T.C.
MARMARA ÜNİVERSİTESİ
AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ
AVRUPA HUKUKU ANABİLİM DALI

THE PROTECTION OF BIOMETRIC DATA IN THE ERA OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN EU LAW

YÜKSEK LİSANS TEZİ

FURKAN DARENDELİ

İSTANBUL- 2023

T.C.
MARMARA ÜNİVERSİTESİ
AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ
AVRUPA HUKUKU ANABİLİM DALI

THE PROTECTION OF BIOMETRIC DATA IN THE ERA OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN EU LAW

YÜKSEK LİSANS TEZİ

FURKAN DARENDELİ

DANIŞMAN
Prof. Dr. MUSTAFA T. KARAYİĞİT

İSTANBUL- 2023

ABSTRACT

The aim of this study is to examine “the Protection of biometric data in the light of artificial intelligence in EU law” from a legal and historical developmental point of view. Today, artificial intelligence technology is developing at a great pace. Technological developments have advantages as well as disadvantages. In the light of artificial intelligence technology, the protection of biometric data should be effectively protected, especially within the scope of the fundamental rights and freedoms of individuals. Biometric data, which is the subject of the thesis, is quite sensitive by nature, as it uniquely identifies biological characteristics. Biometric data is regulated under the category of special personal data in European General Data Protection Regulation (GDPR). Initially, artificial intelligence and biometric systems were used by the EU for asylum and migration management. However, artificial intelligence systems that increasingly serve internal security and require the systematic collection of large amounts of biometric data constitute the area in which various biometric data breaches have occurred and still seem to occur in the future if no effective precautions are taken. There is no European legislation exclusive to biometric data yet. Currently, biometric data is limited in the GDPR, which is the basic regulation on personal data. In addition, there are provisions on biometric data in law enforcement and passport and border security regulations. (Law Enforcement Directive (LED), Council Regulation No 2252/2004, The Schengen Information System (SIS), The Visa Information System (VIS), The Entry-Exit System (EES).)

On the other hand, a draft proposal for artificial intelligence was published by the European Commission for the first time on 21 April 2021. This draft proposal is the first example of legislation on artificial intelligence. The draft proposal will be especially effective in terms of protecting biometric data with its risk-based approach and various protection methods in the EU borders. In this context, how the new draft proposal will be implemented in the future will shape the protection of biometric data. In this thesis, biometric data breaches and ways of their protection will be explained in the light of artificial intelligence technology and solutions will be offered on how to protect biometric data within the context of protection of fundamental rights and freedoms of individuals.

Key Words: Biometric Data, Protection of Biometric Data, Face Recognition Systems, Artificial Intelligence, EU Law, Artificial Intelligence Act, Iris Recognition Systems, Palm Recognition Systems, Fingerprint Recognition Systems.

ÖZET

Bu çalışmanın amacı, "AB hukukunda yapay zekâ çağında biyometrik verilerin korunması" konusunu hukuki ve tarihsel bir bakış açısıyla incelemektir. Günümüzde yapay zekâ teknolojisi büyük bir hızla gelişmektedir. Fakat bu Teknolojik gelişmelerin avantajları olduğu kadar dezavantajları da bulunmaktadır. Yapay zekâ teknolojisi ışığında biyometrik verilerin korunması, özellikle bireyin temel hak ve özgürlükleri kapsamında etkin bir şekilde korunmalıdır. Tezin konusu olan biyometrik veriler, biyolojik özellikleri benzersiz bir şekilde tanımladığı için doğası gereği oldukça hassastır. Biyometrik veriler GDPR'da özel kişisel veriler kategorisi altında düzenlenmektedir. Başlangıçta, AB tarafından sığınma ve göç yönetimi için yapay zekâ ve biyometrik sistemler kullanılmaktaydı. Giderek artan bir şekilde iç güvenliğe hizmet eden yapay zekâ sistemleri, büyük miktarlarda biyometrik verinin sistematik olarak toplanmasını gerektirirdi. Bu durum biyometrik veri ihlallerine yol açtı. Bu yüzden temel hak ve özgürlükleri ele alan bir biyometrik veri düzenlemesine ihtiyaç duyuldu. Henüz münhasıran biyometrik verilerle ilgili bir Avrupa mevzuatı bulunmamaktadır. Halihazırda biyometrik veriler, kişisel verilere ilişkin temel düzenleme olan Avrupa Genel Veri Koruma Tüzüğünde sınırlı olarak yer almaktadır. Ayrıca kolluk ve pasaport ve sınır güvenliği düzenlemelerinde biyometrik verilere ilişkin hükümler bulunmaktadır. (Kolluk Yönergesi (LED), 2252/2004 sayılı Konsey Tüzüğü, Schengen Bilgi Sistemi (SIS), Vize Bilgi Sistemi (VIS), Giriş-Çıkış Sistemi (EES).

Öte yandan, Avrupa Komisyonu tarafından ilk kez 21 Nisan 2021 tarihinde yapay zekâ için bir taslak teklif yayınlandı. Bu taslak teklifi, Dünya'da yapay zekâ ile ilgili mevzuatın ilk örneğidir. Taslak teklifi, özellikle AB sınırlarında risk temelli yaklaşımı, diğer koruma yöntemleri ile birlikte biyometrik verilerin korunması açısından oldukça etkili olacaktır. Bu kapsamda yeni taslak önerinin gelecekte nasıl uygulanacağı biyometrik verilerin korunmasını şekillendirecektir. Bu çalışmada, biyometrik veri ihlalleri ve korunma yolları yapay zekâ teknolojisi ışığında açıklanacak, temel hak ve özgürlükler kapsamında biyometrik verilerin nasıl korunacağı konusunda çözümler sunulacaktır.

Anahtar Kelimeler: Biyometrik Veriler, Biyometrik Verilerin Korunması, Yüz Tanıma Sistemleri, Yapay Zekâ, AB Hukuku, Yapay Zekâ Tüzüğü, İris Tanıma Sistemleri, Avuç İçi Tanıma Sistemleri, Parmak İzi Tanıma Sistemleri.

