driving behavior, consumption habits.
- *or (based on) known or predicted personal or personality characteristics*: The evaluation and classification might not be based on actual social behavior, but on characteristics that are predicted to lead to a particular behaviour.
- *"by public authorities or on their behalf":* The provision mentions public authorities (as controllers) or other entities/people on their behalf (processors etc). So, social scoring by private individuals is allowed? Do private companies offer more guarantees for this processing or social scoring (i.e. social profiling) by private companies is impossible? It has been clear that private companies, such as social media, are able to perform such processing. Moreover, there are some cases where social media processed in unlawful way the collected data. Therefore, such processing should undoubtedly be prohibited by both public and private entities, whether or not they act on behalf of public authorities (140).
- *for a certain period of time*: Since the minor is prohibited ("*a certain period of time"*), the major (*indefinitely*) is prohibited, too.
- The Act refers to systems that *[and especially those which results in] (i) "detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected" or (ii) "that is*

[224] Recital 17 AI ACT: *"AI systems providing* ***social scoring*** *of natural persons for general purpose by public authorities or on their behalf may lead to discriminatory outcomes […]. Such AI systems evaluate or classify the trustworthiness of natural persons based on their social behaviour[…]. Such AI systems should be therefore prohibited".*

unjustified or disproportionate to their social behaviour or its gravity"[225]*:* we note that this case reflects the protection of non-discrimination, which is also a fundamental right of the Union. However, in addition to the principle of non-discrimination, the provision also aims to protect our personal data. This is also evident from Recital 15 AI ACT, which states that: *"[…] social control practices […] are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child".*

Specifically:

- *"(i) detrimental or unfavourable treatment of certain natural persons or whole groups":* The legislator refers to the principle of non-discrimination[226]. Thus, the AI system is prohibited if it introduces discriminatory treatment of the data subject, namely treatment that harms or has negative effects for him/her.
- *"Thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected":* Here, the legislator refers to the principle of purpose limitation as expressed in the Article 5 (1) (b) GDPR. On the one hand, the data are collected for legitimate and specified purposes, and on the other hand, they must not be processed for purposes other than those for which they were collected. Thus, for example, if personal data are collected in the context of driving behavior, they cannot be used for the professional development of an employee, unless the employee is a professional driver.
- *or (ii) "that is unjustified or disproportionate to their social behaviour or its gravity": T*he legislature refers to the principle of proportionality. A restriction of a fundamental right could be lawful, if the controller respects the principle of proportionality. Namely, the means used by the controller to achieve his purposes must be appropriate, necessary, and proportionate (stricto sensu) with the objective pursued. In other words, we should ask the following: (a) Could the controller achieve the purpose if he used this specific means? (If the answer is "yes", we can proceed to the next question, otherwise the restriction is unlawful), (b) Could the controller

[225] Recital 17 AI ACT: *"AI systems providing social scoring […] may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour […]. Such AI systems should be therefore prohibited".*

[226] See above, Chapter 3.

achieve the purpose, if he used less restrictive means? (If the answer is "no", we can proceed to the next question, otherwise the restriction is unlawful), and (c) Is the means legitimate in light of the purpose? (If the answer is "yes", the restrictive means is legitimate; otherwise, the restrictive means is unlawful) (179 pp. 439-466).

Consequently, according to the AI ACT, if an AI system makes a social judgment without a discrimination is lawful. Furthermore, if an AI system makes a social judgment with a justified or proportionate discrimination is lawful, too.

5.4.4. The GDPR and the AI ACT for social scoring: comparison

The German Bundesrat believes that all of these systems should be prohibited. The conditions and special circumstances mentioned in the Act are meaningless, as a risk exists even if social scoring is performed without the use of AI (58). EDPB-EDPS also state that the AI ACT should ban all social scoring. The report argues that current personal data protection legislation does not allow any type of social scoring. In particular, the report states that *"there is no legal basis for processing based on Article 4 LED"* (140 p. 29).

But does social scoring really fall within the scope of the LED? Social scoring as a concept does not seem to have the same purpose as the LED. Social scoring does not seem to fall within the scope of the LED as it does not seem (e.g. in China) to be used for the prevention, detection, prosecution, etc. of crimes. It could, of course, be used for such purposes. We think it is more appropriate to examine the legitimacy of social scoring under the GDPR, regardless of whether the processing is carried out by the state or by a private individual. Although, regardless of whether the applicable law is the GDPR or the LED, this does not diverse the answer.

The controller cannot lawfully carry out a social evaluation under any circumstances, as the social scoring is not compatible with the general principles of the processing[227]. First of all, this processing is not compatible with the purpose limitation. The violation of the purpose limitation principle constitutes unlawful processing, which is prohibited, regardless all the other conditions, such as the nature of the controller/processor and the discrimination against the data

[227] Article 5 GDPR, Article 4 LED.

subject. Discrimination is very likely to be introduced with social scoring, however, it is not a necessary condition for judging social scoring as prohibited, as it is in any case an illegal processing.

However, the above conclusions lead to the following paradoxical result. The GDPR and the LED are stricter than the AI ACT. If EU vote for the AI ACT with this content, there will be two regulations with different protection frameworks. For example, social scoring without the use of AI systems will be prohibited by the GDPR, while social scoring using AI systems will be allowed under certain conditions by the AI ACT. According to the provision, there are specific conditions for prohibiting such processing, which, if not met, processing obviously is lawful, i.e., just a high-risk processing. However, this legal paradox cannot be tolerated. This provision should be revised and social scoring should be generally prohibited.

6. Research: How familiar are we with artificial intelligent systems & data protection law

6.1. Methodology

6.1.1. Goal

In order to understand the importance of the AI ACT, we have already mentioned that we will try to investigate how EU citizens perceive AI and privacy issues. Our goal is to understand, whether EU citizens consider the use of AI systems related to the data protection as useful and secure or they do not trust AI systems at all[228].

To conduct the research, we searched for literature and case law and examined legislation, as presented in the chapters above.

6.1.2. Sample and design criteria

This chapter first defines the criteria on the basis of which the questionnaire was designed.

The following criteria were considered in the selection of the sample[229] :

We have already mentioned what was the occasion for the survey: to determine the relationship of citizens to the issues addressed in this thesis. However, it is impossible to create a representative sample of the entire European population. For this reason, and considering that our research is a pilot project, it was decided that our sample would be European students, namely German and Greek students aged up to 33, whose studies are not relevant to the subject of our research.

Thus, we are primarily concerned with individuals who are from Germany or Greece or who live and study there permanently. We excluded individuals who study in these countries but

[228] For example, do we decide for or against AI by definition? Or does our response depend on the risks AI poses to privacy and other fundamental rights? For example, do we accept the use of AI systems only if they do not involve AI processing, or only if we consider that there are no high risks? Do we consider legal processing to be safe?

[229] The nature of our sampling is non-probabilistic (non-probabilistic sampling) because we rely on techniques that do not apply the laws of probability in selecting the sample, a widely used model in pilot surveys such as this one.

live permanently in other countries because we felt that the sample was not homogeneous and that this could influence the results and thus our conclusions.

The sample consists of ten German and ten Greek students[230] aged up to 33 years, selected at the discretion of the researcher[231]. Since the questions are about topics related to modern technology, it was assumed that young adults of generation "Z" (currently up to about 26 years old) [232] (180) (181) are the ones who can best understand the concepts in a short period of time, have some elementary experience in dealing with AI systems, and can answer such questions in a way that produces assessable results (182) (183) (184). Generation "Z"'s' familiarity with technology is one of its qualitative characteristics. The youngest Millennials (currently 27-33 years old) (185) (186) are also considered to be familiar with technology. In addition, as students are likely to be in any case familiar with such a modern topic and, further, to understand the questionnaire (185) (186)[233].

The survey will be conducted through structured interviews[234], based on a questionnaire containing both "open-ended" and "closed-ended" questions[235]. For a better understanding of the concepts, the questionnaire will also be accompanied by images. From the responses, we

[230] For reasons to be developed below, legal and computer students were excluded from the sample.

[231] In order for the sample to be as representative as possible, the interviews were conducted with both the age category 18-26, and the age category 27-33, both with undergraduate and postgraduate students, both with men and women. However, we will not draw individual conclusions for each of the above categories. Also, although a choice was made based on gender, it was not requested to record the gender of the participants for the following reason. It is now judged that one must enable the subject among three or more sexes, as each one defines himself. Because the interviews were personal, we thought that this was a sensitive piece of information that the interviewee might not want to share with us. Besides, we judge that it was not such a crucial piece of information for us. Therefore, taking into account the principle of minimization and the possible reluctance to participate, we did not ask the participants about it.

[232] There is no commonly accepted exact date for the separation of generations. For our research we took for granted the mention of "CNBC". (256)

[233]There is no commonly accepted chronology for the separation of generations. As our basis we chose the CNN article, because it explicitly refers to the separation of young and old millennials by setting a specific age limit.

[234] With our research we tried to learn about the behaviors of a specific group of citizens in relation to the above practices and to approach the perceptions and motives/reasons for these behaviors.

[235] We opted for a combination of quantitative and qualitative research, both in terms of data collection and methodological approach.

will primarily highlight the relevant statistics [236]. Open-ended questions will help to confirm and justify the results of the closed-ended questions.

Regarding the design criteria of the questionnaire[237], the following decisions were made:

- ✓ Short and concise questionnaire, as not to discourage the participant
- ✓ Formulation of short questions
- ✓ Formulation of clear and unambiguous questions
- ✓ Avoiding questions with negative content
- ✓ Omitting one-sided terms
- ✓ Perception of the participants' ability to answer: the selection of the sample, the questions with examples from everyday life, but also the open questions help to check the reliability of the answers[238].

[236] Both in terms of the totality of responses, and comparatively, according to the "origin" of the respondent.

[237] In particular, the following were taken into account in the research and in the definition of the criteria: Μιλτιάδης Χαλικιας etc, National Technical University of Athens (2015) (281), Απόστολος Μπατσίδης, University of Ioannina, (285), Μαρία Χασάνδρα & Μάριος Γούδας, University of Thessaly (289 pp. 31-48), K. Ζαφειρόπουλος, University of Macedonia, Hellenic Republic (290), Στυλιανή Τζιαφέρη, National University of Athens (2014) (272), Εργαστήριο Ψυχολογίας της Άσκησης και Ποιότητας Ζωής (Laboratory of Exercise Psychology and Quality of Life), University of Thessaly (287), Research Methods, University of West Attica (284), Παπαιωάννου, A. etc, University of Thessaly (288 pp. 341-364), Qualitative Research Methods. Colorado State University (274), University of Southern California Libraries (295), Chenail, Ronald J., Nova Southeastern University (278), Μαρία Σ. Άνθη (2012) (291), Pritha Bhandari (280), Denzin, Norman. K. and Yvonna S. Lincoln (2005) (279 p. 10), Heath, A. W. (1997) (277), Marshall, Catherine and Gretchen B. Rossman (1999) (276), Maxwell, Joseph A. (2009) (275 pp. 214-253), Yin, Robert K. (2015) (273), etc (271), (282), (283), (286).
For the structure of the methodology, the work of Ines Fichtinger, "A Review of Security Operation Centers: State of the Art and Current Challenges", was taken into account (257). Also, criteria mentioned in this work were taken into account, since these could be applied accordingly in our own research, which differs in the way it was carried out. The student for the conduct of his methodology refers to the following sources: Stehr-Green PA, Stehr-Green JK, Nelson A (258), Williams A (2003) (263 pp. 245-252), Boynton PM, Greenhalgh T (2004) (261), Reja U, Manfreda K, Hlebec V et al. (2003) (259), Connor Desai S, Reimers S (2019) (260), Lietz P (2010) (262 pp. 249-272), Fray RB (1996) (264), Taylor-Powell E (2005) (265), Lefever S, Dal M, Matthíasdóttir Á (2007) (266), Kalantari D. H, Kalantari D. E, Maleki S (2011) (294 pp. 935-941), Typeform https://www.typeform.com/ (267), Evans JR, Mathur A (2005) (268 pp. 195-219), Lumsden J (2007) (269), Abraham SY, Steiger DM, Sullivan C (270)

[238] A) Therefore, it was tried to include as many questions as possible from our everyday life to make them understandable.
B) Also, the remaining questions contain "hypothetical examples" derived from the content of the AI ACT. An attempt has been made to accurately reflect some of the content of the AI ACT, while at the same time formulating it in such a way that it is perceived by the reader.

- ✓ The format of the questions: they are mostly closed-ended questions. These questions are multiple-choice (with the option to choose either one or more answers). For questions with multiple answer choices, the number of possible answers was not limited because the goal is not to compare answer choices, i.e., which answer choices are preferred, but whether respondents accept or reject each of these answer choices. Open-ended questions aim to confirm and justify the result of quantitative research.
- ✓ The structure of the questions: the questions were divided into individual sections so that there is a follow-up per group of questions. At the beginning of each individual section, a simple question is asked to understand the topic with an example that relates to our daily life, and then more theoretical questions are asked (based on the AI ACT). The open-ended questions were asked at the beginning of each section to avoid influencing the participants with closed-ended questions that have the same topic.
- ✓ Personal questions were asked at the end of the questionnaire.

6.1.3. Creation

The questionnaire was originally written in "Word", where its structure was formed, a grammar and spelling check was performed. Then the pretests took place, both in an electronic environment and in the form of interviews. Considering the experience with the pretests, it was decided that the interviews should be conducted based on this structured questionnaire, so that the researcher had direct contact and interaction with the participants. This contributed to the understanding of the topic: the subject has the opportunity to ask clarifying questions to the researcher in the form of the structured questionnaire. And in general, he/she can develop his/her thoughts.

At the beginning of the interview, we explained the context in which the research will be conducted and its scope in general, the target group it is aimed at, and the estimated time that will be spent on it. We also provided information about the characteristics of the survey (e.g., anonymity, "subject's right to withdraw at any time"). Finally, we provided contact information (e.g., for submitting requests for deletion) and thanked respondents who would participate in the survey. At the same time, we encouraged them to ask questions and participate.

6.1.4. Pretest

First, five people were invited to participate in order to identify grammatical and lexical errors and issues of ambiguity. Subsequently, five additional individuals assisted in identifying comprehension issues and estimated length of performance. In addition, a random sample of participants was used to determine whether bias, structural errors, comprehension difficulties, and the impersonal or participatory position of the researcher influenced responses.

- ✓ In order to achieve an optimal research result, the most appropriate method chosen was the interview with a structured questionnaire. This means that, in principle, the questionnaire is strictly structured, but the participant has the feeling that it is a relaxed procedure, since he can, if he wishes, ask the researcher for clarifications, but also freely develop his thoughts on the subject. On the contrary, the impersonal questionnaire discourages the active participation of the respondent.
- ✓ In testing, it was found that certain factors can affect the outcome. For example, it was found that it is not useful for subjects to know the exact purpose of our research. This sometimes leads the subjects to give the "right answers", in order not to be judged negatively by the researcher. Therefore, the exact goals of the research should not be disclosed to the subject.
- ✓ Similarly, students who are familiar with the subject because of their studies or their work should not participate. Not only they could influence the result (e.g. about the average we are aware of the topic), but also they tried to give "correct" answers, as it happened above with students who knew the aim of our research. Therefore, these students were excluded from further interviews.
- ✓ The interviews were anonymous, as we did not note names or other information about the participants. In some cases, however, the people we interviewed were known. As long as there is no recording in a file, there is also no data processing covered by the GDPR, as the individuals are not identifiable (anonymization). However, there is also an issue with the confidentiality. We cannot disclose what we collect in our research. In order to create a climate of trust between the researcher and the participants, it should be pointed out that after the extraction of the results, the researcher's anonymous notes will also be deleted. In addition, the respondent should be informed that they are free to leave the interview at any time.

- ✓ Even if open-ended and closed-ended questions with relevant content are asked in the questionnaire, the open-ended questions should have priority. Otherwise, there is a possibility that the respondent will be influenced by the previous closed-ended questions. Therefore, it was considered that open-ended questions should be asked before relevant closed-ended questions.
- ✓ It was understood that questions should be grouped and divided into sections and that there should be some sort of escalation about their difficulty. This helps the interviewee understand a complex topic and follow the flow of the interview easily.
- ✓ It was assumed that it would not be useful to burden the questionnaire with unnecessary definitions. The immediacy of the interview allows us to give the necessary explanations when and where necessary, without tiring the questioner with definitions that are probably difficult to understand anyway. On the contrary, there is the possibility of giving simplified interpretations and examples to understand the facts, if necessary. In addition to the verbal explanations and examples, the researcher could show the interviewee relevant pictures that depicted a particular application of AI systems, so that the subject of the discussion was understandable.
- ✓ It was understood that open-ended questions should not contain sub-questions, as this causes confusion among participants and affects the outcome. Questions should be clear, brief and address only one topic at a time.
- ✓ Accordingly, closed-ended questions should also be short and clear, and the use of multiple-choice questions (with several possible answers) does not affect the subject's judgment or the outcome of the study. Especially in our case, where closed-ended questions are not intended to favour one practice or another, but to help us understand the motives and perceptions of the subject, not for each individual practice, but overall. That is, it is about drawing a conclusion about the subject's criteria. And this can be done even if the subject generally accepts or rejects all possible answers. Any limitation on the number of responses would simply not allow us to know the respondent's opinion on the topics.

6.2. The questionnaire

The questionnaire has been updated several times[239].

After the above corrections, the questionnaire has the following form:

"AI Systems

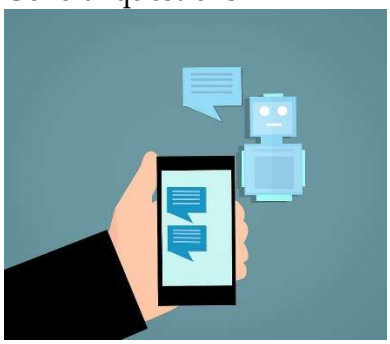
Dear Participant,
this pilot study is conducted as part of my master thesis at the University of Regensburg (Faculty of Business, Economics and Management Information Systems). Please participate only if you are a young

[239] Previously it looked like this: "QUESTIONNAIRE. Dear participants, we warmly thank you for your participation in our research. This research aims to identify how familiar we are with the data protection concerning the technology. Please, take part, if only you are a student, who live in EU. The completion of the questionnaire is expected to take … minutes. All the information you provide will be completely confidential and anonymous and will only be used for the purposes of the study. You can withdraw any data you have provided by emailing the researcher and providing the exact time and day you completed the survey. The researcher will store the answers only for two months, in order to exact results and, then, the researcher will delete the answers. This research is carried out in the context of master thesis for the University of Regensburg.