INDEX

ABSTRACT ..... i.
ÖZET iii
INDEX v
LIST OF TABLES viii
LIST OF FIGURES viii
ABBREVIATIONS ix
INTRODUCTION 1
I. PROTECTION OF BIOMETRIC DATA 4
A. IMPORTANCE OF BIOMETRIC DATA 4
B. BIOMETRIC DATA BREACHES AND SECURITY THREATS 6
C. PRIVACY AND BIOMETRIC DATA 9
II. ARTIFICIAL INTELLIGENCE 12
A. HISTORY OF ARTIFICIAL INTELLIGENCE 12
B. DEFINITION OF ARTIFICIAL INTELLIGENCE 13
C. WHY IS ARTIFICIAL INTELLIGENCE IMPORTANT? 16
D. FUTURE OF ARTIFICIAL INTELLIGENCE 18
E. INTERNATIONAL ARTIFICIAL INTELLIGENCE STRATEGIES 21
F.ARTIFICIAL INTELLIGENCE STRATEGY OF THE EU INSTITUTIONS 21
III. BIOMETRİC DATA 25
A. DEFINITION OF BIOMETRICS 25
B. DEFINITION OF BIOMETRIC DATA 26
C. HISTORY OF BIOMETRIC TECHNOLOGY 27
D. BIOMETRIC TECHNOLOGIES 31
E. BIOMETRIC TECHNOLOGY TYPES 32
1. Facial Recognition 32
2. Fingerprint Technology 34
3. Voice recognition/Verification 34
4. Iris 35
5. DNA 36
6. Keystroke 37
7. Signature 37

IV. LEGAL REGULATIONS.....39
A. INTERNATIONAL REGULATIONS.....39
1. Universal Declaration of Human Rights 39
2. European Convention on Human Rights.....40
B. EU LAW REGULATIONS.....43
1. EU Charter of Fundamental Rights.....43
2. General Data Protection Regulation.....48
2.1 Basic Principles of Processing Biometric Data 48
2.2 Lawfulness of Processing Personal Data.....51
2.2.1.Consent of The Individual Concerned.....51
2.2.2.Contractual Obligation.....51
2.2.3.Legal Obligation.....52
2.2.4.Vital Interests 52
2.2.5.Public Interest and Public Task.....52
2.2.6.Legitimate Interest.....53
2.3. Processing of Special Categories of Personal Data.....54
2.3.1.(9/A) Explicit Consent:.....54
2.3.2.(9/B) Employment, Social Security and Social Protection.....55
2.3.3.(9/C) Vital Interests 56
2.3.4.(9/D) Not-For-Profit Bodies:.....56
2.3.5.(9/E) Made Public by The Data Subject:.....56
2.3.6.(9/F) Legal Claims or Judicial Acts:.....57
2.3.7.(9/G) Reasons of Substantial Public Interest: 57
2.3.8.(9/H) Health or Social Care: 58
2.3.9.(9/I) Public Health:.....58
2.3.10.(9/J) Archiving, Research And Statistics:.....59
2.4. Processing of Biometric Data 59
2.5. Automated Individual Decision-Making, Including Profiling.....60
2.5.1.Use of Automated Decision-Making Systems in The Public Sector.....63
2.5.2.Use of Automated Decision-Making Systems in The Private Sector.....64
2.5.3.Use Of Automated Decision-Making Systems for Individuals.....65
3. Directive 95/46/EC.....66

4. Law Enforcement Directive (LED).....68
5. Council Regulation No 2252/2004.....69
6. Biometric Border Control Regulations.....71
7. EU Artificial Intelligence Act.....73
7.1. Biometric Techniques under AIA Proposal.....75
7.1.1.Real-Time and Post Remote Biometric Identification.....75
7.1.2.Biometric Categorisation.....76
7.1.3.Emotion Recognition.....77
7.2. Risk Based Approach.....78
7.2.1.Unacceptable Risk (Title II).....78
7.2.2.High Risk (Title III).....79
7.2.3. Transparency Risk (Title IV).....80
V. RECOMMENDATIONS ON THE NEED FOR THE PROTECTION OF BIOMETRIC DATA.....82
A. RECOMMENDATIONS FOR AI SYSTEM.....82
1. Recommendations for Artificial Intelligence Act.....82
1.1. Recommendations for Risk Based Approach.....82
1.1.1.Expanding The Scope of The Ban on The Use of Biometric Artificial Intelligence Systems In Public Spaces.....82
1.1.2.The Addition of Online Spaces Along with Public Spaces to The Scope of The Ban.....87
1.1.3.Recommendation of Banning Biometric Categorization.....83
1.1.4.Recommendations of Banning Emotion Recognition Systems.....84
1.1.5.Adding "Vulnerable Individuals" to Risk Groups In The Proposal.....85
1.1.6.Inclusion Of Biometric Categorization Systems In The High-Risk Group.....86
1.1.7.Expanding The Scope of Article 7 of The Proposal Regulating "Amendments to Annex III".....86
1.2. Recommendations for Definitions.....88
B. RECOMMENDATIONS FOR REGULATIONS ON BIOMETRIC DATA.....89
CONCLUSION.....92
BIBLIOGRAPHY.....95

LIST OF TABLES

Table1: direct problem and inverse problem types of biometrics…….8

Table2: Comparison of artificial intelligence and natural intelligence……18

Table3: Progression of several biometric technologies……32

Table4: Various characteristics of each type of biometric technology…….50

LIST OF FIGURES

Figures1: Risk-based approach of the artificial intelligence proposal……85

Figures2: Biometric techniques under the AIA Proposal's risk levels……85

Tüm bu süreçte benden desteklerini ve yardımlarını esirgemeyen Sevgili Ailem'e teşekkürlerimi bir borç bilirim.

ABBREVIATIONS

Art	Article
Art 29 WP	Article 29 Working Party
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
CJEU	Court of Justice of European Union
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Seal
EES	The Visa Information System
EU	European Union
EUCFR	EU Charter of Fundamental Rights
GDPR	General Data Protection Regulation
Ibid.	Above mentioned reference
LED	Law Enforcement Directive
OECD	Organization for Economic Co-operation and Development
op. cit.	Previously mentioned reference
n.d	No Date
para.	Paragraph
p.	Page
SIS	The Schengen Information System
TFEU	Treaty on Functioning of the European Union
UDHR	Universal Declaration of Human Rights
US	The United States of America
UN	The United Nation
VIS	The Visa Information System
WIPO	World Intellectual Property Organization

INTRODUCTION

With the development of technology, biometric data has become the most important trend of today. In addition to providing secure access to physical and logical assets, the increasing need for fraud reduction, fight against crime and criminals and security have made biometric data an important technology. This does not occur without possible legal consequences in the field of human rights. Unless legislators begin to consider the impact of biometrics technology on privacy, human rights, etc, biometric data will always be at risk of being misused and even abused.

In the first part of the thesis, “Importance of biometric data, Privacy and biometric data" will be examined in the light of why biometric data is important and why it should be protected.

On the other hand, Artificial intelligence is now playing a major role in transforming and powering industries all over the world. Artificial intelligence systems can process personal data. Because personal data can contribute to the data sets used to train machine learning systems, that is, to create their algorithmic models. In addition, artificial intelligence systems, from personal data; can generate information, make predictions and use the data obtained.[1] Thanks to artificial intelligence, all kinds of personal data (including biometric data and other sensitive data) can be used to analyze, predict and influence human behavior.[2] The global Artificial Intelligence (AI) market is estimated to reach a market value of 190.61 billion dollars in 2025. The Artificial intelligence annual growth rate between 2020 and 2027 is expected to be 33.2 %. Undoubtedly, this rapid growth has both advantages and disadvantages. Especially concerns about fundamental rights and freedoms are increasing. Moreover, one of the significant concerns is the relationship between artificial intelligence and biometric data. The world legislators are conducting various studies to resolve these concerns. The

[1] Gibson, A., Tessa, M., “Artificial Intelligence In The Public Sector – Inference And Collection” (2020), Available At:https://ovic.vic.gov.au/blog/artificial-intelligence-in-the-public-sector-inference-and-collection. Last Visited 19.03.2022

[2] Giovanni Sartor; Francesca Lagioia, (2020), *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*,European Parliament, 28.03.2022. P.1

draft proposal of artificial intelligence offered by the European Commission constitutes the first artificial intelligence regulation study in the world. In this context, the definition, history, importance of artificial intelligence, artificial intelligence strategies of the European Union and artificial intelligence in the future are examined in the second part.

Biometric methods[3] have existed for thousands of years. Potters from East Asia would put their fingerprints on the clay as it cured. During the Second World War, data, including biometric data, were collected from people by Hitler for the purpose of discrimination against Jews. For this purpose, many steps have been taken in the protection of personal data, including biometric data, after the Second World War with the importance of fundamental rights and freedoms in Europe. Biometric data is divided into two physiological and behavioral. Whereas the biometric data of the person such as fingerprint, iris, retina, palm, face, handprint, iris constitute the physiological biometric data; biometric data such as the person's gait and typing style constitute behavioral biometric data. In the third part of the thesis, the scope of biometric data is discussed. In this context definition of biometrics and biometric data, history of biometric technology, Biometric Technologies, Biometric technology types are mentioned.

In the fourth part of the thesis, the regulations regarding artificial intelligence and biometric data in the EU legal system will be discussed. "Directive 95/46/EC" is the first legal regulation in the EU regarding personal data. GDPR entered into force on 25 May 2018. Although the subject of the study is the protection of biometric data in the light of artificial intelligence technology, other regulations regarding biometric data will also be given limited space. While the subject of protection of biometric data in the light of artificial intelligence technology is discussed, the provisions related to biometric data of the Artificial intelligence draft proposal, which is still in the proposal stage, will be discussed. In addition, the problems related to the subject will be stated and recommendations will be presented. While examining biometric data in the thesis, the following regulations will be mentioned. (Universal Declaration of Human Rights, EU

[3] Biometric methods generally refer to the use of methods to identify a person based on some aspect of their biology.

Charter of Fundamental Rights, European Convention on Human Rights, GDPR, (Law Enforcement Directive (LED), Council Regulation No 2252/2004, The Schengen Information System (SIS), The Visa Information System (VIS), The Entry-Exit System (EES).)

The last section provides recommendations from various research and articles conducted in the EU on the matter of how to protect biometric data in the field of artificial intelligence.

I. PROTECTION OF BIOMETRIC DATA

A. IMPORTANCE OF BIOMETRIC DATA

Biometric methods have existed for thousands of years. During the Egyptian civilization period, Egyptian traders were identified by physical characteristics such as height, weight, eye color, hair color.[4]

At this time, biometric data, which is used successfully and efficiently in scientific research, is an important element of forensic science and a valuable element of access control systems.[5] In addition to providing secure access to physical and logical assets, the increasing need for reducing fraud, fighting against crime and criminals have made biometric data an important technology.[6]

According to the global mobile consumer survey conducted by Deloitte in the US in 2018, regular biometric use for many years has reached a critical level. The survey result showed that 63% of people who make banking transactions from their smartphones and 67% of those who transfer money online from a mobile device use at least one type of biometric authentication.[7]

According to the 2019 Verizon Data Breach Investigations Report,[8] the breach rate of account passwords was 81%. With the more widespread use of biometric data, it

[4] Down, M. P., & Sands, R. J. (2004). "Biometrics: An overview of the technology, challenges and control considerations." Information Systems Control Journal, *4*, 53-56.P.53

[5] Article 29 Data Protection Working Party, (2012) *Opinion 3/2012 On Developments In Biometric Technologies*, P.2

[6]Danny Thakkar, "Importance of Biometric Fingerprinting Technology: Does Your Organization Really Need It? This Will Help You Decide!", (2020), Available At: https://www.bayometric.com/importance-of-biometric-fingerprinting-technology. Last Visited 20.03.2022

[7]Mitek Systems, Inc is a software company that specializes in digital identity verification and mobile image processing using artificial intelligence. See. Mitek systems, "Looking ahead: 7 reasons why biometric security is important for digital identity", (2019), Available At: https://www.miteksystems.com/blog/looking-ahead-7-reasons-why-biometric-security-is-important-for-digital-identity. Last Visited 21.03.2022

[8]See. For other staticks: https://www.verizon.com/business/resources/reports/dbir. Last Visited 21.03.2022

will reduce hacking and prevent password theft. Because a person's biometric data is unique and cannot be copied.[9]

According to miteksystems, seven reasons are given for the importance of biometric data. The first is that biometric data creates a special link between a person and a data record. Biometric data is unique and cannot be copied, so the password is difficult to obtain. Secondly, thanks to biometric data, fraudsters' efforts to create multiple fake digital identities are blocked. Thirdly, Biometric data cannot be changed. Since fingerprints or keyboard patterns cannot be transferred, biometric data is particularly effective at protecting sensitive information such as financial and healthcare records. Fourthly, thanks to the digital identity protection of biometric data, banks aim to increase their online product offerings by opening up their digital infrastructure to third-party fintech providers. Fifthly, biometric data provides convenience and security. Users forget passwords and pins. Consumers lose their smart cards or tokens. However, fingerprints, unlike regular passwords, are always present and fixed. Sixthly, the innate biometry does not change. A haircut and cosmetic surgery can change the contours of the face, On the other hand the innate biological data of the human beings does not change. Lastly, the stolen biometric data may be more difficult to use than normal encryption methods. The effort required to hack a database, steal biometric files, and then create useful copies to gain access to mobile devices or online accounts is much more difficult for identity thieves.[10]

In addition to the above report of miteksystems, the following points can be added to the importance of the use of biometric data. In methods such as password verification, people can easily forget their passwords, but there is no need for this as Biometric data is precise. Biometric identification can be completed in a very short time and uniformly. Furthermore, biometric data is easy to use, requires little storage space and takes about 5 seconds to store.[11]

[9]Mitek Systems, op.cit.

[10] Mitek Systems, op.cit.