1. In what country are you currently living and studying? -Germany, Greece, Other ……
2. What is your level of study? -Undergraduate student (BSc), Postgraduate student (MSc), Doctoral student (PhD), Other
3. Are your studies (or perhaps your work) related to computer science or law? – Yes, No, Other
4. Have you been informed about the protection of personal data (e.g. from the University, government)? – Yes, No, Other
5. Do you use chatbots, when the services or businesses you work with give you such an opportunity? Why? - Yes, No, Sometimes, Other …, Why? ……
6. Would you use a chatbot for a financial or legal issue? Why? -Yes, No, Other....., Why? …….
7. Would you like crucial private companies in your country to be equipped with artificial intelligence systems, in order to process your data, create a profile for you and reply to your applications? What kind of services and why? - Banks e.g. for granting a loan / credit card etc, because...., Insurance Companies for insurance contracts (liability, health etc), because...., Hospitals/clinics for keeping a digital record and making easier diagnosis, because...., Hospitals for the application of some therapies, e.g. physiotherapy, because...., Hospitals for remote surgeries, because...., Law firms for legal advice without human presence, because...., Employers for hiring, because…, Employers for firing, because…, Other businesses like……., because...., No, because...., Another answer....
8. Would you like your country's public services to be equipped with AI systems, in order to process your data, create a profile for you and reply to your applications? What kind of services and why?- Customs offices, for the control of immigrants, because..., Police, to assess the criminal nature of a suspect, because..., Courts, for justice without human presence, because..., Schools/Universities for admitting/rejecting students, Social services for the approval/rejection of a social benefit, Other services.... because..., No, because..., Another answer....
9. Would you like to see public or private services equipped with AI systems, which can collect, process and store your fingerprint or facial, iris and voice recognition features? Which ones and why? - Biometric recognition in police stations (for criminals), because..., Biometric recognition on borders (for immigrants), because..., Cameras (with biometric recognition) on public places (e.g. in public transport stations), because..., Cameras (with biometric recognition) on the policemen's uniform, because..., Biometric recognition during exams for an official certificate (e.g. for driving license) , because..., Biometric recognition at work, when the employee is responsible for a valuable or vulnerable object (e.g. genetic material, secret service files), because..., Other……
10. Do you use the fingerprint or facial or voice recognition feature to lock your phone? Why? - Yes, the fingerprint, Yes, facial recognition, Yes, voice recognition, Another answer, Why?
11. Do you use fitness apps or other health apps on your phone? – Yes, No, Another answer, Why?
12. Do you use any means of protection for your mobile phone and your computer? Which one? - No, Free antivirus, Paid antivirus, Further specialized paid software, I store my files on an external hard disk, Other, Why?
13. Do you use encryption for sharing sensitive files and information? - Yes, for the attachments, Yes, I use an encrypted channel, Both of the above, No, Other, Why?
14. When you visit websites, do you usually read the pop-ups about the cookies policy of the website? Which is your usual choice about cookies?, I accept them all, I reject them all, I specify my choices, I save the default of the website, Other
15. Have you ever been a victim of hacking? - Yes, I know, that I have been, Probably, I don't really know, Probably not, No.

person up to 33 years old and you reside permanently and study (BSc, MSc, PhD etc.) in Germany or Greece. The interview is expected to take about 15 minutes.
Your personal data will not be processed by the researcher. The researcher will not ask you for this information. The researcher will only process the information you are willing to give. Your information will be processed solely for the purpose of conducting this research. Your answers will be analysed anonymously and will only be used to extract the results of the present research. Participation is voluntary and you can withdraw at any time. All responses will be deleted after the researcher has extracted her findings. If you have any queries, you can contact me at Alkisti.Kostopoulou@stud.uni-regensburg.de
Thank you very much for your participation in my research. Your contribution is of great importance to me and I hope that this interview will be of interest to you.
Kind regards,
The researcher.

A. General questions[240]



"This photo by Unknown author licensed CC BY-SA-NC"

1. Would you use an AI chatbot for a financial or legal problem?[241]

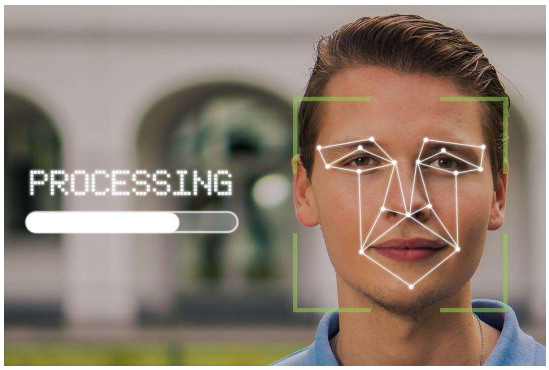
- Just to clarify some questions
- For personalised advice, too
- Other:
- No, I would not use an AI chatbot

2. Would you use apps for medical purposes? What type of app?[242]

- Health apps that measure your heartbeat
- Apps that record your medical data and make diagnoses
- Corona apps that notify you of diagnosed incidents in your area
- Fitness apps that measure your activity and diet
- Other:
- I wouldn't use any of the above apps or any other app of this type

[240] Rationale: we want to give an introduction to the topic and find out, whether the participants avoid the use of AI even if it does not involve the data processing. This will help us to understand in the further questions whether their motives are, for example, that they consider AI systems to be unreliable or unwieldy, regardless of the privacy issues raised.
[241] Rationale: A conversation with a robot: how familiar is that? Do we trust a robot with important issues?
[242] Rationale: Can we see the need to protect their sensitive personal information? What are their criteria? The benefit or the protection of the sensitive data?

B. Biometric Identification



"This photo by Unknown author licensed CC BY-SA-NC"

3. What do you think about the use of remote biometric identification (RBI) systems by private and public services? [243]

4. What do you think about the use of remote biometric identification (RBI) systems by law enforcement authorities?[244]

5. Would you lock your cell phone with fingerprint or facial recognition?[245]

- Yes
- No
- Maybe

6. Would you like to see private companies or public authorities (other than law enforcement) equipped with AI systems that can identify people based on their facial features? What kind of systems? (Note, that a human always intervenes before a decision is made)[246].

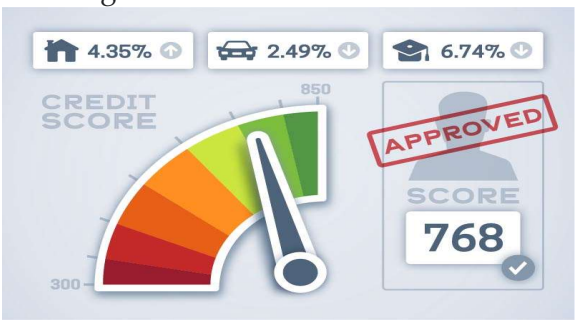
- At driver's license exams to identify the candidate driver (to prevent fraud).
- At the entrance of public or private companies to check if the person entering has an entry permit (e.g. employee, citizen by appointment) (security reasons).
- At the entrance to the workplace, if the employee is responsible for a valuable/valnurable object (e.g., genetic material) (security reasons)
- At the school entrance to verify that the person arriving has a permit (e.g., student, parent, or teacher) (security reasons)
- At university exams to identify the student (to prevent cheating by impersonation).
- Other:
- No, I wouldn't like to see any of these systems in private businesses and public authorities

[243] Rationale: This open-ended question should help us to understand the mindset of the respondent and to better interpret the results of each of the following closed-ended questions.
[244] Rationale: This open-ended question should help us to understand the mindset of the respondent and to better interpret the results of each of the following closed-ended questions.
[245] Rationale: What do we think about biometric identification? Are we aware of the danger?
[246] Rationale: Do we trust private & public services to use RBI AI systems? Can we realize, when the processing is too invasive of our privacy?

7. Would you like to see law enforcement authorities equipped with AI systems that can identify people by their facial features? What kind of systems? (Note that a human always intervenes before a decision is made)[247].

- Police for facial identification of suspects (in police stations).
- Competent authorities for facial identification of immigrants at borders (for security reasons).
- Special cameras with facial recognition could be placed in public places for security reasons
- Police officers could wear special cameras with facial identification on their uniforms
- Police for facial identification of victims (e.g., missing children)
- Other:
- No, I wouldn't want to see any of these systems in law enforcement

C. Profiling



"This photo by Unknown author licensed CC BY-

8.What do you think about the use of intelligent profiling by private and public services? [248]

9. What do you think about the use of intelligent profiling by law enforcement authorities?[249]

10. When you visit websites, do you usually read the pop-up windows about the cookies policy? Which option do you usually choose?[250]

- I accept them all
- I reject them all
- I specify my choice
- I save the website's default settings
- Other:

[247] Rationale: Do we trust law enforcement authorities to use RBI AI systems? Can we realize, when the processing is too invasive of our privacy?

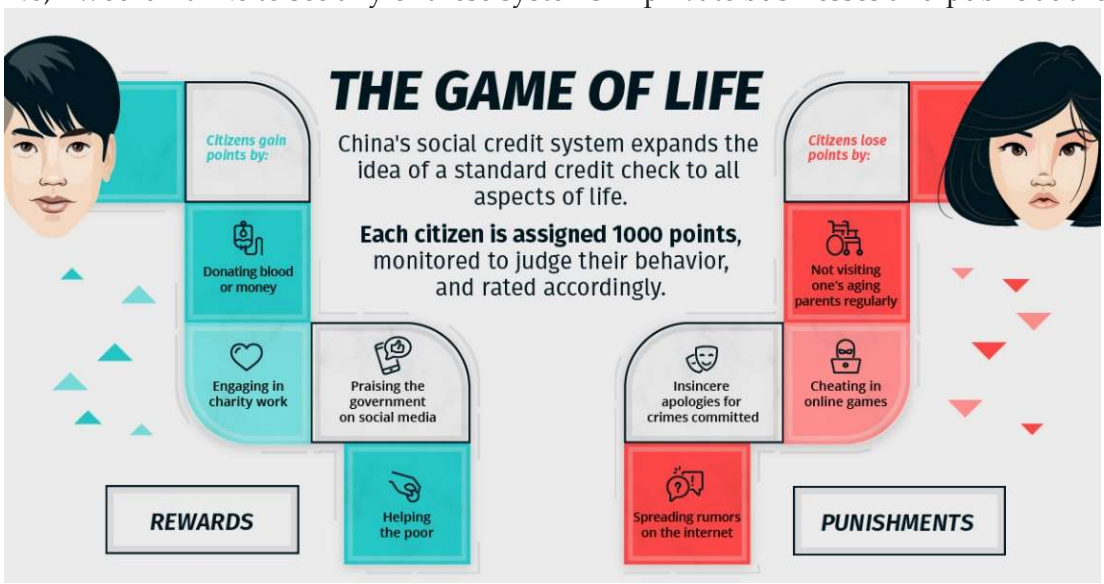
[248] Rationale: This open-ended question should help us to understand the mindset of the respondent and to better interpret the results of each of the following closed-ended questions.

[249] Rationale: This open-ended question should help us to understand the mindset of the respondent and to better interpret the results of each of the following closed-ended questions.

[250] Rationale: How careful are we about our data? Do we agree to the use of our data for marketing or possibly for other further purposes?

11. Would you like to see private companies or public authorities equipped with AI systems that evaluate your eligibility and trustworthiness to access and enjoy essential services and goods? What kind of systems? (Note that a human always intervenes before the final decision)[251]

- Banks for granting a loan/credit card, etc.
- Insurance companies for approving insurance coverage (liability, health insurance, etc.)
- Employers for hiring/firing employees
- Social services for the approval/rejection of a social benefit
- Granting of (state or European) subsidies for small and large companies
- Schools/universities for the admission/rejection of students
- Public authorities for setting up a social credit system (assessing social behaviour & giving rewards or "penalties" to citizens related to social benefits)
- Other:
- No, I wouldn't like to see any of these systems in private businesses and public authorities



"This photo by Unknown author licensed CC BY-SA-NC"

12. Would you like to see law enforcement and judicial authorities equipped with AI systems that evaluate individuals to predict or solve a crime? What type of systems? (Note that a human always intervenes before the final decision)[252]

- Competent authorities assessing the security risk of a particular immigrant's entry to decide whether or not to grant them an entry permit
- Police (e.g., by forensic psychologists) assessing a suspect's personality traits and past criminal behaviour to predict the (re)occurrence of a crime
- Police (e.g., by forensic psychologists) to detect a suspect's emotional state after a crime to identify whether he or she may be the perpetrator of the crime
- Courts "applying the law to a specific set of facts" (before a verdict is reached)
- Other:
- No, I wouldn't want to see any of these systems in law enforcement

[251] Rationale: Do we trust private & public services to use AI systems for profiling? Can we realize, when the processing is too invasive of our privacy?

[252] Rationale: Do we trust law enforcement authorities to use AI systems for profiling? Can we realize, when the processing is too invasive of our privacy?

D. Internet[253]

13. Do you use any protection measures for your cell phone and computer? What kind of?[254]

- Free antivirus
- Paid antivirus software
- Other specialised paid security software
- Other:
- None

14. Do you use encryption to share sensitive files and information?[255]

- Yes
- No
- Sometimes

15. Have you ever been a victim of a hacking attack or digital data breach?[256]

- Yes, I know I have been
- Probably
- I do not really know
- Probably not
- No

E. Personal questions [257]

16. Where are you from or where do you live permanently?

- Germany
- Greece

17. Where do you currently live and study?

- Germany
- Greece

18. How old are you?

- 18-26
- 27-33

19.What is your level of study?

- Undergraduate student (BSc)

[253]This section is about cybercrime. We want to find out if the participants know about the modern forms of cybercrime, but also about the possibilities to protect themselves.

[254] Rationale: How carefully do we handle our personal data? Are we aware of the risk? Are we willing to spend some money on our security?

[255] Rationale: How carefully do we handle our sensitive personal data? Are we aware of the risk?

[256] Rationale: Do we recognize the danger? No one can be sure that they have never been the victim of such an attack. For example, if someone answers that they are sure, they are probably not well informed.

[257] For the rationale of the personal questions, see the methodology in the previous chapter.

- Postgraduate student (MSc)
- Doctoral student (PhD)
- Other:

20. Is your study (or perhaps your work) related to information systems or law?

- Yes
- No

21. Do you feel familiar with privacy law as it relates to the use of AI systems?

- Yes
- Fairly
- Slightly
- No

Thank you for your participation!"

6.3. Results of the research

6.3.1. Closed-ended questions

6.3.1.1. General

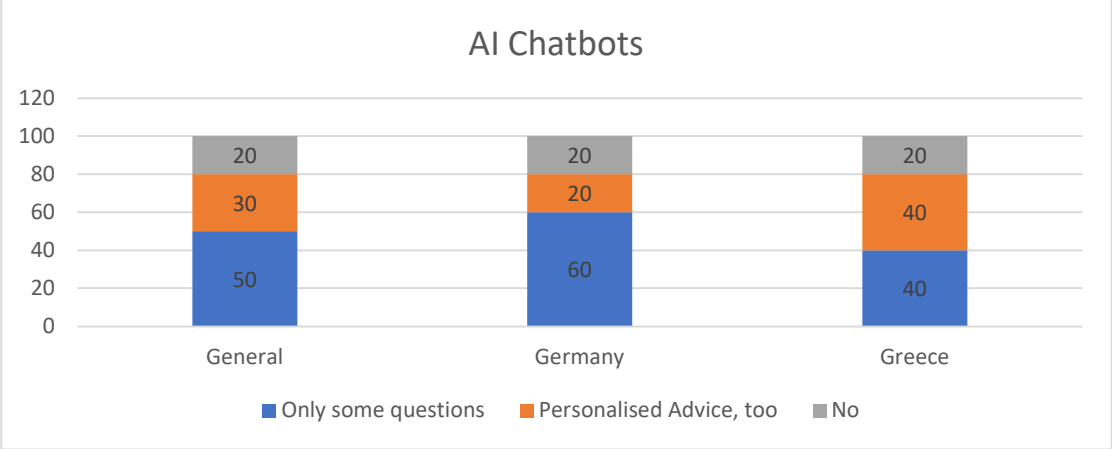
Below we will present and comment on the quantitative results of the questionnaire as they emerge from the closed-ended questions, and we will obtain some initial indications of the participants' perceptions. Under each graph, we will look at the average percentages and then compare the percentages of Germans with those of Greeks. In order to draw conclusions, we will evaluate, where necessary, the known conditions in the two countries. For the reliability of our conclusions, it is possible to evaluate the answers of a whole section or of certain individual questions as well. Second, with the help of open-ended questions, we get a general picture of the respondents' perceptions. At the end, based on the individual conclusions from the interviews, we will draw a general conclusion.

In some charts the sum of percentages is not 100%. This is due to the fact that the corresponding question allowed several answers. In recording them, we tried (as far as possible) to record them with a relative gradation, from the milder processing to the riskier one, taking into account the use of AI. Our criterion for evaluating the results is the legitimacy of the processing, but also the participant's perception of this escalation. In order not to affect the participant, the answers were generally given to him/her in random order and not in the scaling shown in the graph.

6.3.1.2. Artificial intelligent systems in daily life

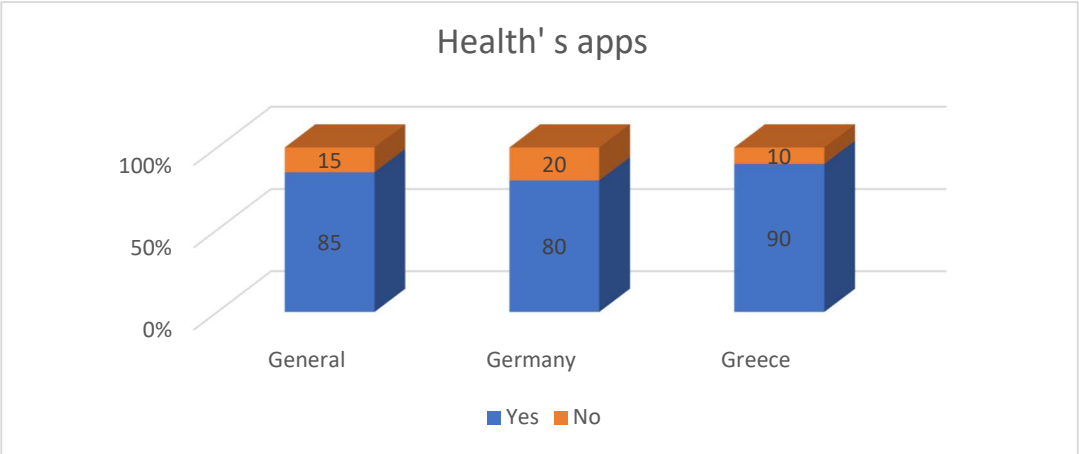
In the first group of questions, we encounter two introductory questions related to the use of advanced applications in their daily lives. These are the use of AI chatbots [258] and some mobile applications, some of which include AI. With these questions, we try to understand for the first time how the participants are used to using AI. This gives us an indication of their confidence in AI practices.