[11] Phadke, S. (2013). "The Importance of a Biometric Authentication System". The SIJ Transactions on Computer Science Engineering & its applications, 1 (4), 128-132. P. 131

As a result, biometric data is very important for both companies and countries. Companies especially prefer to use biometric data as it is difficult to fake. This makes it useful for preventing fraud. For example, many banks and financial institutions use audio tracks to identify their customers. When speaking to a customer service representative, a unique soundtrack is created from more than 100 different physical and behavioral characteristics, such as accent, the shape of your mouth, and vocal tract. This voice ID is then securely stored as a mathematical equation for future verification of the caller's identity. At the same time, finance apps create "voice biometric blacklists" for credit card fraudsters.[12]

Biometric data is accordingly more secure than other data in terms of security and many details. In particular, facial recognition technologies with artificial intelligence have been widely used in countries for security purposes in recent years. According to a market report by Credence Research, the global biometric technology market is expected to reach $34.5 billion by 2022.[13] According to the report, governments around the world are keen to use biometric technologies for access authorization, identification and verification, e-passport management and national border control work. The Asia-Pacific region is expected to have the fastest growth rate, with increasing adoption of biometric technologies in India and China.[14]

B. BIOMETRIC DATA BREACHES AND SECURITY THREATS

Undoubtedly, biometrics have many disadvantages as well as abovementioned advantages. These disadvantages can lead to major data breaches and grievances. The biggest concern with biometric data is its immutability. While it is an advantage that people's biometric data (for instance fingerprints, face, iris and voice) cannot be

[12]Zapproved, "Importance of Biometric Data Privacy", (2019), Available At: https://zapproved.com/blog/just-how-important-is-it-to-protect-the-privacy-of-biometric-data. Last Visited 23.08.2022

[13] See. Global ID Summit, "Identity in a Digital Age:A Glance At The Countries Leading the Revolution," (2018), Available At: https://www.idga.org/events-globalidsummit/downloads/sponsorship-information-mt. Last Visited 23.08.2022

[14] Joe Bosso, "The dangers of government use of biometric data",(2021), Available At: https://blog.avast.com/government-use-of-biometric-data-avast. Last Visited 25.03.2022

changed, it can also be a disadvantage. If these biometric data are hacked or stolen, permanent problems may arise since the stolen biometric data cannot be changed.[15]

In addition, the fact that the biometric data collected falls into the hands of criminal organizations and terrorist organizations is another concern. The US used a biometric data collection program during her stay in Afghanistan. The US military had used devices to capture fingerprints, iris scans and facial images to build a database of the Afghan population to help fight terrorists. This is one of the biggest concerns stemming from the US withdrawal from Afghanistan. Because this Handheld Interagency Identification Equipment, called "HIIDE", is now in the hands of the Taliban and it is feared that this information will now be used to track down Afghan citizens who are helping the US and its allies.[16]

Another major concern is biometric data being hacked. Norton, an anti-malware software company, stated that any collection of data could eventually be hacked. So how can these biometric data breaches appear in daily life? For example, a cybercriminal might try to use a person's biometric data, for example with his/her fingerprint, in a building he/she legitimately uses to gain entry. A person's biometric data probably won't help cybercriminals open a credit account in his/her name. But biometric information has other applications as well. For example, in some places it is used to board a plane.[17]

On August 14, 2019, a major data breach report called "BioStar 2, a Suprema-based security platform" was released. According to this report, South Korea-based Suprema announced that its company learned that BioStar 2 customer user data were accessed without permission for a limited time by third-party security researchers. This data included biometric data of people, such as fingerprint and facial recognition data. The number of data breached included twenty-eight million records from more than one

[15] Zapproved, op.cit.

[16] Bosso, J., op.cit.

[17] Symanovich, S." Biometric data breach: Database exposes fingerprints, facial recognition data of 1 million people", (n.d)., Available At: https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html. Last Visited 01.04.2022

million people. This situation has increased the concerns about the biometric data breach.[18]

Once biometric data is stolen, there is nothing you can do to make it safe again. Of course, if your fingerprint is stolen, you can always use another finger, but you can only do it 10 times. On the other hand, when someone gets your fingerprint data, it is possible to print a copy using conductive ink that can fool biometric scanners. There are also examples of researchers fooling audio scanners with audio conversion tools, iris scanners with replica images, and photo- or even 3D-printed face scanners.[19]

So, what can be done to make biometric security stronger? The easiest way is with passwords. It is common practice to store passwords by first encrypting or "hashing" them. [20] Therefore, this method can be used to make biometric data more secure. Another way to make biometric systems more secure is to use the blockchain technology used by cryptocurrencies like Bitcoin. Thanks to blockchain technology, personal data can be stored on multiple computers around the world in a distributed location protected by cryptography. However, even these measures may not be enough to keep biometric systems secure forever.[21]

DIRECT PROBLEM	INVERSE PROBLEM
Signature identification	Signature forgery
Handwriting character recognition	Handwritten text forgery
face recognition	Face reconstruction and mimics animation

[18] BBC, "Biostar 2: Suprema plays down fingerprint leak reports",(21.08.2019), Available At: https://www.bbc.com/news/technology-49418931. Last Visited 02.04.2022

[19] Hewage, Chaminda, “Stolen Fingerprints Could Spell The End Of Biometric Security”,(2019), Available At: https://theconversation.com/stolen-fingerprints-could-spell-the-end-of-biometric-security-heres-how-to-save-it-122001. Last Visited02.04.2022

[20] Ibid.,

[21] Ibid.,

Voice identification and speech recognition	Voice and speech synthesis
Iris and retina identification	Iris and retina image synthesis
Fingerprint identification	Fingerprint imitation
hand geometry identification	Hand geometry imitation
Infrared identification	infrared image reconstruction
Gait identification	Gait modeling
Ear identification	Ear-print imitation

Table 1 taken from the source mentioned in the footnote shows direct and inverse problem types of biometrics.[22]

C. BIOMETRIC DATA AND PRIVACY

Another important concern is that biometric systems violate people's privacy. Privacy is a fundamental right on which many other human rights are built, necessary for the protection of autonomy and human dignity.[23]

The use of biometric data raises questions about a person's ability to decide what information about themselves is willing to make available to others, which inevitably affects that person's right to privacy.[24] Regarding privacy concerns, the following are important: Firstly, with regard to the creation of large centralized databases, in the doctrine, there are concerns about how this biometric data, which is private and personal, can be used without the consent of the people. Secondly, with regard to covert collection, it is the confidential collection and use of biometric data without the consent of the person. For example, facial information can be easily

[22] Wang, P. S., & Yanushkevich, S. N. *op. cit.*P.250

[23]Privacy International," what is privacy" , (n.d), Available At: https://privacyinternational.org/explainer/56/what-privacy. Last Visited 03.04.2022

[24] Ebelogu, C. & Amujo, O. & Adelaiye, O. & Silas, F. (2019). "Privacy Concerns in Biometrics", IEEE-SEM, Volume 10, Issue 7, July-2019 ISSN 2320-9151,(45-52), P.46

captured and used without people realizing that they are being photographed. Thirdly, with regard to cross matching, for instance, when police choose to cross match using fingerprints during a criminal investigation, it can create a danger to innocent people. Innocent people have the right to live in anonymity and to be free from surveillance. These rights should not be violated. Fourthly, with regard to secondary information, another privacy concern is related to secondary information that may be found in biometric features that were originally collected for a different primary purpose. This may cause concern with privacy. For example, iris images used in authentication systems can provide additional information about a person's health.[25]

It should be emphasized that another important concern is the production of fake content based on biometric data. One of the most recent examples of this is DeepFake. A new era has been entered with the artificial intelligence-based video-audio processing technology known as 'Deepfake'. Because, with Deepfake, it is now easier for ordinary users to pretend that a person has said something they have never said or gone somewhere they have never been.[26]

The Deepfake received attention after it was discovered that pornographic films ostensibly starring Hollywood stars in 2017 were deepfakes. Many deepfakes of well-known politicians, artists, and statesmen began to circulate later.[27]

Again, in a video circulating on the internet, a girl made a deep fake video of her grandfather and sent it to her mother as a birthday present for her mother. But the grandfather died in a car accident when the mother was 16 years old. The aim of the girl, who re-enacted the video of her deceased grandfather and sent it to her mother, is to make her mother happy. But the girl's mother was shocked, and she was offended with her daughter for a while.

Deepfake is a technology that can be used to manipulate people easily. Elections may be affected by deepfake technology. There may even be wars in the

[25] Ibid..,, P.48-49
[26] Temir, E. (2020). Deepfake: new era in the age of disinformation & end of reliable journalism. Selçuk İletişim, 13(2), 1009-1024. P.1009
[27] Ibid.,. P.1019

future because of this technology. However, Deepfake can be used for good purposes as well as its scary aspects. A dead actor can be played in a new movie thanks to deepfake.

Another important concern is the use of automated decisions based on artificial intelligence algorithms in Biometric data. For example, Google's face recognition algorithm inadvertently identified black people as gorillas.[28] In 2016, ProPublica reported that an artificial intelligence tool used in courtrooms across the United States to predict future crimes, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), was biased against Black defendants.[29]

Biometric methods used by private companies and government agencies led to privacy violations. GDPR and other above-mentioned regulations were insufficient in this regard, the risk-based approach brought together with the new Artificial intelligence Regulation proposal prepared by the EU Commission will eliminate some privacy concerns in this regard.[30] Inadequate regulation of biometric data can lead to malicious activity, profiling, surveillance and discrimination.[31] As a result, there should be an effective regulation in place to address concerns against biometric data breaches.[32]

[28] Hacker, P. (2018). "Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law." Common Market Law Review, 55(4). Available at SSRN: https://ssrn.com/abstract=3164973, 1143-1186. P.1145

[29] Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, ProPublica, " Macnine Bias", (2016), Available At: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Last Visited 30.08.2022

[30] Natalia Mesa, "Can the criminal justice system's artificial intelligence ever be truly fair?", (2021), Available At: https://massivesci.com/articles/machine-learning-compas-racism-policing-fairness. Last Visited 20.03.2022

[31]Carpenter, D., McLeod, A., Hicks,(2018) C, (2018= Privacy and biometrics: An empirical examination of employee concerns. Inf Syst Front 20, 91–110 Available At: https://doi.org/10.1007/s10796-016-9667-5. Last Visited 20.03.2022

[32] In this context, "Recommendations for Artificial Intelligence System Using Biometric Data" is given below.

II. ARTIFICIAL INTELLIGENCE

A. HISTORY OF ARTIFICIAL INTELLIGENCE

The word ‘’Artificial intelligence’’ was first used by John McCarthy (computer scientist at Stanford) at the Dartmouth conference in 1955, since then the word artificial intelligence has taken its place in world literature.

By the 1960s, there have been significant advances in the field of artificial intelligence such as symbolic integrations, word puzzles, chess-playing programs, and General Problem Solver (CPR).[33]

In 1970 Marvin Minsky stated in Life Magazine that a machine with the general intelligence of the average person could be developed in three to eight years.[34] This was a very important claim for that time. Because artificial intelligence technology was in its infancy. In the beginning, important scientists such as Marvin Minsky were very optimistic that the development of artificial intelligence would progress very quickly.[35] However, the progress of artificial intelligence decelerated between 1974 and 1980 as a result of the writing of reports criticizing developments in the field of artificial intelligence.[36]

By the 1980s, the American artificial intelligence association was founded and started its work. This was an important institution for those who would work in the field of artificial intelligence for years to come.

Deep Blue, produced by IBM in 1997, became the first computer chess system to beat world chess champion Garry Kasparov. With the increase in investments made by countries in artificial intelligence with the millennium age, the development of artificial intelligence technology has accelerated.

---

[33] Hallevy, G. (2013). *When robots kill artificial intelligence under criminal law*. UPNE. P.2-3

[34] Haenlein, M., & Kaplan, A. (2019). “A brief history of artificial intelligence: On the past, present, and future of artificial intelligence.” California management review, 61(4), 5-14. P.8

[35]Benjamin Kuipers, " Progress in AI" (2019, Avaialble At: https://web.eecs.umich.edu/~kuipers/opinions/AI-progress.html. Last Visited 30.08.2022

[36]Tanya Lewis, A Brief History of Artificial Intelligence, (2014), Available At: https://www.livescience.com/49007-history-of-artificial-intelligence.html . Last Visited 30.08.2022

In 2000, Honda's Asimo robot, which can work as a waiter and walk fast, was introduced. In 2009, Google began developing self-driving vehicles. In 2011, the speech machine named Watson, manufactured by IBM, defeated the language champions. In 2011, Apple introduced "Siri", an intelligent personal assistant and information explorer. In 2014, Facebook's new technology, the new face recognition success rate was announced as 97.25%. In 2017, University of Nottingham scientists developed an artificial intelligence system that scans routine medical data to predict which patients will have a stroke or heart attack within 10 years. [37]

B. DEFINITION AND LEGAL STATUS OF ARTIFICIAL INTELLIGENCE

Today, there is no precise definition of intelligence. However, the definition of intelligence can be said as one's processes of reasoning, thinking, understanding, judging and drawing conclusions from them. The intelligence, which is described as human thinking and comprehension, can be imitated through certain software and various ways. Colo describes that artificial intelligence can best be understood as a set of techniques aimed at approximating some aspects of human or animal cognition using machines.[38]