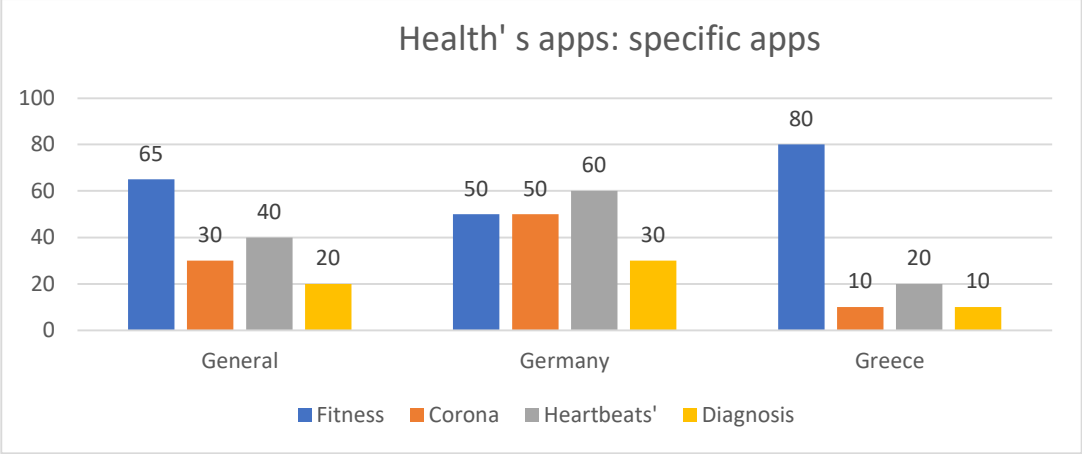
[258] We should emphasize that not all chatbots operate using AI. However, we explicitly refer to them.



Based on the above, we find that most participants are positive about the use of chatbots. However, they prefer not to trust them their personal information, but to ask general questions. Therefore, they seem to prefer privacy over the convenience and immediacy offered by a bot. However, a significant percentage of participants would not use AI bots at all. We can therefore surmise that this percentage of participants are unlikely to find chatbots practical. There is probably a cautious attitude towards the use of AI, at least in the area of this practice. Behind this rejection, however, may be a general reluctance to trust a bot.

Germans and Greeks are equally suspicious of bots in principle. 20% of them do not and would not use them. The Germans seem to be a bit more cautious about privacy than the Greeks. They do trust the usefulness and reliability of chatbots, except for their personal affairs.

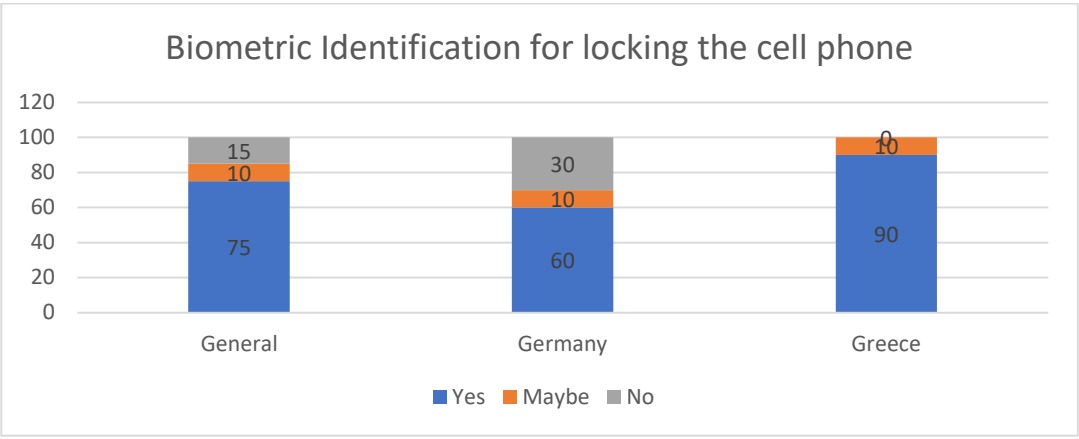




In the graph above, we see clear differences between the Germans and the Greeks. This is probably related to how widespread some applications are in these countries. Above, we have tried to escalate the data processing. However, it is likely that only the last application (to diagnose diseases) uses AI which poses even greater risks to sensitive personal data. Therefore, it is understandable that participants are cautious about this processing. After all, there are significant risks, both for personal data and the trustworthiness of apps.

However, what does not seem to worry users is the possible use of their data for purposes other than the original ones or the interception by hackers. This impact should also be correlated with the latest charts that capture whether users take measures to avoid hacking and data breaches.

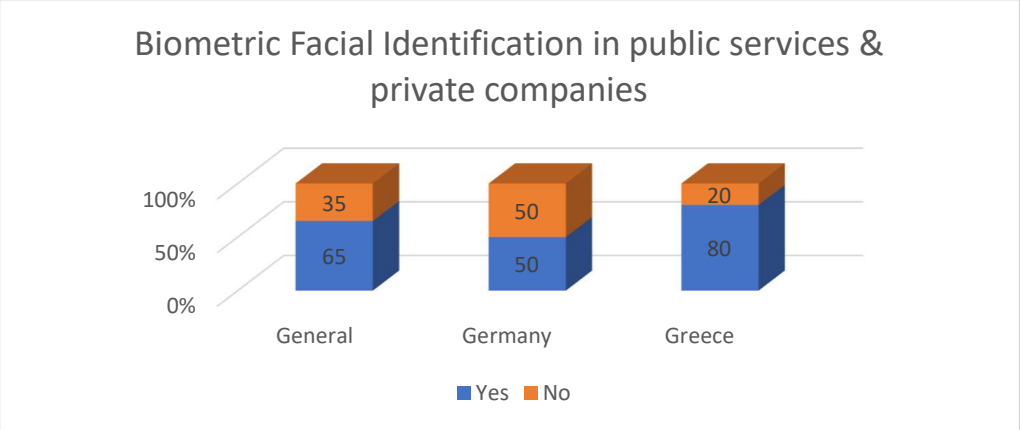
6.3.1.3. Biometric identification



Above we found that a significant majority in Germany and the vast majority in Greece use or are willing to use a biometric feature to lock their cell phone. We developed above the danger

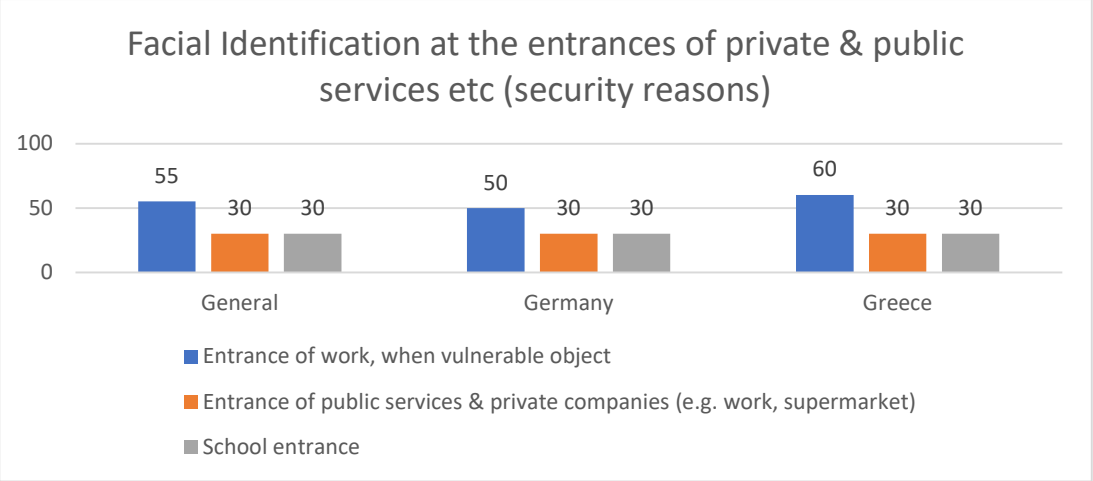
of this action. Intercepting such a feature can have consequences for the rest of our lives. This issue should also be related to the questions in the last section on cybercrime.

Below we will see processing that involve biometric facial recognition in various private and public sector services.



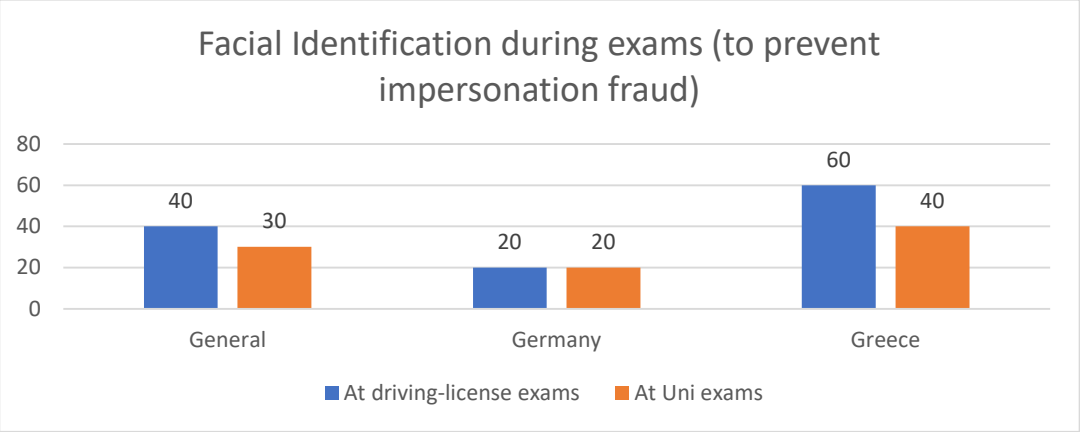
Using the above chart, we find that respondents are on average open to such processing in public and private services. However, there is a significant difference between the samples. The Greeks seem quite willing to dispose of their image, while the Germans are more cautious. The answers here are similar to the answers to the question above about the use of biometric data on cell phones. What could be the cause of such a significant difference between Germans and Greeks?

Analysing the theory and previous case-law, we found that Germany has already conducted several pilot applications of such processing. There is also a great interest in their application, especially in the field of law enforcement. Therefore, Germans are able to know the function and also the consequences of such processing much better than Greeks.



Above we noted that the German and Greek responses are consistent. We note that the participants are skeptical about facial identification at the entrances of public authorities and private companies. However, there is a difference in processing when biometric identification concerns sensitive data, such as the storage of biological material. Case-law and legal literature agree that in such a case biometric identification is permitted. The use of AI systems at the entrance of stores is permissible according to the AI ACT (high risk). However, under the GDPR, it is doubtful whether this processing is compatible with the principle of minimisation. For example, the Swedish Data Protection Authority, as mentioned above, fined a school for biometric recognition of students. The purpose limitation principle and the minimisation requirement have been violated.

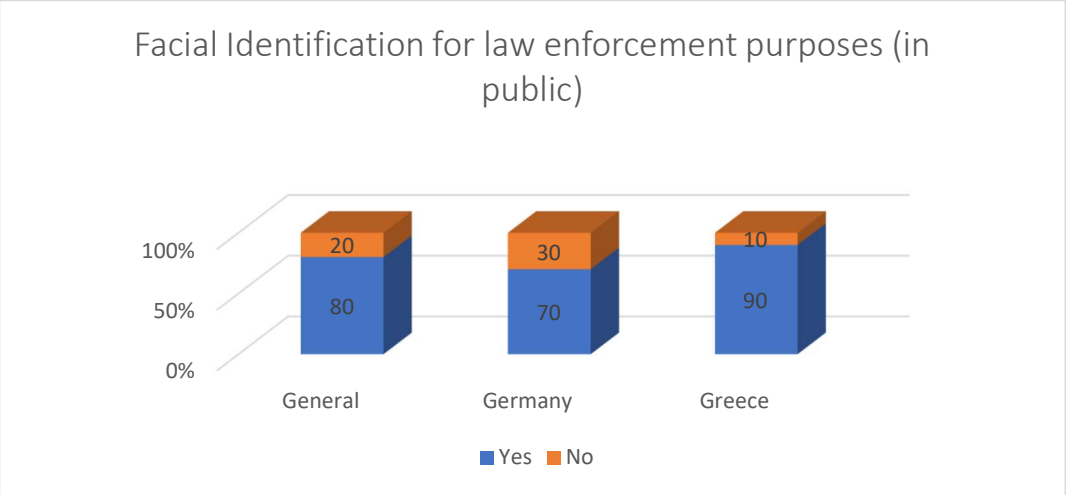
Although the AI ACT does not prohibit such a processing, the GDPR consider this processing as unlawful. Therefore, the above responses of the participants are reasonable and it seems that their criteria and concerns are justified. Perhaps we would expect even lower participation in the latter case (i.e. school entrance).



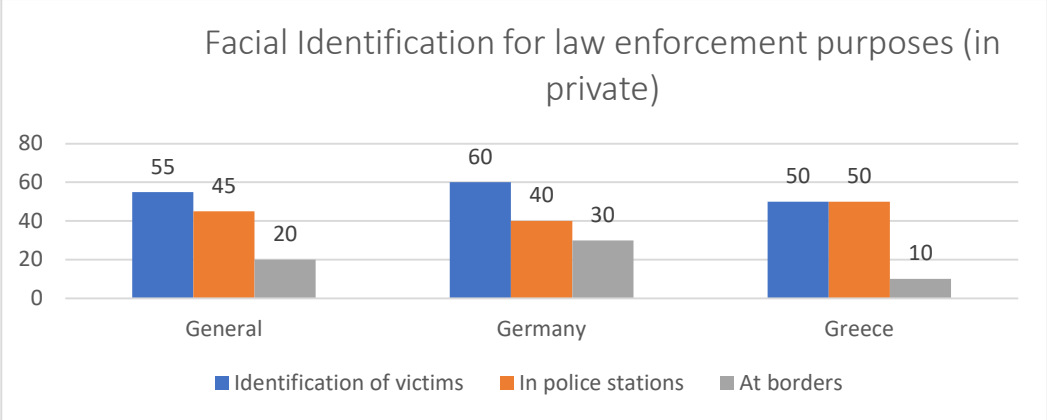
What we have first to emphasize in the above graph is that we have very big differences between the samples at driving-license exams. The Greeks are willing to provide their biometric data. Opinion 1/2021 of the Hellenic Data Protection Authority consider as lawful the las according to which driver's license applicants are identified biometrically during the test. This procedure is familiar to Greek students who already have or intend to obtain a driver's license.

There is not so much variation biometric identification at Uni exams. Though the Germans are more cautious. This processing is allowed according to the AI ACT. However, when applying the GDPR, we note that such processing would pose a problem in terms of the principle of minimisation. There are also more lenient means of identifying a student. The reasons are the same for which the Swedish authority fined the school.

In general, the sampling criteria here are reasonable. The Germans' intense is certainly to protect personal data. While the answers of the Greeks seem to be influenced by the Greek law about facial identification during driving-license exams.

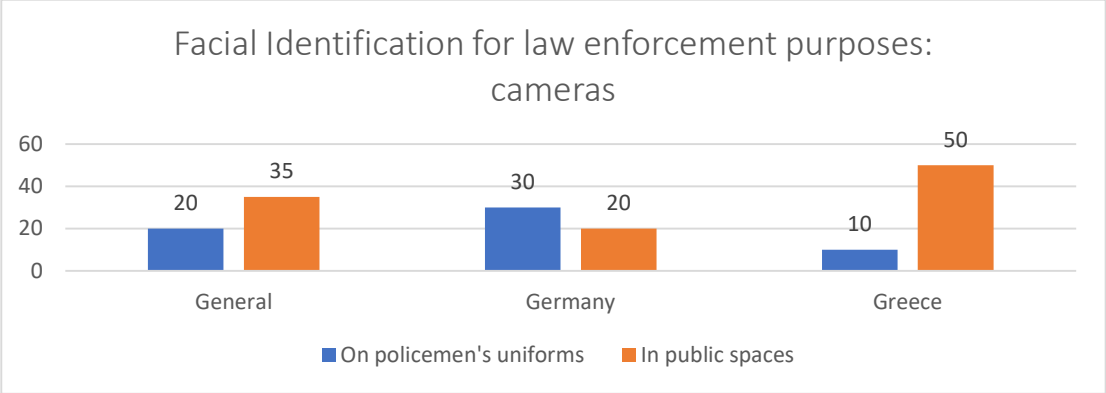


From the graphic above we can conclude that participants are not generally negative about facial identification for law enforcement purposes. In fact, the vast majority of Greeks are positive, as they were for the processing of biometric data described above.



On average, participants seem to accept processing for the purpose of identifying victims or perpetrators, while they are skeptical of biometric identification of migrants at the border.

In particular, regarding victim identification, Germans and Greeks are largely comfortable with their biometric identification. According to the LED and Directive 2018/1862, such processing is even legitimate under certain conditions. As for biometric identification by the police, again according to the LED and Directive 2018/1862, this is also possible in Schengen countries, also under strict conditions. Finally, biometric identification of third country migrants is allowed under the Directive 2018/1860 in very limited cases. So, the criterion of the participants is correct and it aims to protect the data subjects.



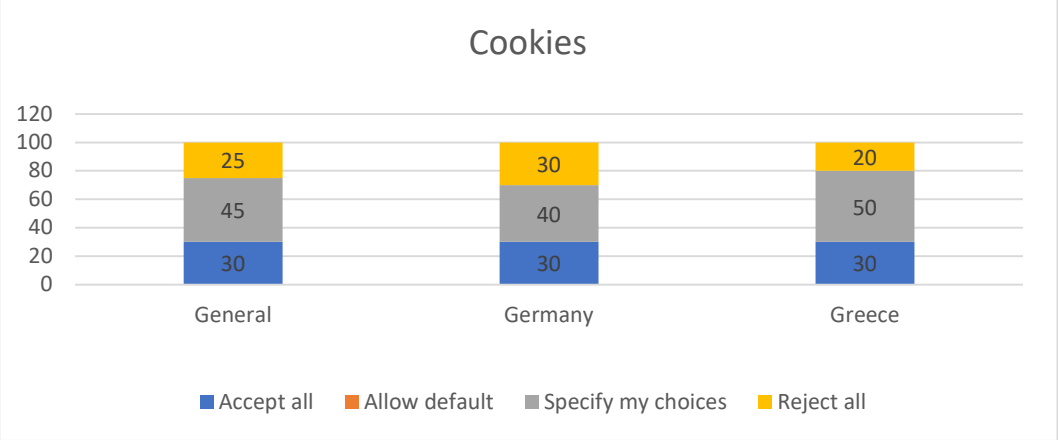
In view of the above, we think that we should first examine the responses of the Germans. We see that there is a gradation that makes sense. It is the minority that relies on these procedures. As for the camera on the uniforms of police officers, it follows from No. 59/2018 decision of the Hellenic Data Protection Authority that it is an unlawful processing. However, in this particular case, no legal basis was found. We would not say that such processing is prohibited in all circumstances.

On the other hand, the Greeks prefer biometric identification cameras in public places though this processing restricts the freedom of the data subject much more than the camera on the uniform of the police officer. It is difficult for us to see here the motivations on the Greek side that influence the average so much. However, the answers of the Germans are reasonable.

With respect to the above passage, we can draw a general conclusion: Germans seem to understand the dangers to personal data. This conclusion derives especially from the fact that their answers follow the gradation of processing. In contrast, the Greeks show unreasonable confidence in biometric identification and apparently ignore the risks involved.