Human beings are inherently thinking beings. However, can machines think? This is a question that has been going on for 100 years. This question was first addressed by Alan Turing in 1950. According to Turing, the question "Can machines think?" should begin with the definition of the terms "machine" and "thinking". While analyzing the question, Turing tries to find an answer with the method he defines as "the imitation game".[39] There are 3 terminals: the interrogator, a female user and a male user. The interrogator queries both users in turn. In the imitation game the interrogator has to find out who is male and who is female. But according to the rule of the game, the man

[37] Karla Lant,"Confirmed: Ai Can Predict Heart Attacks And Strokes More Accurately Than Doctors", (2017), Available At: https://futurism.com/neoscope/confirmed-ai-can-predict-heart-attacks-and-strokes-more-accurately-than-doctors . Last Visited 30.08.2022

[38] Calo, R. (2017). "Artificial intelligence policy: a primer and roadmap." *UCDL Rev.*, *51*, 399-475,p.404

[39] Turing, A. M., & Haugeland, J. (1950). "Computing machinery and intelligence", Cambridge, MA: MIT Press. (pp. 29-56). P.67

will try to convince the interrogator that he is a woman. In the second stage, one of the users is still a human and the other is a computer this time. The interrogator is being tested by being asked various questions. If the interrogator cannot distinguish between man and machine, the machine passes the test. In a nutshell, it can be defined as a test system based on a better understanding of the distinction between humans and machines. This test, put forward by Turing, has been considered the philosophy and foundation of artificial intelligence since 1950.

Based on the Turing test, the definition of artificial intelligence can be briefly defined as imitating intelligent human behavior. According to the definition of artificial intelligence made by the European Parliament, "Artificial intelligence refers to the ability of a machine to demonstrate human abilities, including reasoning, learning, planning and creativity. Artificial intelligence allows technical systems to perceive their environment, take care of what they perceive, solve problems and take action in order to achieve a specific goal".[40]

In summary, artificial intelligence is a technology that allows machines to demonstrate intelligence similar to that of humans or animals. Initially, Artificial Intelligence was limited to memorizing data and producing results; however, it has evolved into much more, with machines performing tasks such as speech recognition, object recognition, text translation, and much more.[41] In short, the definition of artificial intelligence can be summarized in four categories as follows: systems that think like people, systems that act like people, systems that think rationally, systems that act rationally.[42]

However, artificial intelligence technologies have already taken over our lives in recent years. As they become a main force in the world, the area is shifting from

[40] European Parliament, "What is artificial intelligence and how is it used?", September 4, 2020, Available At:www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used. (last visited 01.01.2021)

[41]Signalsvc, "Role of Artificial Intelligence and Machine Learning in Speech Recognition", (2021), AvailableAt:https://signalscv.com/2021/07/role-of-artificial-intelligence-and-machine-learning-in-speech-recognition, Last Visited 10.10.2021

[42] Kok, J. N., Boers, E. J., Kosters, W. A., Van der Putten, P., & Poel, M. (2009). *Artificial intelligence: definition, trends, techniques, and cases*. EOLSS Publications, 1, 270-299. P.1

simply building systems that are intelligent to building intelligent systems that are human-aware and trustworthy.[43]A prime example of this is machine learning. Machine learning is part of artificial intelligence. Without being explicitly programmed, machine learning algorithms create a model based on sample data, known as training data, to make predictions and make decisions.[44] An algorithm serves as the starting point for systems that have the mechanics required for machine learning. Without an algorithm, there would be nowhere to begin the programming process. That is, algorithms are step-by-step instructions that guide the computer complete a calculation.[45]

It is a matter of great debate whether artificial intelligence systems have criminal and legal responsibility as a result of their actions. First of all, it is necessary to determine the legal status of AI systems in the current legal order. For this, some views are included in the doctrine. These; These are the views that attribute "personality" to AI and the views that AI cannot be seen as "person". [46]

Views that attribute personality to AI; can be said as slavery views, natural person views, legal person views, electronic persons views. Those who defend the views of slavery describe AI systems as the slaves of people. The main problem here is that the concept of slavery has been abandoned in a way that cannot be used again in the contemporary legal system. Therefore, it is problematic.[47] Another view is legal personality. According to this view, the legal status of artificial intelligence is legal personality. In 2020, it regulated a resolution with recommendations to the Commission on a civil liability regime for AI, in which it expressly states; technically, artificial intelligence systems could be the direct or indirect source of harm or damage.

[43] Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G& Teller, A. (2016). *Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence*. Stanford University. P.14

[44] Koza, J. R., Bennett, F. H., Andre, D., & Keane, M. A. (1996). "Automated design of both the topology and sizing of analog electrical circuits using genetic programming. In Artificial intelligence in design*",* (pp. 151-170), Springer, Dordrecht. P:154

[45]Rockcontentwriter," Artificial Intelligence Algorithm: Everything You Need To Know About It ",(2021), Available at: https://rockcontent.com/blog/artificial-intelligence-algorithm/%20efficiently, Last Visited (22.08.2022)

[46] Darama, S "Yapay Zekanin Hukuki Statüsü Hakkindaki Görüşler Üzerine Değerlendirme",(2021), Avaiable At: https://www.ozgunlaw.com/makaleler/yapay-zekanin-hukuki-statusu-hakkindaki-gorusler-uzerine-degerlendirme-744. Last Visited 19.02.2023

[47]Kaya F , "Yapay Zeka Ve Yapay Zekanin Hukuki Kişiliği Meselesi", (2021), Available At: http://blog.ilem.org.tr/yapay-zeka-ve-yapay-zekanin-hukuki-kisiligi-meselesi. Last Visited 21.02.2023

However, it is almost always the result of someone creating, deploying, or tampering with systems. So, there is an outside intervention. Therefore, it is concluded in the report that it is not necessary to give legal personality to artificial intelligence systems.[48] The electronic personhood model recommended by the European Parliament in the euRobotics report is considered to be the most comprehensive personality model among existing models. The electronic personality model is thought to bring an important innovation to artificial intelligence technology in terms of legal responsibility.[49] Consequently, there is a need for a system that focuses on a piecemeal approach in areas of law affected by AI, without establishing any special status for AI.[50]

C. THE IMPORTANCE OF ARTIFICIAL INTELLIGENCE

So why is artificial intelligence so important? The use of the word artificial intelligence in social, written and visual media is increasing. In a study by Bloomberg, the use of the word artificial intelligence in the media has increased approximately 40 times in the last 10 years.[51]

Artificial intelligence technology started with science fiction novels and films, such as the novel "Frankenstein" written by Mary Shelley in 1818, "The Terminator" directed by James Cameron in 1984, "matrix", released in the 1990s, the "I robot" released in the 2000s and the film "Her", released in the 2010s, which have increased the popularity of artificial intelligence. However, nowadays, it constitutes an essential point in our lives. So, what is the increasing importance of artificial intelligence in recent years? To find the answer to this question, first of all, it is necessary to examine the differences between artificial intelligence and intelligence.

---

[48]European Parliament , "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence",(2020), Available At: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html. Last Visited 21.02.2023

[49] Şahin, G. Ö., & Şahin, Ç., (2022) "Yapay Zekali Varliklara Elektronik Kişilik Modeli Taninmasina İlişkin Eurobotics Raporu Ve Fikri Mülkiyet Sorunu Bağlaminda Meseleye Yaklaşim". İnönü Üniversitesi Hukuk Fakültesi Dergisi, 13(1), 110-128. P.110

[50]Simonart, V, "Artificial Intelligence And Legal Personal", Available At: https://liedekerke.com/en/insights/artificial-intelligence-and-legal-personality. Last Visited 21.02.2023

[51] Bloomberg Intelligence, "Business-focus on artificial intelligence rising",(2017), 11.10.2021 Available At: https://www.bloomberg.com/professional/blog/business-focus-artificial-intelligence-rising-2/,Last Visited

Artificial intelligence, which cannot be lost or forgotten as long as computer systems and programs do not change, is rather permanent, whereas natural intelligence may change over time as employees change places, or people with natural intelligence may forget the information they have.

Artificial intelligence can be easily copied from one computer to another and extended to people, whereas in the case of natural intelligence, transferring a specialty from one person to another requires a long apprenticeship and even if this is achieved, the specialty cannot be fully transferred to another person. Artificial intelligence is cheaper compared to natural intelligence. That is why, the purchase and use of computers can be provided much cheaper than human use in most areas.[52] Artificial intelligence as a computer technology is more consistent, whereas natural intelligence is unstable, variable and irregular. This is due to differences between the nature of the human being and the possessor of natural intelligence. Artificial intelligence can be documented by monitoring the system's activities, whereas natural intelligence is difficult to reproduce. Artificial intelligence is faster. While one doctor can make a diagnosis in ~10 minutes, artificial intelligence system can make a million for the same time.[53]

In some cases, there are situations where natural intelligence is still superior to artificial intelligence. Natural intelligence which provides people with the ability to use and benefit from experiences learned through their senses is more creative.[54] Most artificial intelligence systems however work with inputs. Briefly, these comparisons can be shown in the table as follows:

[52] Feyzioğlu, G, (2021*) Gelişen Teknolojiler ve Hukuk II – Dijitalleşen Dünyada Yapay Zeka*:, Onikilevha Yayıncılık P. (3)

[53]Dezhic,E, "Artificial vs Natural Intelligence", (2017), Available At: https://becominghuman.ai/artificial-vs-natural-intelligence-82ccd056b212 , Last Visited 22.08.2022

[54] Bozüyük, T., Yağci, C., Gökçe, İ., & Akar G. "Yapay Zeka Teknolojilerinin Endüstrideki Uygulamalari",(2005), Available At: www.teknoloji.isparta.edu.tr/assets/uploads/sites/134/files/is-yeri-egitimi-6-hafta-odev-notu-08052020.pdf, P.9, Last Visited 25.10.2021

Artificial Intelligence	Natural Intelligence
Permanent	Easily Forgotten
Can Be Easily Copied	It Is Difficult To Transfer.
More Consistent	Unstable, Variable And Irregular
Cheaper	More Costly
Can Be Documented	Can't Be Documented Easily
It Works with Inputs.	More Creative

Table 2. Comparison of artificial intelligence with natural intelligence

Artificial intelligence is used in many fields today. Artificial intelligence is used in the fields of cyber security and defense industry, voice assistants, language translations, navigation, social security, e-commerce, robots, smart home technologies, home appliances, medicine and health, automotive, etc. Although artificial intelligence is used in various sectors. With the further development of artificial intelligence technology in the future, the importance of artificial intelligence will undoubtedly increase in terms of individuals, companies and governments. Artificial intelligence is reliable and cheaper when taken into account in the industrial dimension.

D. THE FUTURE OF ARTIFICIAL INTELLIGENCE

One of the most frequently asked questions today is "at what point will artificial intelligence be in the future". Another question is "What will be the future importance of artificial intelligence"? Tim Urban, the founder of the popular Web site "Wait but why", answers this question as follows: "Artificial intelligence (AI) is not just an important topic, but by far the most important aspect of our future."[55]

[55] Urban, T., "The AI Revolution: The Road to Superintelligence.", (2015, June 22). Available At: https://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html, Last Visited 08.11.2021

Artificial intelligence today is one of the most emphasized topics for countries, companies, people and scientists. The future position of artificial intelligence, which still has a limited development today, is a matter of curiosity. Throughout history, there have been various predictions about the development of artificial intelligence. When the general thoughts of scientists on this subject are examined, it is observed that they are divided into two as positive and negative.

One of the negative views is that artificial intelligence still has limited use**.** According to Dr. Ó hÉigeartaigh, even a dog does not have intelligence with cognitive abilities. He says that those who are able to perform actions in the world, such as learning, adapting, thinking and doing many other things, are still only biological beings.[56] Indeed, although hÉigeartaigh's thought is exaggerated about the use of artificial intelligence, it can be said that today's use of artificial intelligence is limited considering today's technology.

Another negative opinion about the future of artificial intelligence is that artificial intelligence will pose a danger to the future. Physicist Stephen Hawking and founder of Tesla and SpaceX argue that artificial intelligence can be potentially very dangerous. Elon Musk compares the danger dimension of artificial intelligence to the danger of North Korea. Microsoft founder Bill Gates also believes there is reason to be wary of artificial intelligence's danger to the future, but he believes the good can outweigh the bad if managed correctly. So why do so many important people believe how dangerous artificial intelligence can be? There are many reasons for this.[57] First, the example of "Social manipulation" can be given. Social media is very effective in target marketing due to its autonomous supported algorithms. During the 2016 US presidential election, Cambridge Analytica tried to influence others using data from 50 million Facebook users. Therefore, an investigation was opened against Cambridge Analytica.

[56] Britishcouncil, "What will be our future in a world of AI", Available At: https://www.britishcouncil.org.tr/en/programmes/education/cubed/AI. Last Visited 15.08.2022

[57]Marr, B. “Is Artificial Intelligence Dangerous? 6 AI Risks Everyone Should Know About.”, (2018, December 19), Available At: www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know-about/?sh=1aec3a572404. Last Visited 15.11.2021,

On the other hand, there are a lot of positive opinions about the future of artificial intelligence. According to venture capitalist Dr. Kai-Fu Lee, 2018 Artificial intelligence is going to change the world more than anything in the history of mankind. More than electricity.[58] Google CEO Sundar Pichai said artificial intelligence will have a greater impact on the world than some of the most common innovations in history.[59] This opinion is quite important. Because Google is one of the most invested companies in artificial intelligence in the world.