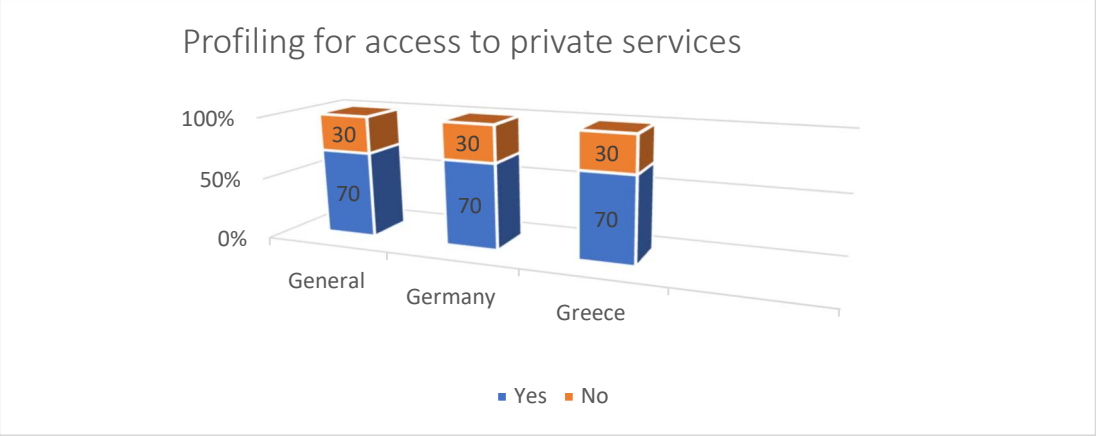
6.3.1.4. Profiling

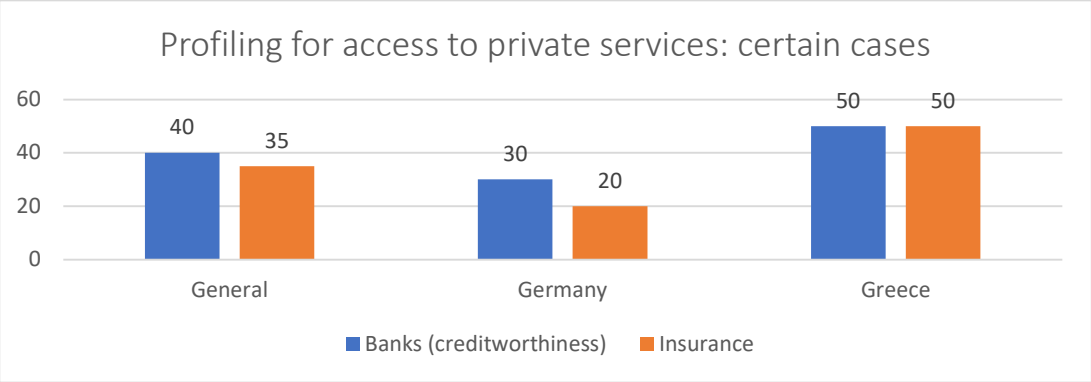
The next category of questions concerns profiling, which we have already discussed above.



Here we ask participants about their habits with respect to our known "cookies". The habits of Germans and Greeks are similar here. This may be because the topic of cookies is widely known. Moreover, there is no right or wrong answer. Someone would not like his/her data to be used for "marketing purposes", while someone else may be facilitated by targeted advertising. However, there is always a risk our data to be used for a purpose other than the initial.

Next, we will examine participants' perceptions of profiling. We informed participants that human intervention take place in any case.





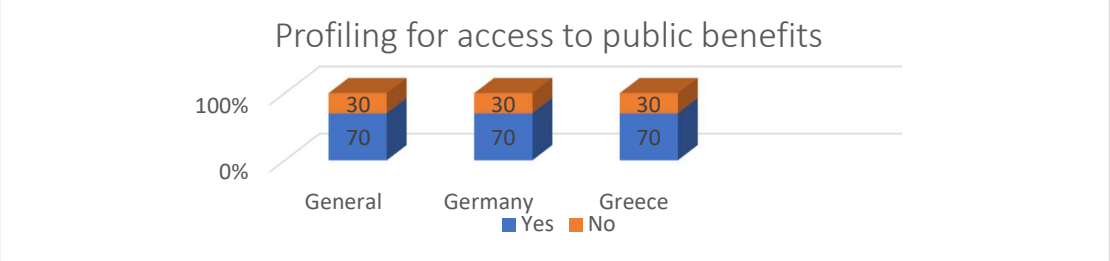
In general, it seems that evaluating creditworthiness by the banks is accepted. Although the processing does not involve special categories of data, it is a processing that poses significant risks to the data subject, as stated above. The use of AI exacerbates the risk. Nevertheless, the participants consider this processing as reliable. We note that responses vary between samples. Greeks seem to trust such systems very much[259].

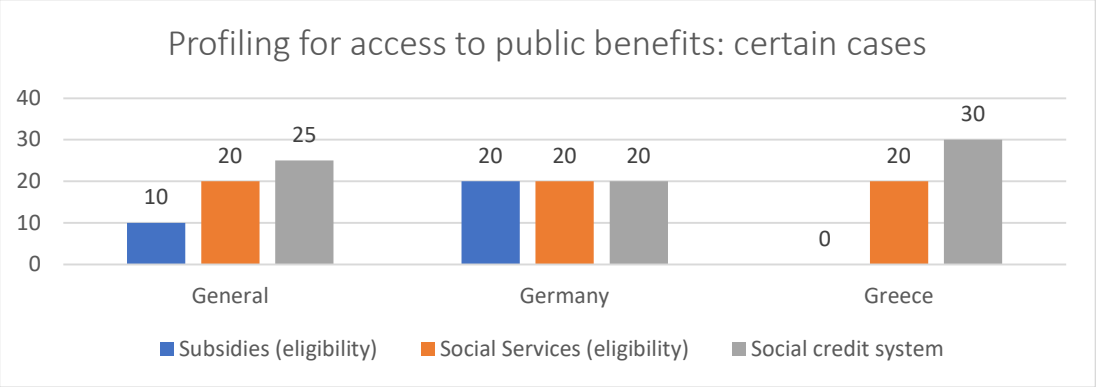
[259] We would like to try to approach this result. It is well known that in the context of the economic crisis that began in Greece 15 years ago, Greeks faced significant problems related to their credit system. On the one hand, many people found themselves in a situation where they could not repay loans that had been generously given by banks in the past, and on the other hand, the banking system itself had a liquidity problem because of this whole situation. Since then, lending in Greece has decreased dramatically because it is very difficult for banks to approve loans. Whereas in the past, credit was approved by the heads of the individual branches, now credit is approved only by the bank's head office, i.e. impersonally. Customers know that their profile will be taken into account when loans are rejected, and many resent this because the lack of credit is not conducive to growth. However, it seems that the age groups we are addressing have a different perspective, because it is somewhat difficult to ignore such a current and well-known situation. So, we could say that Greece's over -indebtedness - which occurred in the past - means that young people today trust absolute numbers more than the human factor. However, this is only our assessment. It remains to be seen whether this will be confirmed when the open-ended questions are evaluated, which may provide further information.

Participants, and especially Greeks, consider insurance companies as reliable, too. The risks are indeed similar for both the above cases concerning the simple data[260]. However, concerning the data of special categories, the processing is prohibited – in principle [261]. In light of the above, the answers have a reasonable escalation.

However, we see an important difference between the samples. Greeks seem to have high confidence in the processing of data by insurance companies, although it was emphasised that the processing may also concern data of special categories[262]**.** In Germany, on the other hand, insurance is more widespread. So, they can easily understand the risks. The results of the Germans in this graph have a logical escalation and we can understand that they are based on the data protection law. On the other hand, this is not happening in the Greeks' answers.

Next, we will look at profiling in the context of our access to public benefits.





[260] There is no mention of this in the AI ACT. However, "the nature of the data", "the scope of the processing" and "the risks for the data subjects" should be taken into account.

[261] Article 22 (4) GDPR.

[262] This difference could be explained by the following. Greeks do not usually take out private insurance - unless it is compulsory, e.g. car insurance or household insurance if a mortgage loan has been granted. Private health insurance is not particularly common (most have only compulsory insurance), nor is liability or professional insurance, etc. (with the exception of doctors, who are insured in case of medical error). Therefore, their experience in this matter is not particularly great, which may affect their judgment.

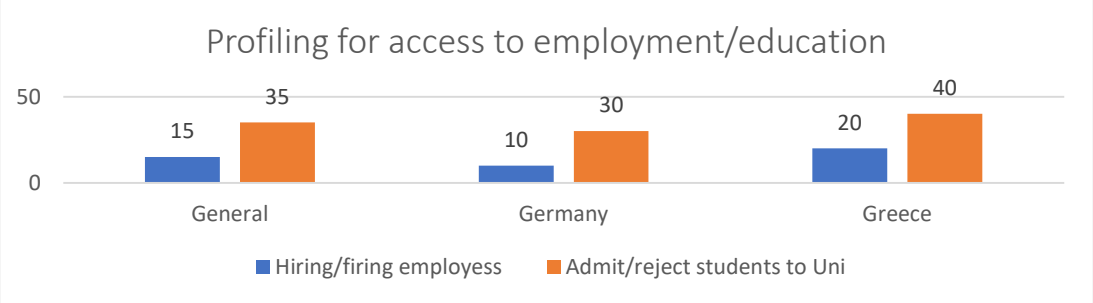
In general, we find that very few people entrust an AI system to evaluate a company in order to subsidize it. The responses differ significantly between Greeks and Germans[263]. This is not primarily though the data protection the reason why Greeks consider as unreliable the profiling for public benefits, because there is not a logic to the escalation between processing.

There seems to be a consensus among the participants concerning social benefits. They seem somewhat suspicious. Such a processing poses risks for personal data. Access to a social benefit, such as a grant, may be vital for the survival of the data subject, and its refusal may have a significant effect on him/her.

Concerning social credit system, participants were informed about how it works, as it is an unknown concept in Europe. It is - in principle - an illegal procedure, as stated above. However, the subjects considered this processing as more reliable that the latter. The answers of the individual samples do not show any significant differences. All of them agree with such a system.

The answers to this subsection, considering their correlations, seem to be far from legal correctness. The result shows that the participants, especially the Greeks, either do not care about personal data and the risks of using AI systems or do not understand them.

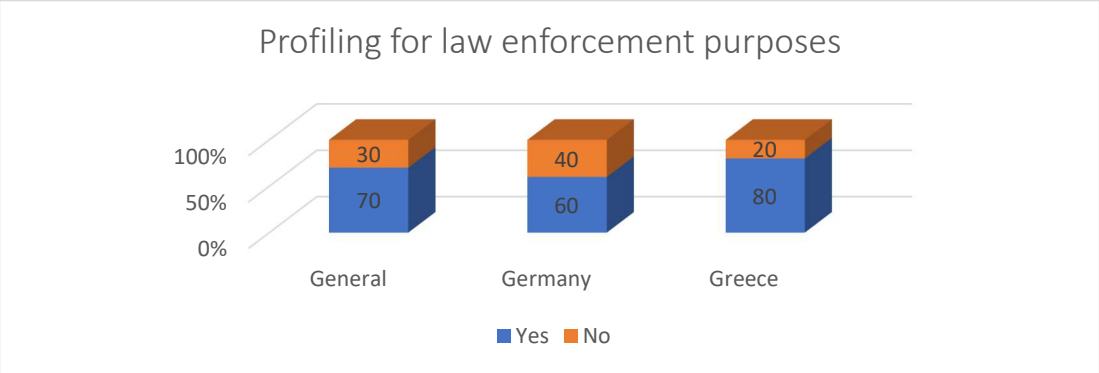
The next two categories are examined together as it is considered that there is some connection between them.



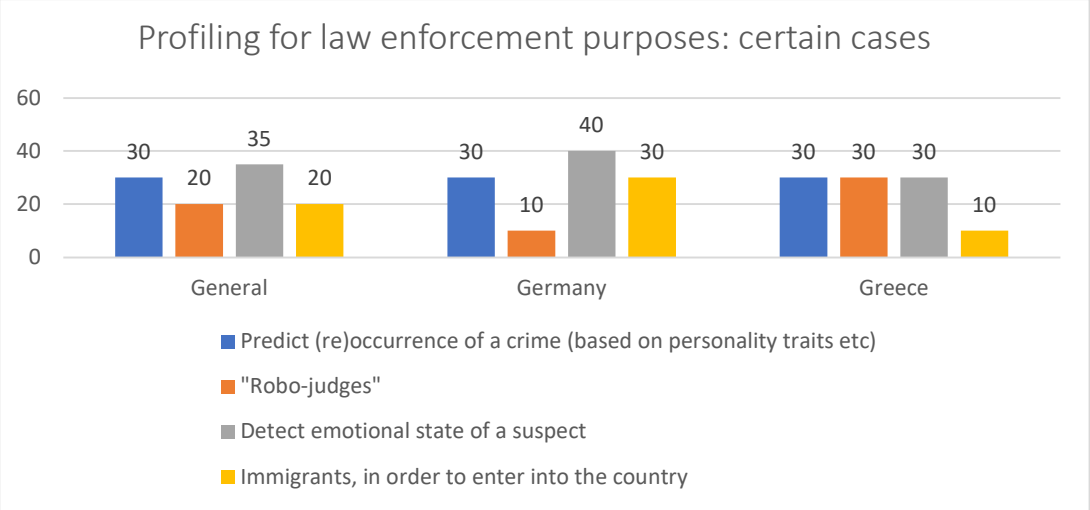
Respondents are quite skeptical about the use of AI in hiring/firing employees, while they trust them in selection/dismissal of students. According to the AI ACT, both are high-risk processing.

[263] The fact that this is a case usually involving a substantial sum of money may have played a role here. Thus, the motivation could be the reliability of the result.

We can suppose here that participants took into account that an AI system could allow a discrimination, such as race.



At the AI ACT, the following processes are grouped under the categories of law enforcement, migration, and administration of justice. However, it is assumed that they are relevant to each other and can be examined together.



All the above are listed as high-risk practices at the AI ACT. However, the above classification has been attempted on our part based on the risks of the processing as defined by the data protection law. The above processing is not directly governed by the GDPR, but by either the LED or other special legislation.

The participants agree that we can predict a crime, if we are based on personality traits and we can avoid a reoccurrence, if we take into account that a person committed a crime before. However, these conclusions ignore the right of the subject to ask for the erasure of certain crimes after many years.

Concerning robo-judges, we have already seen above the dangers of this processing. In the graph we see some differences between the answers of the Germans and the Greeks. We can understand the Germans' skeptic about such a practice.

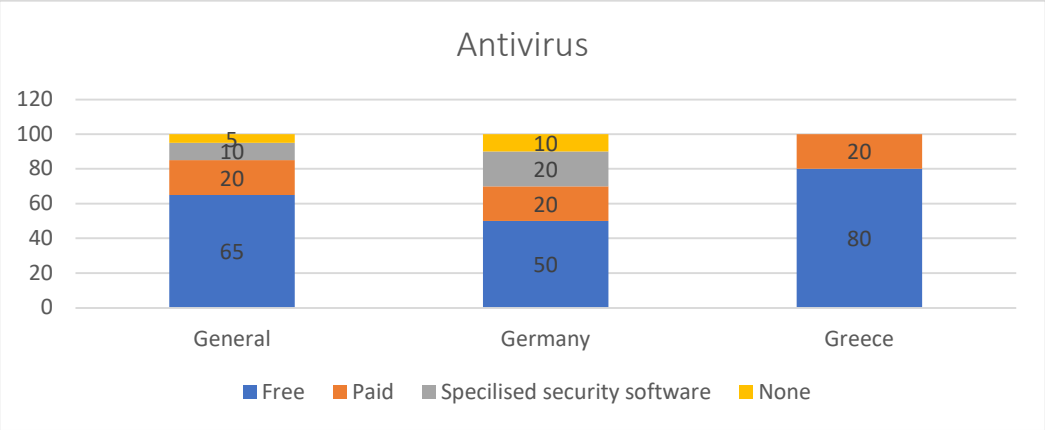
The detection of the emotional state of the offender and its further evaluation is – in principle - an unlawful processing [Art. 10 (2) LED], unless special conditions exist. So, the escalation here is not reasonable.

Concerning profiling of immigrants also poses significant risks. It is in principle unlawful processing, because the data processed are of special categories. Furthermore, there is a difference in the responses of each sample.

Although the goal of the survey is not the respondents to give legally correct answers, it is important to know if they have a perception that approaches privacy issues. As we have pointed out, all the above practices occur significant problems. However, the AI ACT consider them as high-risk and, consequently, lawful practices.

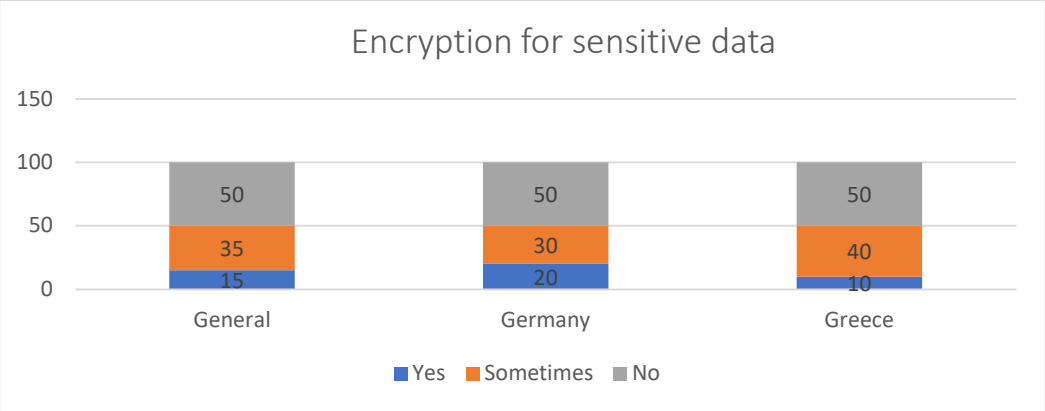
6.3.1.5. Cybercrime

Below we can see some diagrams concerning the habits of the participants that we will associate with cybercrime. In some cases, cybercrime takes place through AI systems.



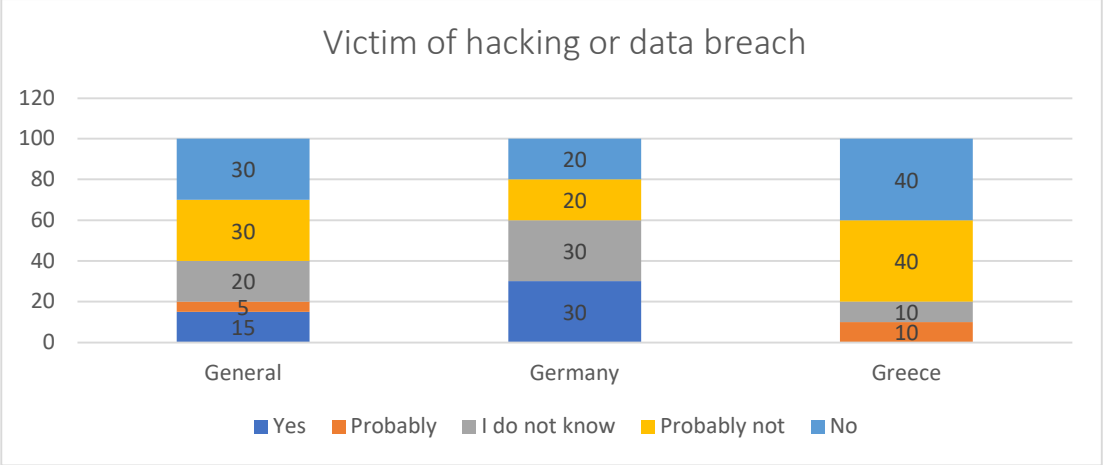
The graph shows that the vast majority of participants are taking measures to protect themselves from hackers, etc. However, the need for a secure antivirus program or other security software has not been identified, especially in Greece. This is despite the fact that, on the one hand, they can offer more benefits and, on the other hand, the software you pay for will not use your

personal data for purposes other than protecting you. On the contrary, there are rumors that this is the case with some companies that offer free antivirus programs. In 2020, there was a big scandal in America about a certain company whose subsidiary sold its users' data on the darkweb and made significant profits from it (187).



Only 50% of respondents use encryption when communicate sensitive data. The Swedish Data Protection Authority fined a healthcare provider who used encrypted emails while the attachments themselves were not encrypted. The authority considered that this was an insufficient measure (188). Individuals are not required to use encryption, of course. However, this shows our perception about privacy. When even channel encryption was insufficient, you realize how dangerous it is to communicate without any encryption.

When choosing a provider, man should consider protection from third parties, but also protection from the provider. That is why many providers state that the features of their services are not only encryption, but also zero access on their part. Sure, if we pay a provider, we are probably more secure. However, there are providers, both for email and instant messaging, that have encryption in the specifications of their services.



In the graph above, we can observe the paradox that Greeks are sure or almost sure that they are not victims of a hacking attack or a digital data breach. This is despite the fact that they usually do not use encryption, nor do they take special care when choosing an antivirus programme. It would be significant if we knew how much money they would be willing to spend on the security of their data, how much a potential intrusion would cost them, but also how likely they think it is. The Germans, on the other hand, seem to be more consistent than in their earlier answers, in which they proved that they care more about protecting their privacy.

6.3.1.6. Interim conclusion

Taking into account all the above graphs based on the closed-ended questions of the questionnaire, it appears that the Greeks' answers are significantly flawed in most of the questions. They know cannot realize neither the risks to their privacy nor how to protect themselves. Of course, in some cases, priority may be given to another criterion, such as the reliability of the system, ease of use, cost, etc. In all these cases, however, a pattern can be discerned: Indifference or ignorance regarding the data protection. This is not happening with Germans, while only in a few or even controversial cases we disagreed with their criterion.

6.3.2. Answers to open-ended questions

6.3.2.1 Biometric identification

The following results are based on the participants' responses to the open-ended questions, after categorising the responses and mainly capturing the majority. In order to fully evaluate and understand each response in this section, for each individual response to an open-ended question from a participant, we considered the response to the corresponding closed-ended question.

- **Regarding biometric recognition by private entities:**

Greeks believe that these practices would be very helpful, if the government controls the data controllers. Otherwise, the information given could be used for further purposes. These thoughts show us, that they can understand the principle of the purpose limitation and of the accountability, even if they do not know their existence.

Germans are cautious about such practices. There is a significant difference with the Greeks here. They are concerned not only about further unlawful processing, but also about the trustworthiness of such systems! The reason may be that there are many failures in the use of these systems until now and the Germans are aware of this.

- **As for biometric recognition by law enforcement:**

Greeks believe that these are useful tools that can support the work of the police. However, concerns are also expressed about privacy and freedom of expression (especially in cases where the cameras are placed in the police officer's uniform or in a publicly accessible place). We have already seen that simple video surveillance also interferes with "the freedom of expression", "the right of assembly", etc. The risks here are greater.

Except for biometric identification of victims, Germans are generally skeptical of such procedures. They are concerned about the reliability of the systems, about their privacy, about the abuse of the power by law enforcement authorities, about the possible constant surveillance, but also about the tracing of the persons concerned. That is a very important comment. We have already seen court decisions mention data protection authorities' s concern about constant surveillance of bystanders who are not associated with criminal activity.

6.3.2.2. Profiling

- **Regarding profiling (by private and public services) for the purpose of eligibility or creditworthiness, etc.:**

Most Greeks seem to consider the objective "judgment" of such a system very important. On the contrary, they consider the subjective judgment of the individual to be an uncontrolled and arbitrary. Moreover, some believe that this step is absolutely necessary and should be taken, even if it imposes some restrictions on the individuals concerned. Therefore, some of them are willing to give up their rights in order to enjoy an incorruptible system. However, there are also many who are concerned about the risks of such systems, but they are still not able to specify the risks.

Germans seem to be more skeptical about profiling in this area. They are concerned about the data protection and seem to be aware of the risks that such processing entails.

- **Regarding the eligibility of officials and students:**

Here the answers differ from those given above. The Greeks are particularly concerned about the possibility of discrimination if an algorithm decides whether to include them. They fear that even human judgment may be influenced by the automated profile. It reminds us of the "no substantial human intervention", that we examined in Article 22 GDPR. They also raise the issue that reliability should be regulated and verified when AI systems are used.

Concerning hiring, Germans are even more cautious than Greeks. They are concerned about discrimination and the errors that can occur when evaluating such a system. They are partially accepting of an AI system in college, while there is a greater fear of discrimination through profiling in the workplace.

- **Regarding profiling for law enforcement purposes:**

The Greeks believe that the practices described are very useful tools for the police. However, they are concerned about the possible discrimination against individuals, especially immigrants.

It is primarily discrimination that worries the Germans in this subsection, and especially regarding its use by judges.

6.3.3. Conclusion of the research

The answers to the open-ended questions are particularly helpful in understanding the perceptions of the participants. From the above, it appears to the Greeks that in many cases their criterion is not only the protection of personal data, but, for example, the arbitrariness of the state with regard to social benefits, which they believe can be limited by an objective evaluation by a system. This is clearly related to the special conditions in a state that make society skeptical of the human factor. But there are also concerns about the data and other fundamental rights' protection. Therefore, transparency and control are necessary for the proper functioning of such systems. We understand the criteria of the Greeks. We would say that there are concerns, but there is no knowledge about the extent of the risks and the ways to protect against them.

Germans are generally more cautious about using AI systems than Greeks. It is derived from their responses, especially the open-ended ones, that they understood the dangers of using such systems very well.

Concerning the above, especially the open-ended questions, there were significant differences between Greeks and Germans. We cannot draw a general conclusion about whether our sample is, on average, aware. It is important to note that each individual, depending on the specific conditions in his/her country, may or may not be familiar with the protection of his/her personal data when processed by AI systems. Germany is a country that has managed to adequately inform its citizens about the topic under discussion, on the one hand, due to its familiarity with technology in general, but also due to its faster compliance with the GDPR. In contrast, there is some concern in Greeks, but certainly no knowledge. Greece is a country that in fact delayed complying with the GDPR and it may be too early to educate its citizens in this way. However, their information and familiarity with the data using AI systems is at least elementary.

6.3.4. Suggestions for a further questionnaire

In a further (especially probabilistic) research, the closed-ended questions could be formulated as follows: Every single answer of this questionnaire could be a self-contained question. The possible answers to this question would not be "yes" or "no", but there could be a gradation, e.g., "I do not agree at all, I do not agree, I am neutral, I agree, I completely agree". This would

provide even more information about how each participant feels about these practices. In addition, not just one but several questions could be asked about each practice. Thus, in addition to "agree" and "disagree", escalation would be possible: "I think it is dangerous, I think it is somewhat dangerous, I do not know, I think it is somewhat safe, I think it is safe".

To limit the size of the questionnaire, for such detailed questions, we could address only a section of the above questionnaire (e.g., "biometric identification" or "profiling" only) rather than all the questions we currently addressed. This would keep the variety of questions at a level that would not discourage participants. However, to cover all the material, two or three similar questionnaires should be created, each containing one section. So, in this way, we could have perhaps two or three questionnaires.

Finally, other open-ended questions could be asked, e.g., each closed-ended question as directly described above, i.e., each individual processing of personal data, could be accompanied by a corresponding open-ended question aimed at better understanding of the closed-ended question.

7. Conclusion

Artificial intelligence is growing up fast. This is the reason why European Union has opted for a detailed regulation of AI-related issues, i.e. the AI ACT. The AI ACT is intended to be a comprehensive regulation for manufacturers, suppliers and users of AI systems. As we have seen, the main purposes of the regulation are (a) users' trust in AI systems and, thus, the development of the European economy, (b) as well as the protection of users, i.e. not only their physical integrity, but also the protection of their fundamental rights, including personal data. So, the AI ACT must be a guide for controllers, processors and data subjects, too. The recent legislation on personal data, i.e. GDPR, LED etc, has already provided for the data protection in relation to AI systems.

However, European citizens are not familiarized with the privacy risks AI systems could pose, nor how to be protected. It would indeed be important for the data subject to be able to consult a text that specifies exactly which practices are prohibited and which are allowed; under what conditions and under what requirements. A text that lists concrete cases can increase the trust of Europeans, so that the market function properly. An exhaustive list of AI practices could be a valuable tool to adequately address AI issues related to the data protection. Thus, the AI ACT seems to be necessary to enhance consumer trust in AI. But what about the legal framework already exists? Is not the GDPR adequate for automated data processing?

From the above comparative analysis between the GDPR/the LED and the AI ACT, we identified that the new Regulation contradicts the existing legal framework. Although the AI ACT itself states in its explanatory memorandum that it aims to respect personal data, this attempt is not successful. If the European Union applies the AI ACT in its current form, parallel and contradictory provisions will exist in the legal world and it may result in legal uncertainty. For example, social scoring is allowed according to the AI ACT, although it should be prohibited according to the existing legal framework. Furthermore, post remote biometric identification in publicly accessible spaces for law enforcement purposes is allowed according to the AI ACT, while it is considered as a prohibited processing according to the LED. We have also identified further contradictions in the above analysis.

Several Member States pointed out such problems in order to be addressed. The German Federal Council ("Bundesrat") has conducted an exhaustive analysis about the relevant contradictions.

It would not be though enough to address the specific problems that have been pointed out. Although an exhaustive list of AI practices would be useful, it would always pose some risks. It is extremely difficult for all the contradictions to be addressed, as new practices will regularly be added to the Annex of the AI ACT. Amending a regulation is not an easy nor a quick process. Would it be ever possible to harmonise the AI ACT with the GDPR and the LED? Currently, the AI ACT has failed to comply with the GDPR etc. So, which is the value of the AI ACT related to data protection?

The AI ACT sets out the requirements that must be met for AI practices to be lawful. Namely, the AI ACT sets out technical measures that must be met for data processing to be lawful, too. Provided that the GDPR and the LED are technologically neutral, this legal framework does not set up specific measures, in order the controller to be complied with the GDPR etc. So, as long as the controller implement appropriate technical and organisational measures, he complies with the GDPR. Further, the detailed measures help the controller to be able to demonstrate that he complies with the GDPR. So, the requirements that set up the AI ACT contribute to the accountability of the controller. Accountability, i.e., demonstrating that the controller complies with the GDPR, is one of the fundamental principles of the Article 5 GDPR. Therefore, compliance with all the requirements listed in the AI ACT supports the principle of accountability and thus the protection of personal data. Whether, however, these measures are sufficient, should be evaluated by scientific experts, e.g. computer engineers. In this way, the AI ACT can contribute to the data protection. So, the AI ACT can support data protection law, and in particular the accountability principle, by providing for appropriate technical and organisational measures.

The current data protection framework, however, is quite sufficient, as it can fully meet the requirements of new technological developments, even though it is technologically neutral. It is reasonable for the law to remain technologically neutral, because this neutrality means adaptability. For example, while Directive 95/46 may was outdated provided that it could not cover the technological developments of the time, this does not mean that the law needs to be updated with every single technological development or AI practice, at least not at the level of an EU regulation. We therefore understand the EU's intention, on the one hand, to provide clarity in legislation with a detailed and technologically updated regulation and, on the other

hand, to strengthen citizens' trust in AI, but, as our analysis above has already shown, this cannot ultimately be achieved with the AI ACT, at least not in the form in which the AI ACT is currently formulated. We must though satisfy the need for citizens to become familiar with AI systems and personal data, as well as to address the legal issue.

8. Suggestions

As mentioned above, an exhaustive list with AI practices seems useful. It is proposed that these listed and exhaustively cited practices be summarized in a text coordinated and published by the EDPB[264]. Similar work was done by the Article 29WP, which was effectively replaced by the EDPB, after the entry into force of the GDPR. For example, the Working Party has issued a detailed list of criteria according to which a DPIA must be carried out. In addition, the EDPB explicitly refers that: "*Our main tasks and duties are: providing general guidance (including guidelines, recommendations and best practices) to clarify the law and to promote a common understanding or EU data protection laws [...]*" (189). It would indeed be important to carry out this work in cooperation with the European Council of Artificial Intelligence, which establishment and tasks are provided for in Art. 58 AI ACT and in which the EDPS also participates[265].

In this way, we can support the citizens' need for information and enhance their trust in AI. Public information also could be supported by appropriate information campaigns, while trust can be strengthened through the use of codes of conduct. It is important to encourage controllers to establish codes of conduct, as provided for in both the GDPR and the AI ACT.

Furthermore, as pointed out in Chapter 2 of this thesis, there is a major problem with the definition of AI systems. There is no universally accepted scientific definition, and this creates problems. Also, as mentioned above, the German Federal Council has judged the definition adopted by the EU to be quite broad, and there are specific recommendations from the Federal Council for appropriate corrections. The problem lies primarily in the following. Almost every application of internet technology uses even simple algorithms. In this sense, the definition of the AI ACT covers almost all the applications. In contrast, the Federal Council has indicated that only self-learning systems should be considered as AI systems. This is a question of utmost importance. If the AI ACT contains a definition that is not accepted by the scientific community or is simply wrong, the consequence is that the GDPR will not be applied correctly. For example, under the above conditions, it is possible to consider systems as high-risk that in real do not

[264] "*The EDPB is established by the General Data Protection Regulation (GDPR) [and] [...] is composed of representatives of the EU national data protection authorities (national supervisory authorities) and the European Data Protection Supervisor (EDPS)*" (189).

[265] As mentioned above, the European Data Protection Supervisor also participated in the EDPB.

pose significant risks to users. This failure also contributes to citizens not knowing which systems pose a risk to them and which do not. At the same time, it discourages those responsible for monitoring, such as manufacturers and retailers, from investing in such systems when the requirements are disproportionate to the benefits. As a result, the market is impaired and the goals of the AI ACT are not furthered. So, if the Federal Council is correct, the concept of AI systems should be defined properly.

Considering the above and the fact that the current legal framework for the protection of personal data is adequate and must remain technologically neutral, the AI ACT can contribute to the data protection in the following way: firstly, scientists should correctly formulated the definition of AI systems and, secondly, they should verify, whether the requirements, obligations and, in general, the technical and organisational measures mentioned in the AI ACT are sufficient for the proper functioning of AI systems and our security. If this is the case, the AI ACT could be considered important for the protection of our personal data, as the technical and organisational measures are crucial for compliance with the accountability principle. Only if the technical and organisational measures are clear and complete can data controllers actually comply with the law and demonstrate this. Information campaigns, codes of conduct and a list of prohibited and permitted practices by the EDPB and the European Artificial Intelligence Board can help to promote public trust in AI. The list on behalf of these councils will have two advantages. First, it can be more easily amended, and second, it will be produced by bodies with the most appropriate scientific staff and experience.

But finally, we should not forget that the law follows the needs of society. If the use of AI systems is considered essential to people's quality of life, then more technical and organisational measures should be taken to enable more AI practices. The development and deployment of AI systems should be accompanied by a corresponding development of technical protection measures. Therefore, it is science and technology that can support and promote the use of AI in our daily lives.

References

1. **EUR-LEX. Access to European Union law.** ***https://eur-lex.europa.eu/.*** **[Online] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.**

2. https://eur-lex.europa.eu/. ***EUR-lex. Access to European Union Law.*** **[Online] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF.**

3. EUR-lex. Access to European Union Law. ***https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.*** **[Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.**

4. EUR-lex. Access to European Union law. ***https://eur-lex.europa.eu/legal-content.*** **[Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN.**

5. Anthony , H. D. The Mechanical Technology of Greek and Roman Antiquity by A. G. Drachmann. ***The British Journal for the History of Science.*** **Cambridge University Press , 2009, Vol. 1, 3.**

6. Καζαντζάκης, N. and Κακριδής, I. ***Μετάφραση Ομήρου Ιλιάδας.*** **s.l. : Ίδρυμα Μανώλη Τριανταφυλλίδη, 1955.**

7. Nillson, Nils. ***The quest for Artificial Intelligence.*** **Stanford University : Cambridge University Press, 2009.**

8. Wikipedia. The Free Encyclopedia. ***wikipedia.*** **[Online] https://en.wikipedia.org/wiki/Talos.**

9. Κυδωνάκη, Μ. Αθηνοδρόμιο. ***athinodromio.*** **[Online] 2017. https://www.athinodromio.gr/%ce%b7-%ce%b9%cf%83%cf%84%ce%bf%cf%81%ce%af%ce%b1-%cf%84%cf%89%ce%bd-%cf%81%ce%bf%ce%bc%cf%80%cf%8c%cf%84-%ce%b7-%ce%b5%ce%be%ce%ad%ce%bb%ce%b9%ce%be%ce%ae-%cf%84%ce%bf%cf%85%cf%82/.**

10. ***1945: Η ψηφιακή επανάσταση.*** **Μαγκλίνης, Ηλ. Αθήνα : Καθημερινή. Available at https://www.kathimerini.gr/world/781582/1945-i-psifiaki-epanastasi/, 2014, Καθημερινή.**

11. Καζαντζής, Χρ. ΓΥΜΝΑΣΙΟ ΝΕΑΣ ΚΑΛΛΙΣΤΗΣ. ***gym-n-kallist.rod.sch.*** **[Online] 2012. http://gym-n-kallist.rod.sch.gr/programs/2012-13/agogis_1/index.htm.**

12. Dyson, G. ***Turing's Cathedral. The Origins of the Digital Universe.*** **s.l. : Pantheon Books, 2012.**

13. Wikipedia The Free Encyclopedia. ***wikipedia.org.*** **[Online] https://en.wikipedia.org/wiki/Church%E2%80%93Turing_thesis.**

14. Wikipedia. Wikipedia. The Free Encyclopedia. ***wikipedia.*** **[Online] https://en.wikipedia.org/wiki/Alan_Turing.**

15. Copeland, B. J. Standford Encyclopedia of Philosophy. ***plato.stanford.edu.*** **[Online] 2017. https://plato.stanford.edu/entries/church-turing/.**

16. SanSimeraComputers. Σας σήμερα στους υπολογιστές. ***San Simera Computers. Wordpress.*** **[Online] 11 05, 2011. https://sansimeracomputers.wordpress.com/2013/11/05/ai/.**

17. Akst, J. TheScientist.Exploring life, inspiring innovation. ***the-scientist.*** **[Online] 2019. https://www.the-scientist.com/foundations/machine--learning--1951-65792.**

18. Βλαχάβας κλπ, Ι. . ***Τεχνητή Νοημοσύνη.*** **s.l. : Εκδόσεις Πανεπιστημίου Μακεδονίας, 2020.**

19. Anyoha, R. Harvard University. The Graduate School of Arts and Sciences. ***sitn.hms.harvard.edu.*** **[Online] 2017. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.**

20. History Of AI. ***historyof.ai.*** **[Online] 2019. https://historyof.ai/snarc/.**

21. IBM Cloud Education. IBM. ***ibm.*** **[Online] 07 15, 2020. https://www.ibm.com/cloud/learn/machine-learning.**

22. University of Bristol. ***https://www.bristol.ac.uk.*** **[Online] 2008. https://www.bristol.ac.uk/news/2008/212017945378.html.**

23. Britannica. ***https://www.britannica.com.*** **[Online] https://www.britannica.com/biography/John-McCarthy.**

24. Butz, M. Towards Strong AI. ***Künstliche Intelligenz*** **. SpringerLink. Available at https://link.springer.com/article/10.1007/s13218-021-00705-x, 2021.**

25. Ελπίδης, Χρ. techgear. ***techgear.gr.*** **[Online] 11 9, 2019. https://www.techgear.gr/techniti-noimosyni-ithika-zitimata-provlimatismoi-kai-kindynoi-25786.**

26. Russell, S and Norvig, P. ***Artificial Intelligence: A Modern Approach".*** **s.l. : Prentice Hall, 3rd edition, 2009.**

27. Wikipedia. The Free Encyclopedia. ***Wikipedia.*** **[Online] https://en.wikipedia.org/wiki/Aristotle.**

28. Wikipedia. Wikipedia. The Free Encyclopedia. ***Wikipedia.*** **[Online] https://en.wikipedia.org/wiki/Immanuel_Kant.**

29. Knachel, Matthew. Deductive Logic II: Sentential Logic. ***Fundamental Methods of Logic.*** **Milwaukee : University of Wiscosin Milwaukee. Available at https://dc.uwm.edu/phil_facbooks/1/, 2017.**

30. Αριστοτέλης. ***Ἀναλυτικά πρότερα. Ἅπαντα Ἀριστοτέλους.*** **s.l. : National Technical University of Athens (ntua.gr), pp. Βιβλίο 1ο, Κεφάλαιο 1ο, παρ. 24b, στίχοι 18-22.**

31. Τσιότσου, Ό. Σπουδαστήριο Θετικών και Ανθρωπιστικών Σπουδών, Γ. Κυριακίδης - Ι. Ανδρεάδης. ***spoudastirio.edu.*** **[Online] https://www.spoudastirio.edu.gr/sites/default/files/pdfs/1_aristotle.pdf.**

32. Smith, R. Aristotle's Logic. ***Stanford Encyclopedia of Philosophy.*** **Available at https://plato.stanford.edu/entries/aristotle-logic/, 2018.**

33. ***Πολιτικές έννοιες: Μια σύντομη ανάλυση του ορθολογισμού.*** **Κωνσταντίνου, K. 2019, Politically Incorrect incorrect.gr.**

34. Wikipedia The Free Encyclopedia. ***wikipedia.org.*** **[Online] https://en.wikipedia.org/wiki/Rationalism.**

35. Bynum, William. ***Short History of Science.*** **Athens : Patakis, 2014.**

36. Μηχανή του Χρόνου. ***https://www.mixanitouxronou.gr.*** **[Online] https://www.mixanitouxronou.gr/skeftome-ara-iparcho-i-diatiposi-tou-kartesiou-pou-xechorise-tin-ili-apo-to-pnevma-o-kataskopos-pou-othise-tin-epistimi-ke-kathierose-tous-orous-chpszavg-stin-algevra/.**

37. Αντικλείδι. ***antikleidi.*** **[Online] 05 23, 2020. https://antikleidi.com/2020/05/23/orthologismos/.**

38. Wikipedia. The Free Encyclopedia. ***wikipedia.*** **[Online] https://en.wikipedia.org/wiki/Empiricism.**

39. Wikipedia. The Free Encyclopedia. ***wikipedia.*** **[Online] https://en.wikipedia.org/wiki/George_Boole.**

40. Tutorialspoint. tutorialspoint. Simply Easy Learning. ***tutorialspoint.*** **[Online] https://www.tutorialspoint.com/computer_logical_organization/boolean_algebra.htm#:~:text=Boolean%20Algebra%20is%20used%20to%20analyze%20and%20simplify,algebra%20was%20invented%20by%20George%20Boole%20in%201854..**

41. Σαν Σήμερα. ***sansimera.*** **[Online] https://www.sansimera.gr/biographies/1499.**

42. Wikipedia. Gottlob Frege. ***wikipedia.org.***

43. Sluga, H. Frege and the Rise of Analytic Philosophy". ***in Inquiry.*** **1975, p. vol. 18.**

44. Dobrev, D. Comparison between the two definitions of AI. ***Institute of Mathematics and Informatics, Bulgarian Academy of Sciences.*** **2013.**

45. Wikipedia. Wikipedia. The Free Encyclopedia. ***wikipedia.*** **[Online] https://en.wikipedia.org/wiki/Turing_test.**

46. TURING, A. M. I.—COMPUTING MACHINERY AND INTELLIGENCE. *Mind.* **Oxford Academic, https://doi.org/10.1093/mind/LIX.236.433, 1950, Vol. Volume LIX, Issue 236.**

47. Adam, A. *What can the history of AI learn from the history of science?* **London : Springer-Verlag, 1990.**

48. McLeod, S. SimplyPsychology. *simplypsychology.org.* **[Online] 2020. https://www.simplypsychology.org/behaviorism.html.**

49. Whalen, Th. A Computational Behaviorist Takes Turing's Test. *Parsing the Turing Test.* **s.l. : 2009 Springer Science+Business Media B.V. Available at https://link.springer.com/chapter/10.1007/978-1-4020-6710-5_21?noAccess=true, 2007.**

50. Thagard, P. Stanford Encyclopedia of Philosophy. *https://plato.stanford.edu.* **[Online] 2018. https://plato.stanford.edu/entries/cognitive-science/.**

51. ΕΚΠΑ. Γνωσιακή επιστήμη. *http://cogsci.phs.uoa.gr/gnwsiaki-epistimh.html.*

52. Wikipedia. Wikipedia. The Free Encyclopedia. *https://en.wikipedia.org.* **[Online] https://en.wikipedia.org/wiki/Machine_learning.**

53. Mitchell, T. *Machine Learning.* **New York : McGraw Hill, 1997.**

54. Ala-Pietilä etc, P. *Independent high-level expert group on artificial intelligence set up by the European commission a definition of ai: main capabilities and disciplines definition developed for the purpose of the AI HLEG'S deliverables.* **Brussels : European Commission. Available at https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_policy_and_investment_recommendations.pdf, 2019.**

55. Wikipedia. Wikipedia. The Free Encyclopedia. *https://en.wikipedia.org.* **[Online] https://en.wikipedia.org/wiki/Artificial_neural_network.**

56. Γιακουμάκης, Δ. LiBertyPress. *https://libertypress.gr/ai-psychology/.* **[Online] 2018. https://www.bing.com/search?q=%CE%97+%CE%B1%CE%BB%CE%BB%CE%B7**

%CE%BB%CE%B5%CF%80%CE%AF%CE%B4%CF%81%CE%B1%CF%83%CE%B7+%CF%84%CE%B7%CF%82+%CF%84%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE%CF%82+%CE%BD%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%BD%CE%B7%CF%82+%CF%83%CF%.

57. Datenschutz Agentur. Daten. Schutz. Agenten. *Datenschutz Agentur.* **[Online] 2020. https://datenschutz-agentur.de/blog/hambacher-erklaerung-zur-kuenstlichen-intelligenz/.**

58. Bundesrat. *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union.* **2021. 488/21.**

59. Wikipedia. Wikipedia. The Free Encyclopedia. *www.wikipedia.org.* **[Online] https://en.wikipedia.org/wiki/Laws_of_robotics#:~:text=%20The%20Three%20Laws%20are%3A%20%201%20A,the%20First%20or%20Second%20Laws.%20%5B1%5D%20More%20.**

60. Tietz, T. ShiHi Blog. Daily blog on science, tech & art in history. *http://scihi.org.* **[Online] 2018. http://scihi.org/isaac-asimov-laws-robotics/.**

61. Rodrigues, R. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology.* **Available at https://www.sciencedirect.com/science/article/pii/S2666659620300056, 2020, Vol. 4.**

62. CartlandLaw. Cartland Law. *https://cartlandlaw.com.* **[Online] https://cartlandlaw.com/sophia-robot-citizenship-and-ai-legal/.**

63. *ROBOSTOP Facebook shuts off AI experiment after two robots begin speaking in their OWN language only they can understand.* **Beal, J. and Jehring, A. s.l. : The Sun. Available at https://www.thesun.co.uk/tech/4141624/facebook-robots-speak-in-their-own-language/, 2017.**

64. Ben-Israel etc., Is. *Towards Regulation of AI Systems, Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the*

Council of Europe's standards on human rights, democracy and the rule of law. **s.l. : Compiliation of contributions prepared by CAHAI Secretaria, 2020.**

65. Specktor, Brandon. Live Science. *https://www.livescience.com.* **[Online] 06 13, 2022. https://www.livescience.com/google-sentient-ai-lamda-lemoine.**

66. doctv. *www.doctv.gr.* **[Online] 06 15, 2022. https://www.doctv.gr/page.aspx?itemid=spg16846&fbclid=IwAR3aCzyYUXpt-Kd4D0Y-aF4P0POW1OrejdmjWHYahISvFNTzNbdJVi1gTs4.**

67. Κουκιάδης, Δ. Οι κανονιστικές προκλήσεις της τεχνητής νοημοσύνης και το ζήτημα της αναγνώρισης της προσωπικότητας. *ΔΙΜΕΕ.* **Νομική Βιβλιοθήκη. Available at www.qualex.gr, 1 2020, pp. 17- 23.**

68. Panel for the Future of Science and Technology. European Parliamentary Reaserch Service. *Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence.* **s.l. : Scientific Foresight Unit. Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf, 2021.**

69. EuropeanParliament. *Report with Recommendations to the Commission on Civil Law Rules on Robotics.* **Brussels : europarl.europa.eu, 2017.**

70. EuropeanCommission. *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the impact of artificial intelligence, the Internet of Things and robotics on security and responsibility.* **Brussels : European Commission. Available at https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en, 2020.**

71. Ben-Israel, Isaac etc. *Towards Regulation of AI Systems, Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law, Compilation* **. s.l. : Compilation of contributions prepared by the CAHAI Secretariat, 2020.**

72. Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. ***Ethical Guidelines for Trustworthy Artificial Intelligence.*** **Brussels : European Commission. Available at https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf, 2018.**

73. Ala-Pietilä etc, P. ***Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, Policy and Investment Recommendations for trustworthy AI.*** **Brussels : European Commission. Available at https://www.europarl.europa.eu/cmsdata/196378/AI%20HLEG_Policy%20and%20Investment%20Recommendations.pdf, 2019.**

74. Masters, Robin Allen QC and Dee. ***REGULATING FOR AN EQUAL AI: A NEW ROLE FOR EQUALITY BODIES, Meeting the new challenges to equality and non-discrimination from increased digitisation and the use of Artificial Intelligence.*** **Brussels : European Network of Equality Bodies. Available at https://equineteurope.org/wp-content/uploads/2020/06/ai_report_digital.pdf, 2020.**

75. CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (CONVENTION 108). ***Profiling and Convention 108+: Suggestions for an update of Recommendation 2010(13) on profiling.*** **s.l. : Directorate General of Human Rights and Rule of Law. Available at https://rm.coe.int/t-pd-2019-07rev-eng-report-profiling/168098d8aa, 2020.**

76. MichaelDukakisInstitute. ***Artificial Intelligence and Democratic Values.*** **s.l. : Center for AI & Difital Policy, Michael Dukakis Institute for Leadership & Innovation, caidp.dukakis.org/aisci-2020, 2020. p. 326.**

77. etc, E Wierda. Privacy of patient data in quality-of-care registries in cardiology and cardiothoracic surgery: the impact of the new general data protection regulation EU-law. ***European Heart Journal - Quality of Care and Clinical Outcomes,.*** **Oxford Academic. Available at https://doi.org/10.1093/ehjqcco/qcy034, 2018, Vol. 4, 4.**

78. Supervisor, European Data Protection. *Opinion on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a* **. Brussels : Available at https://www.statewatch.org/media/documents/news/2013/jul/eu-edps-smart-borders-opinion.pdf, 2013.**

79. Βόρρας, Α. and Μήτρου, Λ. Τεχνητή Νοημοσύνη και προσωπικά δεδομένα – Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679. *ΔΙΜΕΕ.* **Νομική Βιβλιοθήκη. Available at www.qualex.gr, 4 2018, pp. 460-466.**

80. Bussche, Paul Voigt · Axel von dem. *The EU General Data Protection Regulation (GDPR). A Practical Guide.* **Berlin : Springer. Available at https://link.springer.com/content/pdf/10.1007/978-3-319-57959-7.pdf, 2017.**

81. European Commitee of the Regions. *Opinion. European Approach to artificial intelligence - Artificial Intelligence Act (revised opinion).* **s.l. : European Commitee of the Regions, 2021.**

82. EuropeanCommission. *Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI ACT) and amending certain union legislative acts.* **Brussels : European Commission. Available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/AUTRES_INSTITUTIONS/COMM/COM/2022/04-25/COM_COM20210206_EN.pdf, 2021.**

83. Ιγγλεζάκης, Ιωάννης. *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (ν. 4624/2019).* **s.l. : Interactive Learning, 2020.**

84. Council of Europe. *Details of Treaty No.108.* **s.l. : www.coe.int.**

85. Article 29 Data Protection Working Party. *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680).* **s.l. : European Commission. Available at https://ec.europa.eu/newsroom/article29/items/610178, 2017. WP258.**

86. Κανέλλος, Λεωνίδας. *The GDPR Handbook.* **Αθήνα : Νομική Βιβλιοθήκη. Available at www.qualex.gr, 2020.**

87. Article 29 Data Protection Working Party. ***Guidelines on Automated individual decision-making and Profiling.*** **s.l. : http://ec.europa.eu/justice/data-protection/index_en.htm, 2018. WP251.**

88. European Commission. ***ec.europa.eu.*** **[Online] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en.**

89. Wrigley, Sam. Bots, the GDPR and Regulatory. [book auth.] Marcelo Corrales etc. ***Taming AI: Robotics, AI and the future of Law: Perspectives in Law, Business and Innovation.*** **s.l. : KYUSHU UNIVERSITY, SPRINGER, 2018.**

90. Μήτρου, Λ. ΙΙΙ. Προστασία δεδομένων by design/by default. [book auth.] Γ. Γιαννόπουλος etc. ***Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR).*** **Αθήνα : Νομική Βιβλιοθήκη. Available at www.qualex.gr, 2021.**

91. ***Facebook: Reconstructing Communication and Decostructing Privacy Law? MCIS 2009 Proceedings.*** **Mitrou, A.M. Piskopani and L. s.l. : MCIS 2009 Proceedings, 2009. Vol. http://aisel.aisnet.org/mcis2009/70.**

92. Party, Article 29 Data Protection Working. ***Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*** **s.l. : European Commission, 2017. WP248.**

93. Neuwirth, Rostam J. CGTN See the difference. ***news.cgtn.*** **[Online] 02 08, 2022. https://news.cgtn.com/news/2022-02-08/AI-and-human-mind-Manipulation-and-dangers-of-subliminal-AI-systems--17sA7bWEU5G/index.html.**

94. Lopatto, Elizabeth. The Verge. ***theverge.*** **[Online] 04 08, 2021. https://www.theverge.com/2021/4/8/22374749/elon-musk-neuralink-monkey-pong-brain-interface.**

95. Lodinová, Anna. Application of biometrics as a means of refugee registration: Focusing on UNHCR's strategy. *Development, Environment and Foresight.* **http://def-journal.eu/index.php/def, 2016, Vol. 2, 2.**

96. Smith, M. & Miller, S. *Biometric Identification, Law and Ethics.* **s.l. : Springer, 2021.**

97. eu-LISA. *SIS II.* **s.l. : Available at https://www.eulisa.europa.eu/AboutUs/MandateAndActivities/CoreActivities/Pages/SIS-II.aspx.**

98. Muzafer Saračevič, Mohamed Elhoseny, Aybeyan Selimi & Zoran Lončeravič. Possibilities of Applying the Triangulation Method in the Biometric Identification Process. [book auth.] Mohamed Elhoseny, Jude D. Hemanth Stepan Bilan. *Biometric Identification Technologies Based on Modern Data Mining Methods* **. s.l. : Springer International Publishing, 2021.**

99. Mohammad H. Ghaeminia, Shahriar B. Shokouhi & Abdollah Amirkhani. Biometric Gait Identification Systems: From Spatio-Temporal Filtering to Local Patch-Based Techniques. [book auth.] Mohamed Elhoseny, Jude D. Hemanth Stepan Bilan. *Biometric Identification Technologies Based on Modern Data Mining Methods* **. s.l. : Springer International Publishing, 2021.**

100. Stepan Bilan, Mykola Bilan & Andrii Bilan. Interactive Biometric Identification System Based on the Keystroke Dynamic. [book auth.] Mohamed Elhoseny, Jude D. Hemanth Stepan Bilan. *Biometric Identification Technologies Based on Modern Data Mining Methods.* **s.l. : Springer International Publishing, 2021.**

101. Stepan Bilan, Mykola Bilan, Andrii Bilan & Sergii Bilan. Analysis of the Dynamics of Handwriting for Biometric Personality Identification Based on Cellular Automata. [book auth.] Mohamed Elhoseny, Jude D. Hemanth Stepan Bilan. *Biometric Identification Technologies Based on Modern Data Mining Methods.* **s.l. : Springer International Publishing, 2021.**

102. Mykola Bilan, Andrii Bilan & Stepan Bilan. Identification of a Person by Palm Based on an Analysis of the Areas of the Inner Surface. [book auth.] Mohamed

Elhoseny, Jude D. Hemanth Stepan Bilan. ***Biometric Identification Technologies Based on Modern Data Mining Methods.*** **s.l. : Springer International Publishing, 2021.**

103. Ruslan Motornyuk, Andrii Bilan & Stepan Bilan. Research of Biometric Characteristics of the Shape of the Ears Based on Multi-Coordinate Methods. [book auth.] Mohamed Elhoseny, Jude D. Hemanth Stepan Bilan. ***Biometric Identification Technologies Based on Modern Data Mining Methods.*** **s.l. : Springer International Publishing, 2021.**

104. European Data Protection Board. ***edbp.europa.eu.*** **[Online] https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en.**

105. European Union Agency for Fundamental Rights. ***Facial recognition technology: fundamental rights considerations in the context of law enforcement.*** **Luxembourg : Publication Office of the European Union. Available at https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law, 2020.**

106. THALES. Buildimg a future we can all trust. ***thalesgroup.*** **[Online] 01 28, 2022. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/eurodac.**

107. Χριστίνα-Ειρήνη Ασημακοπούλου, DEA - ΜΔΕ, Δικηγόρος. Το δικαίωμα εναντίωσης σε αυτοματοποιημένες αποφάσεις υπό τον Ν 2472/1997 και υπό τον ΓΚΠΔ 2016/679 - Δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης και Τεχνητή Νοημοσύνη. ***Πειραϊκή Νομολογία.*** **Τράπεζα Νομικών Πληροφοριών Qualex, 2020, 4.**

108. Harvard Law Review Organisation. WISCONSIN SUPREME COURT REQUIRES WARNING BEFORE USE OF ALGORITHMIC RISK ASSESSMENTS IN SENTENCING. — State v. Loomis,. ***Harvard Law Review.*** **https://harvardlawreview.org/, 2017, Vol. 130 Harv. L. Rev. 1530.**

109. Κανέλλος, Λεωνίδας. ***Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο και στη διακστική πρακτική.*** **Αθήνα : Νομική Βιβλιοθήκη, 2021.**

110. Zoltán Kozma, Mark Almasy. DLA Piper (Global law firm). ***dlapiper.com.*** **[Online] 04 12, 2022. https://blogs.dlapiper.com/privacymatters/hungary-record-gdpr-fine-by-the-hungarian-data-protection-authority-for-the-unlawful-use-of-artificial-intelligence/.**

111. Rick's cloud. ***rickscloud.com.*** **[Online] 2022. https://rickscloud.com/intelligent-cars-ai-and-the-automotive-industry/.**

112. EUROPEAN DATA PROTECTION SUPERVISOR. ***edps.europa.eu.*** **[Online] https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en.**

113. Mildebrath, Tambiama Madiega and Hendrik. ***Regulating facial recognition in EU. In-depth analysis.*** **s.l. : European Parliamentary Research Service, 2021.**

114. ***https://european-union.europa.eu.*** **[Online] https://european-union.europa.eu/index_en.**

115. ***Fingerprinting.*** **Thomas Whetstone, Jean-Paul Brodeur. https://www.britannica.com/topic/police/Crime-scene-investigation-and-forensic-sciences, s.l. : Encyclopedia Britannica, Vol. Police technology.**

116. ***Johann Christoph Andreas Mayer.*** **Wikipedia. s.l. : https://de.wikipedia.org/wiki/Johann_Christoph_Andreas_Mayer.**

117. Ashbourn, Julian. ***Biometrics: Advanced identity verification: the complete guide.*** **s.l. : Springer, 2000.**

118. ***Francis Galton.*** **Wikipedia. s.l. : https://en.wikipedia.org/wiki/Francis_Galton.**

119. ***Juan Vucetich (1858–1925).*** **National Library of Medicine in USA. s.l. : https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/biographies/vucetich.html, Vol. Biographies.**

120. ***Edward Henry.*** **Wikipedia. s.l. : https://en.wikipedia.org/wiki/Edward_Henry.**

121. Robert Allen, Pat Sankar, Salil Prabhakar. Fingerprint identification technology. [book auth.] James Wayman etc. ***Biometric Systems.*** **s.l. : Springer, 2005.**

122. ***The Bertillon system.*** **National Library of Medicine in USA. s.l. : https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/technologies/bertillon.html, Vol. Tecnologies.**

123. European Union Agency for Fundamental Rights. ***Preventing unlawful profiling today and in the future: a guide.*** **Luxembourg : Publications Office, fra.europa.eu., 2018.**

124. NewEurope, "Sweden authorises the use of facial recognition. NEWEUROPE. ***neweurope.*** **[Online] 2019. https://www.neweurope.eu/article/sweden-authorises-the-use-of-facial-recognition-technology-by-the-police/.**

125. ***Facial recognition in school renders Sweden's first GDPR fine.*** **s.l. : European Data Protection Board. Available at https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv, 2019.**

126. Edvardsen, Sofia. iapp. ***iapp.*** **[Online] https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/.**

127. Az.: RN 9 K 19.1061, Available at https://www.datenschutz.eu/urteile/Keine-Rechtsbehelfe-neben-der-DSGVO-Verwaltungsgericht-Regensburg-20200806/. Regensburg : Verwaltungsgericht, Urteil v. 06.08.2020.

128. Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD). ***Der Bayerische Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit, 28. Tätigkeitsbericht, Berichtzeitraum 2017/2018.*** **München : BayLfD, 2019. Entschließung der 93. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 29./30. März 2017.**

129. Berliner Beauftragte für Datenschutz und Informationsfreiheit. ***Datenschutz und Informationsfreiheit, Jahresbericht 2018.*** **s.l. : ARNOLD group, 2019.**

130. —. ***Datenschutz und Informationsfreiheit, Jahresbericht 2020.*** **Berlin : ARNOLD group, 2021.**

131. 17 K 203/19, Hamburg : Administrative Court of Hamburg, 23/10/2019.

132. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. *Tätigkeitsbericht, Datenschutz, 2020.* **Hamburg : Druckerei Siepmann GmbH, 2021.**

133. Polizei Hamburg: Datenbank zum Gesichtsabgleich gelöscht. *datensicherheit.de.* **[Online] 05 28, 2020. https://www.datensicherheit.de/polizei-hamburg-datenbank-gesichtsabgleich-loeschung.**

134. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. *Tätigkeitsbericht. Datenschutz 2020.* **Hamburg : Druckerei Siepmann GmbH, 2021.**

135. Fussey, P. and Murray, D. *The human rights, big data and technology project. Independent Report on the London Metropolitan Police Service' s Trial of Live Facial Recognition Technology.* **Essex : Economical and Social Research Council. University of Essex. Available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf, 2019.**

136. Supervisor, European Data Protection. *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.* **s.l. : European Data Protection Supervisor. Available at https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf, 2017.**

137. (EDPS), European Data Protecrion Supervisor. *THE EDPS VIDEO-SURVEILLANCE GUIDELINES* **. Brussels : EDPS. Available at https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf, 2010.**

138. Masterman, Roger. The independence of the judiciary. *The separation of the judicial branch.* **s.l. : Cambridge University Press, 2011.**

139. *Roman Zakharov v. Russia.* **ECHR. Strasbourg : ECHR, 04.12.2015.**

140. European Data Protection Broad - European Data Protection Supervisor. *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of*

the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). **s.l. : https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf, 2021.**

141. Χιωτέλλης, Α. Προσωπικά δεδομένα και πιστοληπτική ικανότητα. *Χρηματοπιστοτικό Δίκαιο.* **Νομική Βιβλιοθήκη. Available at qualex.gr, 2010, 3.**

142. Μ. Μυλώση, Ευ. Αλεξανδροπούλυ – Αιγυπτιάδου. Προσωπικά δεδομένα οικονομικής συμπεριφοράς και ηλεκτρονική επεξεργασία από την ΤΕΙΡΕΣΙΑΣ ΑΕ. *ΔΙΜΕΕ.* **Νομική Βιβλιοθήκη. Available at qualex.gr, 2015, 1.**

143. Abedjan, Ziawasch etc. *Data Profiling. Synthesis Lectures on Data Management.* **San Rafael, California : Morgan & Claypool Publishers, 2019.**

144. SCHUFA. [Online] https://www.schufa.de.

145. SCHUFA. *SCHUFA.* **[Online] 10 2020. https://www.schufa.de/schufa-en/schufa-notification-according-to-art-14-gdpr/.**

146. *How AI Supports Financial Institutions for Deciding Creditworthiness. Artificial Intelligence (AI) emerges as the most accurate, instant, and practical method to check the payback abilities of borrowers.* **Chawla, Rachit. s.l. : Entrepreneur India, 2018. https://www.entrepreneur.com/article/310262.**

147. Robalinho, Manuel Silva. Credit Score using Machine Learning. *DataDrivenInvestor.* **[Online] https://medium.datadriveninvestor.com/credit-score-using-machine-learning-cc1a383808ea.**

148. *AI for Credit Scoring – An Overview of Startups and Innovation.* **Mejia, Niccolo. s.l. : Emerj. The AI Research and Advisory Company. Available at https://emerj.com/ai-sector-overviews/ai-for-credit-scoring-an-overview-of-startups-and-innovation/, 2019.**

149. World Eonomic Forum. *Identity in a Digital World. A new chapter in the social contract.* **Switzerland : World Eonomic Forum, 2018.**

150. *Globalists embrace leveraging social media, location & behavioral data for alternative credit scoring. Analyzing an individual's personality & social behavior*

for credit scoring risks introducing CCP-style social credit system: perspective. **Hinchliffe, Tim. s.l. : The Sociable. Available at https://sociable.co/government-and-policy/globalists-embrace-social-media-location-behavioral-data-alternative-credit-scoring/, 2021.**

151. Professor Dr. Michael Ronellenfitsch, Hessischen Beauftragten für Datenschutz und Informationsfreiheit. *Achtundvierzigster Tätigkeitsbericht zum Datenschutz und Zweiter Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit.* **Wiesbaden : AC medienhaus GmbH, 2020.**

152. 2965, Athens : Greek Council of State, 2017.

153. *Forderungsmeldung an SCHUFA bei Urteil ohne vorherige Androhung rechtmäßig.* **Az.: 4 U 90/19, Berlin : Kammergericht Berlin, 2019.**

154. Ronellenfitsch, Professor Dr. Michael. *Neunundvierzigster Tätigkeitsbericht zum Datenschutz und Dritter Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit.* **Wiesbaden : AC medienhaus GmbH, 2021.**

155. 3040/2017, Athens : Greek Council of State, 2017.

156. B6-22/16, Germany : Bundeskartellamt (Federal Cartel Office), 2019.

157. Bundeskartellamt. *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate* **. s.l. : Bundeskartellamt, 2019.**

158. Berliner Beauftragte für Datenschutz und Informationsfreiheit. *Datencshutz und Informationsfreiheit, Jahresbericht 2021.* **Berlin : ARNOLD group, 2022.**

159. *China's Social Credit System: Speculation vs. Reality. How far along is China's much-hyped social credit system – and where is it heading next?* **Jessica Reilly, Muyao Lyu, and Megan Robertson. s.l. : The diplomat, 2021.**

160. *China's 'social credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy.*

Canales, Katie. s.l. : Insider, 2021, Vols. https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

161. Hoffman, Samantha. ***Programming China: The Communist Party's autonomic approach to managing state security.*** **s.l. : Mercator Institute for China Studies, 2018.**

162. Botsman, Rachel. ***Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart.*** **London : Penguin Business, 2017.**

163. wikipedia.org. [Online] https://en.wikipedia.org/wiki/Social_Credit_System.

164. ***Inside China's Plan to Give Every Citizen a Character Score. New Scientist Available at*** **. Hodson, Hal. s.l. : Newscientist, 2015 . https://www.newscientist.com/article/dn28314-inside-chinas-plan-to-give-every-citizen-a-character-score/.**

165. ***A Chinese university suspended a student's enrolment because of his dad's bad social credit score.*** **Chan, Tara Francis. s.l. : Insider, 2018. https://www.businessinsider.com/china-social-credit-affects-childs-university-enrolment-2018-7.**

166. ***Chinese dog owners are being assigned a social credit score to keep them in check — and it seems to be working.*** **Perper, Rosie. 2018. https://www.businessinsider.com/china-dog-owners-social-credit-score-2018-10.**

167. ***China's Chilling 'Social Credit' Blacklist. A lawyer is barred from buying a plane ticket because a court found his apology 'insincere.'.*** **Wang, Maya. s.l. : Human Rights Watch (Published in: The Wall Street Journal), 2017. https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist.**

168. ***The truth and reality of China's social credit system.*** **Bei, Fan Zhengjie and Zhang. Brussels : EUobserver.com, 2019. https://euobserver.com/stakeholders/145779.**

169. ***How China Wants to Rate its Citizens.*** **Fan, Jiayang. s.l. : The New Yorker, available at https://www.newyorker.com/news/daily-comment/how-china-wants-to-rate-its-citizens, 2015.**

170. Kshetri, Nir. Big data's role in expanding access to financial services in China. *International Journal of Information.* **2016, Vol. 36, 3.**

171. Zurn, Christopher F. Identity or Status? Struggles over 'Recognition' in Fraser, Honneth, and Taylor. *Constellations. An International Journal of Critical and Democratic Theory.* **John Wiley & Sons Ltd, 2003, Vol. 10, 4.**

172. Cinnamon, Jonathan. Social Injustice in Surveillance Capitalism. *Surveillance & Society.* **University of Exeter, UK, 2017, Vol. 15, 5.**

173. Ashwin Acharya, Max Langenkamp and James Dunham. *Trends in AI Research for the Visual Surveillance of Populations. CSET Data Brief.* **s.l. : Center for Security and Emerging Technology. Georgetown University of USA, 2022.**

174. Nash, Jim. *China intensifies biometrics, video surveillance research as social credit market builds.* **s.l. : BiometricUpdate.com, 2022. https://www.biometricupdate.com/202201/china-intensifies-biometrics-video-surveillance-research-as-social-credit-market-builds.**

175. *China to introduce digital ID cards nationwide.* **Macdonald, Ayang. s.l. : BiometricUpdate.com, 2022. https://www.biometricupdate.com/202203/china-to-introduce-digital-id-cards-nationwide.**

176. Article 19, Free Word Centre. *Emotional Entanglement: China's emotion recognition market and its implications for human rights.* **s.l. : Article 19, Free Word Centre, 2021.**

177. *China's Social Credit System: AI-driven panopticon or fragmented foundation for a sincerity culture?* **Borak, Masha. s.l. : Technode.com, 2017. https://technode.com/2017/08/23/chinas-social-credit-system-ai-driven-panopticon-or-fragmented-foundation-for-a-sincerity-culture/.**

178. *Is China's social credit system as Orwellian as it sounds?* **page, Karen Haoarchive. s.l. : MIT Technology Review, 2019. https://www.technologyreview.com/2019/02/26/137255/chinas-social-credit-system-isnt-as-orwellian-as-it-**

sounds/#:~:text=There%20is%20actually%20no%20AI%20or%20other%20technology,system%20is%20designed%20to%20incentivize%20lawfulness%20and%20integrity..

179. Sauter, Wolf. Proportionality in EU Law: A Balancing Act? *Cambridge Yearbook of European Legal Studies.* **Cambridge University Press. Available at https://www.cambridge.org/core/services/aop-cambridge-core/content/view/156C8294184A2B4C8C7A619F124D9E82/S1528887000003128a.pdf/proportionality_in_eu_law_a_balancing_act.pdf, 2013, 15.**

180. Wikipedia. The Free Encyclopedia. *wikipedia.org.* **[Online] https://en.wikipedia.org/wiki/Generation_Z.**

181. Γκόγκου, Μ. OW. *www.ow.gr.* **[Online] https://www.ow.gr/living/erevna-i-gen-z-den-einai-mono-paidia-tis-texnologias/.**

182. Z. *generationz.* **[Online] https://generationz.com.au/articles/technology/.**

183. HP. *https://garage.hp.com.* **[Online] https://garage.hp.com/us/en/modern-life/generation-z-redefining-the-world.html.**

184. Vigo, Julian. Forbes. *www.forbes.com.* **[Online] 08 31, 2019. https://www.forbes.com/sites/julianvigo/2019/08/31/generation-z-and-new-technologys-effect-on-culture/.**

185. Wikipedia. The Free Encyclopedia. *wikipedia.org.* **[Online] https://en.wikipedia.org/wiki/Millennials.**

186. CNN. *edition.cnn.com.* **[Online] https://edition.cnn.com/2017/05/01/health/young-old-millennial-partner/index.html.**

187. SoftwareLab.org. *softwarelab.* **[Online] 2022. https://softwarelab.org/avast-antivirus-review/#:~:text=In%202020%2C%20Avast%20was%20caught%20in%20a%20scandal,Have%20a%20look%20at%20Bitdefender%20or%20Norton%20instead..**

188. European Data Protection Board. *edpb.europa.eu.* **[Online] 02 21, 2022. https://edpb.europa.eu/news/national-news/2022/swedish-authority-privacy-protection-imy-fines-region-uppsala-breaches-its_en.**

189. European Data Protection Board. *edpb.europa.eu.* **[Online] https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en.**

190. Wikipedia. Gottfried Wilhelm Leibniz . *wikipedia.org.*

191. —. Propositional calculus. *wikipedia.org.*

192. Χίου, Θ. Τεχνητή Νοημοσύνη και Πνευματική Ιδιοκτησία – σε ποιον ανήκουν οι δημιουργίες μηχανών;. *ΔΙΜΕΕ.* **2 2020, pp. 200-224.**

193. Μπουρμάς, Γ. *Ποινική Προστασία Περιβάλλοντος, Ερμηνευτικές προσεγγίσεις & ειδικότεροι δογματικοί προβληματισμοί.* **Αθήνα : Νομική Βιβλιοθήκη, 2020.**

194. Καράκωστας, Ι. *Δίκαιο Προστασίας Καταναλωτή.* **Αθήνα : Νομική Βιβλιοθήκη, 2016.**

195. *What Is Computer Vision & How Does it Work? An Introduction.* **Babich, Nick. s.l. : https://xd.adobe.com, 2020.**

196. *SRILAB. s.l. : https://www.sri.inf.ethz.ch.*

197. Yongquan Dong, Zichen Zhang and Wei-Chiang Hong. A Hybrid Seasonal Mechanism with a Chaotic Cuckoo Search Algorithm with a Support Vector Regression Model for Electric Load Forecasting. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecasting by Artificial Intelligent Technologies.

198. Jiyang Wang, Yuyang Gao and Xuejun Chen. A Novel Hybrid Interval Prediction Approach Based on Modified Lower Upper Bound Estimation in Combination with Multi-Objective Salp Swarm Algorithm for Short-Term Load Forecasting. Energies. www.mdpi.com/journal/energies , 2019, Vols. Short-Term Load Forecasting by Artificial Intelligent Technologies.

199. Zhang, Xing. Short-Term Load Forecasting for Electric Bus Charging Stations Based on Fuzzy Clustering and Least Squares Support Vector Machine Optimized by Wolf Pack Algorithm. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecasting by Artificial Intelligent Technologies.

200. Gregory Merkel, Richard I. Povinelli. Identity and Ronald H. Brown, Short-term forecasting of natural gas load with deep neural network reflux †. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecast by Artificial Intelligent Technologies.

201. Miguel López, Carlos Sans, Sergio Valero and Carolina Senabre. Empirical Comparison of Neural Network and Auto-Regressive Models in Short-Term Load Forecasting. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecasting by Artificial Intelligent Technologies.

202. Gregory D. Merkel, Richard J. Povinelli ID and Ronald H. Brown. Gregory D. Merkel, Richard J. Povinelli Short-Term Load Forecasting of Natural Gas with Deep Neural Network Regression †. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-term load forecasting from artificial intelligent technologies.

203. Fu-Cheng Wang, Yi-Shao Hsiao and Yi-Zhe Yang. The Optimization of Hybrid Power Systems with Renewable Energy and Hydrogen Generation. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecasting by Artificial Intelligent Technologies.

204. Wei Sun, Chongchong Zhang. A Hybrid BA-ELM Model Based on Factor Analysis and Similar-Day Approach for Short-Term Load Forecasting. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-term Load Forecasting by Artificial Intelligent Technologies.

205. Chengdong Li, Zixiang Ding, Jianqiang Yi, Yisheng Lv and Guiqing Zhang. Deep Belief Network Based Hybrid Modelfor Building Energy Consumption Prediction. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-term Load Forecasting by Artificial Intelligent Technologies.

206. Mergani A. Khairalla, Xu Ning, Nashat T. AL-Jallad and Musaab O. El-Faroug. Short-term forecast for energy consumption through Stacking heterogeneous ensemble learning model. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-term load forecasting from artificial intelligent technologies.

207. Benjamin Auder, Jairo Cugliari, Yannig Goude and Jean-Michel Poggi. Scalable Clustering of Individual Electrical Curves for Profiling and Bottom-Up Forecasting. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecasting by Artificial Intelligent Technologies.

208. Yunyan Li, Yuansheng Huang and Meimei Zhang. Short-Term Load Forecasting for Electric Vehicle Charging Station Based on Niche Immunity Lion Algorithm and Convolutional Neural Network. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-term Load Forecasting by Artificial Intelligent Technologies.

209. Jihoon Moon, Yongsung Kim, Minjae Son and Eenjun Hwang. Hybrid Short-Term Load Forecasting Scheme Using Random Forest and Multilayer Perceptron †. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-term Load Forecasting by Artificial Intelligent technologies.

210. Benjamin Auder, Jairo Cugliari, Yannig Goude and Jean-Michel Poggi. Scalable Clustering of Individual Electrical Curves for Profiling and Bottom-Up Forecasting. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecasting by Artificial Intelligent Technologies.

211. María del Carmen Ruiz-Abellón, Antonio Gabaldón and Antonio Guillamón. María del Carmen Ruiz-Abellón 1, Antonio Gabaldón 2, IDLoad Forecasting for a Campus University Using Ensemble Methods Based on Regression Trees. Energies. www.mdpi.com/journal/energies, 2019, Vols. Short-Term Load Forecasting by ARtificial Intelligent technologies.*

212. Council of Europe. Artificial intelligence and judicial systems: The so-called predictive justice . s.l. : https://experts-institute.eu/wp-content/uploads/2, 2018.

213. Information Privacy, Definition. Techopedia. s.l. : https://www.techopedia.com/definition/10380/information-privacy, 2017.

214. Types of EU law. European Commission. s.l. : https://ec.europa.eu/info/law/law-making-process/types-eu-law_en.

215. Francis Galton. Famous Psychologists. s.l. : https://www.famouspsychologists.org/francis-galton/.

216. Alphonse Bertillon. Wikipedia. s.l. : https://en.wikipedia.org/wiki/Alphonse_Bertillon.

217. Smith, Marcus. DNA evidence in the Australian legal system. Australian Journal of Forensic Sciences. 2017, Vol. 49, 2.

218. 'Anonymised' data can never be totally anonymous. Hern, Alex. https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds, s.l. : The Guardian, 2019, Vol. Data protection.

219. Papanikolaou, Aikaterina. Course in Law and Electronic Communications. s.l. : University of Piraeus, https://evdoxos.ds.unipi.gr/courses/LAWICT104/, 2020.

220. Σισιλιάνος, Λίνος - Αλέξανδρος. Άρθρο 8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου. Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (Ερμηνεία κατ' Άρθρο). s.l. : Νομική Βιβλιοθήκη, 2017.

221. Kennedy v. the United Kingdom. ECHR. s.l. : ECHR, 18.05.2010.

222. Szabo and Vissy v. Hungary. ECHR. s.l. : ECHR, 12.01.2016.

223. Klass and others v. Germany. ECHR. s.l. : ECHR, 06.09.1978.

224. Dragojević v. Croatia. ECHR. s.l. : ECHR, 15.01.2015.

225. Tele2 Sverige AB (C-203/2015) vs Post-och telestyrelsen, Secretary of State for the Home Department (C-698/15) vs Tom Watson. European Court of Justice. s.l. : https://european-union.europa.eu/institutions-law-budget/law/find-case-law_en, 21.12.2016.

226. CENTRUM FÖR RÄTTVISA v. SWEDEN. ECHR. STRASBOURG : ECHR, 19.06.2018/04.02.2019.

227. The association for European Integration and human rights and Ekimdzhiev vs. Bulgaria. ECHR. Strasbourg : ECHR, 28.06.2007/30.01.2008.

228. Dimitru Popescu v. Romania. ECHR. Strasbourg : ECHR, 26.04.2007 .

229. Federal Commissioner for Data Protection and Freedom of Information. BfDI. BfDI. [Online] https://www.bfdi.bund.de/EN/Fachthemen/Gremienarbeit/Datenschutzkonferenz/datenschutzkonferenz_node.html#:~:text=Data%20Protection%20Conference%20The%20committee%20of%20Independent%20German,%E2%80%93%20meets%20twice%20a%20year%20under%20rotating%20chairma.

230. —. BfDI. BfDI. [Online] 1 11, 2022. https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/EN/2022/01_DSK-Vorsitz-2022.html#:~:text=The%20DSK%20consists%20of%20the%20independent%20data%20protection,and%20working%20together%20to%20promote%20its%20further%20development..

231. Polizei Hamburg: Datenbank zum Gesichtsabgleich gelöscht. datensicherheit.de. [Online] 05 28, 2020. https://www.datensicherheit.de/polizei-hamburg-datenbank-gesichtsabgleich-loeschung.

232. Πρόστιμο 665.000 ευρώ σε τράπεζα για παράνομη χρήση τεχνολογίας Τεχνητής Νοημοσύνης για την ανάλυση συναισθημάτων των πελατών της. Lawspot.gr. [Online] 05 03, 2022. https://www.lawspot.gr/nomika-nea/prostimo-665000-eyro-se-trapeza-gia-paranomi-hrisi-tehnologias-tehnitis-noimosynis-gia?lspt_destination=upgrade.

233. AI-based speech-signal processing technology and data protection. NAIH-85-3/2022, Budapest : [Hungarian] National Authority for Data Protection and Freedom of Information, 2022.

234. Referring court: Oberlandesgericht Düsseldorf. Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on . C-252/21, Official Journal of the European Union : Court of Justice, 2021.

235. SCHUFA. [Online] https://www.schufa.de.

236. Wikipedia. Yelp. Wikipedia.org. [Online] https://en.wikipedia.org/wiki/Yelp.

237. κλπ, Δ. Τζουγανάτος. Δίκαιο του Ελεύθερου Ανταγωνισμού - 1ος τόμος, Ουσιαστικό δίκαιο του ελεύθερου ανταγωνισμού. s.l. : Νομική Βιβλιοθήκη, 2020.

238. κλπ., Δ. Τζουγανάτος. Δίκαιο του Ελεύθερου Ανταγωνισμού - 1ος τόμος, Ουσιαστικό δίκαιο του ελεύθερου ανταγωνισμού. s.l. : Νομική Βιβλιοθήκη, 2020.

239. Wikipedia. The free Encyclopedia. Wikipedia. [Online] https://en.wikipedia.org/wiki/Propositional_calculus#:~:text=Propositional%20calculus%20is%20a%20branch%20of%20logic.%20It,including%20the%20construction%20of%20arguments%20based%20on%20them..

240. Wikipedia. The free Encyclopedia. Wikipedia. [Online] https://en.wikipedia.org/wiki/Age_of_Enlightenment.

241. Wikipedia. The free Encyclopedia. Wikipedia. [Online] https://en.wikipedia.org/wiki/Ren%C3%A9_Descartes.

242. Wikipedia. The free Encyclopedia. Wikipedia. [Online] https://en.wikipedia.org/wiki/Baruch_Spinoza.

243. Wikipedia. The free Encyclopedia. Wikipedia. [Online] https://en.wikipedia.org/wiki/Gottfried_Wilhelm_Leibniz.

244. Wikipedia. The Free Encyclopedia. Wikipedia. [Online] https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist).

245. Wikipedia. The Free Encyclopedia. wikipedia. [Online] https://en.wikipedia.org/wiki/Baruch_Spinoza.

246. Wikipedia. The Free Encyclopedia. wikipedia. [Online] https://en.wikipedia.org/wiki/Article_29_Data_Protection_Working_Party#:~:text=The%20Article%2029%20Working%20Party%20%28Art.%2029%20WP%29%2C,European%20Data%20Protection%20Supervisor%20and%20the%20European%20Commission..

247. κλπ, Δ. Λαδάς. Εργατικές Διαφορές. Δικονομικά Ζητήματα. Αθήνα : Νομική Βιβλιοθήκη. Available at qualex.gr, 2019.

248. Μίτλεττον, Φ. κλπ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 15 χρόνια λειτουργίας, Επετειακή Διημερίδα, 23 & 24.05.2013, Κείμενα Εισηγήσεων. Αθήνα : Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2014.

249. Greek Council of State. 442, Athens : Greek Council of State, 2014.

250. Press release. Judgements and decisions of 11 June 2020. Strasbourg : European Court of Human Rights. The Registrar of the Court., 2020.

251. P.N. v. Germany. 74440/2017, Strasbourg : European Court of Human Rights (ECtHR), 11/06/2020.

252. McKeith, William. The Sydney morning herald. smh.com.au. [Online] 7 14, 2019. https://www.smh.com.au/national/cctv-is-watching-students-and-teachers-but-how-much-surveillance-do-schools-need-20190712-p526o9.html.

253. Tiresias. Relible information for right decisions. tiresias. [Online] http://www.tiresias.gr/en/company.html.

254. ΕΚΠΑ. University of Athens. http://cogsci.phs.uoa.gr. [Online] http://cogsci.phs.uoa.gr/gnwsiaki-epistimh.html.

255. European Commission. https://ec.europa.eu. [Online] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

256. Vega, Nicolas. CNBC. cncb.com. [Online] 05 13, 2021. https://www.cnbc.com/2021/05/13/older-millennials-are-still-keeping-up-with-the-latest-tech.html#:~:text=The%20oldest%20millennials%20may%20be%20turning%2040%2C%20but,tech%20Published%20Thu%2C%20May%2013%20202110%3A34%20AM%20EDT.

257. Fichtinger, Ines. A Review of Security Operation Centers: State of the Art and Current Challenges. s.l. : Universität Regensburg, 2019.

258. etc, Stehr-Green PA. Developing a Questionnaire. Focus on Field Epidemiology. 2 (2).

259. Reja U, Manfreda K, Hlebec V et al. Open-ended vs. Close-ended Questions in Web Questionnaires. 2003.

260. Connor Desai S, Reimers S. Comparing the use of open and closed questions for Web-based measures of the continued-influence effect. s.l. : doi: 10.3758/s13428-018-1066-z, 2019.

261. Boynton PM, Greenhalgh T. Selecting, designing, and developing your questionnaire. s.l. : doi: 10.1136/bmj.328.7451.1312, 2004.

262. P, Lietz. Research into questionnaire design: A summary of the literature. International Journal of Market Research. doi: 10.2501/S147078530920120X, 2010, Vol. 52, 2.

263. A, Williams. How to … Write and Analyse a Questionnaire. Journal of Orthodontics. doi: 10.1093/ortho.30.3.245, 2003, Vol. 30, 3.

264. RB, Fray. Hints for designing effective questionnaires. Practical Assessment, Research &Evaluation. 1996. Vol. 5, 3.

265. E, Taylor-Powell. Questionnaire Design: Asking Questions with a Purpose. Program Development and Evaluation. . s.l. : Available at https://vulms.vu.edu.pk/courses/HRM619/Downloads/How_to_ask_questions_through_questionnaire.pdf, 2005.

266. Lefever S, Dal M, Matthíasdóttir Á. s.l. : doi: 10.1111/j.1467-, 2007. Vol. 38, 4.

267. Typeform. Typeform . [Online] https://www.typeform.com/.

268. Evans JR, Mathur A. The value of online surveys. Internet Research. s.l. : doi: 10.1108/10662240510590360, 2005. Vol. 15, 2.

269. J, Lumsden. Online-Questionaire Design Guidelines. In: Baker JD, Reynolds RA, Woods R (eds) Handbook of research on electronic surveys and measurements. s.l. : IGI Global (701 E. Chocolate Avenue Hershey Pennsylvania 17033 USA), Hershey, 2007.

270. Abraham SY, Steiger DM, Sullivan C. Electronic and mail self-administered questionnaires: A comparative assessment of use among elite populations. In: Proceedings of the Section on .

271. Academic Skills. http://skillsacademic.weebly.com. [Online] http://skillsacademic.weebly.com/taurhoiotagammaomeganuomicronpiomicron943etasigmaeta.html.

272. Τζιαφέρη, Στυλιανή. ΤΡΙΓΩΝΟΠΟΙΗΣΗ, (Ποιοτική σε συνδυασμό με ποσοτική έρευνα). Αθήνα : University of Athens & University of Peloponnisos, 2014.

273. Yin, Robert K. Qualitative Research from Start to Finish, mentioned in: https://libguides.usc.edu/writingguide/qualitative. s.l. : 2nd edition. New York: Guilford, 2015.

274. Writing@CSU. Colorado State University. Qualitative Research Methods, mentioned in: https://libguides.usc.edu/writingguide/qualitative. s.l. : Colorado State University.

275. Maxwell, Joseph A. Designing a Qualitative Study. [book auth.] Leonard Bickman and Debra J. Rog. The SAGE Handbook of Applied Social Research Methods, mentioned in: https://libguides.usc.edu/writingguide/qualitative. s.l. : eds. 2nd ed. Thousand Oaks, CA: Sage, 2009.

276. Marshall, Catherine and Gretchen B. Rossman. Designing Qualitative Research, mentioned in: https://libguides.usc.edu/writingguide/qualitative. s.l. : 3rd edition. Thousand Oaks, CA: Sage, 1999.

277. Heath, A. W. The Proposal in Qualitative Research. The Qualitative Report 3, mentioned in: Qualitative Methods - Organizing Your Social Sciences Research Paper - Research Guides at University of Southern California (usc.edu). 1997.

278. Chenail, Ronald J. Introduction to Qualitative Research Design, mentioned in: Qualitative Methods - Organizing Your Social Sciences Research Paper - Research Guides at University of Southern California (usc.edu). Texas, USA : Nova Southeastern University, first published 2011, updated 2021.

279. Denzin, Norman. K. and Yvonna S. Lincoln. Introduction: The Discipline and Practice of Qualitative Research, mentioned in: Qualitative Methods - Organizing Your Social Sciences Research Paper - Research Guides at University of Southern California (usc.edu). [book auth.] Norman. K. Denzin and Yvonna S. Lincoln. The Sage Handbook of Qualitative Research. s.l. : Thousand Oaks, CA: Sage, eds. 3rd edition, 2005.

280. Bhandari, Pritha. Scribbr. www.scribbr.com. [Online] 02 10, 2022. https://www.scribbr.com/methodology/qualitative-research/.

281. Μιλτιάδης Χαλικιάς, Αλεξάνδρα Μανωλέσου, Παναγιώτα Λάλου. Μεθοδολογία Έρευνας και Εισαγωγή στη Στατιστική Ανάλυση Δεδομένων με το IBM SPSS STATISTICS. Athens : National Technical University of Athens. Available at https://eclass.uoa.gr/modules/document/file.php/PRIMEDU306/Biblio%20Statistics%20SPSS%20Kalipos.pdf, 2015.

282. Ανάβασις. Εκπαιδευτικός Όμιλος. www.anavasis.gr. [Online] https://www.anavasis.gr/blog/poiotiki-ereuna-kai-poiotiki-analisi.

283. iziPen team. iziPen. izipen.gr. [Online] 9 21, 2020. https://izipen.gr/blog/methodologia-ereunas/.

284. University of West Attica. https://eclass.uniwa.gr. [Online] https://eclass.uniwa.gr/modules/document/file.php/MECH112/%CE%A0%CE%91%CE%A1%CE%9F%CE%A5%CE%A3%CE%99%CE%91%CE%A3%CE%95%CE%99%CE%A3/%CE%9C%CE%95%CE%98%CE%9F%CE%94%CE%9F%CE%99_%CE%95%CE%A1%CE%95%CE%A5%CE%9D%CE%91%CE%A3%20Copy.pdf.

285. Μπατσίδης, Απόστολος. University of Ioannina. http://users.uoi.gr. [Online] 2014. http://users.uoi.gr/abatsidis/SPSSClassNotes2014.pdf.

286. StepUp. https://stepupadvisor.gr. [Online] https://stepupadvisor.gr/dhmiourgia-erwthmatologiou-ereynas-ti-na-prosexeis/.

287. University of Thessaly. lab.pr.uth.gr. [Online] http://lab.pe.uth.gr/psych/index.php?option=com_content&view=article&id=87&Itemid=245&lang=el.

288. Παπαιωάννου, Α., Θεοδωράκης Ι., & Γούδας, Μ. Ποιοτικές – ερμηνευτικές μέθοδοι έρευνας στη φυσική αγωγή. Για μία καλύτερη φυσική αγωγή. Θεσσαλονίκη : Εκδόσεις Χριστοδουλίδη. Available at http://lab.pe.uth.gr/psych/images/stories/pdf/various/diavaste_perissotera_gia_poiotikes_methodoys_ereynas.pdf.

289. Γούδας, Μαρία Χασάνδρα και Μάριος. Κριτήρια εγκυρότητας και αξιοπιστίας στην ποιοτική – ερμηνευτική έρευνα. Επιστημονική Επετηρίδα της Ψυχολογικής Εταιρείας Βορείου Ελλάδος,. University of Thessaly. Available at http://lab.pe.uth.gr/psych/images/stories/pdf/various/kritiria_egyrotitas_kai_aksiopistias_stin_poiotiki_ereyna.pdf, 2003, Vol. 2.

290. Ζαφειρόπουλος, Κ. University of Macedonia, Hellenic Republic. compus.uom.gr. [Online] http://compus.uom.gr/YEP109/document/lectures/lecture_03/erwthseis.pdf.

291. Άνθη, Μαρία. Μεθοδολογία ποσοτικής και ποιοτικής έρευνας. Επιστημονικές Εργασίες Τριτοβάθμιας Εκπαίδευσης. s.l. : Μ. Σιδέρη. SiderisBooks. Available at https://www.emeis.gr/methodologia-posotikis-kai-poiotikis-ereunas/, 2012.

292. Abedjan, Ziawasch etc. Data Profiling. Synthesis Lectures on Data Management. San Rafael, California : Morgan & Claypool Publishers, 2019.

293. 137/2020, Athens : Greek Court of State, 2020.

294. Kalantari D. H, Kalantari D. E, Maleki S. E-survey (surveys based on e-mail & web). Procedia Computer Science. s.l. : doi: 10.1016/j.procs.2010.12.153, 2011. Vol. 3.

295. University of Southern California (USC) Libraries. https://libguides.usc.edu. [Online] https://libguides.usc.edu/writingguide/qualitative#:~:text=Characteristics%20of%20

Qualitative%20Research%201%20Naturalistic%20--%20refers,because%20they%20are%20%E2%80%9Cinformation%20rich%E2%80%9D%20and%20illuminative.%20.

296. Wikipedia. The Free Encyclopedia. wikipedia.org. [Online] https://en.wikipedia.org/wiki/Claude_Shannon.

297. The Editors of Encyclopaedia Britannica. cogito, ergo sum. [https://www.britannica.com/topic/cogito-ergo-sum]

298. European Commission. White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020. Brussels : European Commission, 2020.

299. Wikipedia. Wikipedia. The Free Encyclopedia. wikipedia.org. [Online] https://en.wikipedia.org/wiki/Turing_test.