By looking at recent years it can be seen that the development of artificial intelligence types has accelerated. People have begun to encounter countless examples of artificial intelligence. We now live in a world where search engines, online shopping portals, the internet of things, 3D printers, driverless vehicles, smart homes and offices, augmented reality applications, chatbots, personal digital assistants and robot surgeons. The list of these fields of usage is increasing day by day.[60]

Since a great degree of sensitive information is at stake, biometric data protection is not only a legal necessity but also imperative to protecting and maintaining countries and businesses reputation. Countries and businesses regularly store biometric data about clients, staff, business partners and more. Since organizations look toward the future of data privacy and data protection regulations, robust cybersecurity solutions are necessary. Undoubtedly, governments and businesses will focus on artificial intelligence using biometric data privacy to ensure the protection of their citizen employees, clients and organization. [61]

---

[58] Thomas, M. "The Future of AI: How Artificial Intelligence Will Change the World.", (2021, January 21). Available At: https://builtin.com/artificial-intelligence/artificial-intelligence-future. Last Visited 18.11.2021,

[59]Clifford, C, "Google CEO: A.I. is more important than fire or electricity.", (2018, February 1), Available At:https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html. Last Visited 18.11.2021

[60] BAK, B (2018). "Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk". Türkiye Adalet Akademisi Dergisi, (35), 211-232. p.212

[61] Valerie Rivera,"What the Future of Data Protection Means for Your Business", (januayr 5 2022), Available At: https://www.insight.com/en_US/content-and-resources/2022/the-future-of-data-protection.html. Last Visited 22.08.2022

E. INTERNATIONAL ARTIFICIAL INTELLIGENCE STRATEGIES

In recent years, the investment of countries in artificial intelligence has increased. Especially with COVID 19, the use of artificial intelligence has accelerated and intensified the digitalization trend that started before the pandemic. Global spending on artificial intelligence by countries is projected to double between 2020-2024. Spending on artificial intelligence by countries, most of whom are G20 member states, is expected to grow from US$50 billion in 2020 to over US$110 billion in 2024.[62]

Countries and international organizations have created their artificial intelligence strategies to increase future global competitiveness which also affect the future of humanity. National artificial intelligence strategies were first published in 2017. As of December 2020, thirty-two countries have completed and published their artificial intelligence strategies. In addition, twenty-two countries are still developing their artificial intelligence strategies.[63] It is not surprising that the Far East countries, which have invested heavily in artificial intelligence technologies, have announced their national strategies. The remarkable point here is that no steps were taken by the European Union institutions and member states in the beginning until 2018.

F. ARTIFICIAL INTELLIGENCE STRATEGY OF THE EU INSTITUTIONS

In the White Paper that "European Approach to Excellence and Trust" was published by the European Commission, it is mentioned why the artificial intelligence strategy is necessary. The Commission underlined that there is a need for a robust European approach based on the European artificial intelligence strategy. Secondly, it states that the EU should act as a whole by addressing the opportunities and challenges of artificial intelligence. According to the EU Commission, it is important to maintain

[62] OECD, *Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers*, (2021), Available At: https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf, Last Visited 21.11.2021

[63] Stanford University, *CHAPTER 7: AI Policy and National Strategies* , (2021), Available At: https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf. Last Visited 22.11.2021

the EU's technological leadership and to make new technologies available to the entire the European Union and important steps should be taken for this purpose.[64] In this context, the following processes have taken place within the scope of artificial intelligence in the EU.

In October 2017, the Council asked the Commission to present its artificial intelligence strategy. A strategy paper was published in the study carried out by the European Commission on April 10, 2018.[65] In the published article, the following strategies have been reached in particular: Increasing Europe's technology and industrial capacity with artificial intelligence to provide better access to public sector data. By increasing the development of artificial intelligence, to establish innovative business models and create new qualified jobs development.[66]

In addition, some committees working within the EU commission work on Artificial Intelligence and publish reports. For example, it aimed to create the "artificial intelligence ecosystem" of the Committee on the Environment, Public Health and Food Safety.[67]

On 8 June 2018, the "High Level Expert Group" was established by the EU Commission. "Ethics Guidelines for Trustworthy AI"[68] has been published by the "High Level Expert Group" on April 8, 2018, for the development of artificial intelligence technologies in accordance with ethics and law. "High Level Expert Group" made another important report on July 17, 2020. In this context, the reliability of artificial

[64] See. European Commission. *White Paper on Artificial Intelligence: A European approach to excellence and trust,* (2020*),* Available At: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Last Visited 25.11.2021

[65] Çetin S., (2021*) Gelişen Teknolojiler ve Hukuk II – Yapay Zeka: Yapay Zeka Stratejileri ve Hukuk*:, Onikilevha Yayıncılık P. (21-75)

[66]See. Jrc Science Hub Community, *EU Declaration on Cooperation on Artificial Intelligence,* (2018*), Available* At: https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence . Last Visited:22.08.2022

[67] European Parliament, *Motion For A European Parliament Resolution* , (2019), Available At: https://www.europarl.europa.eu/doceo/document/A-8-2019-0019_EN.html. Last Visited 25.11.2021

[68] European Comission, "Ethics guidelines for trustworthy AI", (2019), Available At: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Last Visited 02.12.2021

intelligence systems and a checklist "The Assessment List for Trustworthy Artificial Intelligence" (ALTAI) have been published.[69]

On the other hand, the European Union has many fund projects to support artificial intelligence studies. The “Horizon Europe” project is one of the most important R&D studies of the EU carried out within the scope of artificial intelligence since 2018. The total size of this project is 95.5 billion Euros.[70] Horizon Europe is a financing program that aims to increase the UN's Sustainable Development Goals and the EU's competitiveness.[71]

Besides, another important organization is "The European AI Alliance”. The European AI Alliance is a forum where all aspects of the development and impact of artificial intelligence can be broadly and openly discussed. This alliance started its work in June 2018. [72]

The "AI4EU" consortium was established in January 2019 to create the first European Artificial Intelligence with the support of the European Commission under the H2020 program. "AI4EU" is a collaborative ecosystem platform that aims to promote value, growth, human-centered and reliable artificial intelligence research by uniting the artificial intelligence community.[73]

In February 2020, the European Commission published the first White Paper on Artificial Intelligence called "The European Approach to Excellence and Trust". The Commission Report on the Safety and Liability Implications of Artificial Intelligence,

[69] See for detailed information: ALTAI,” The Assessment List for Trustworthy Artificial Intelligence” Available At: https://altai.insight-centre.org/ . Last Visited:02.12.2021,

[70] Çetin S. , op.cit. P. (21-75)

[71] See. European Commission. *Horizon Europe.* Available at: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en. Last Visited 01.12.2021

[72] European Commission, "The European AI Alliance” Available At: https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance. Last Visited 03.12.2021

[73] See. ai4europe. *ai4europe*(n.d.). Available At: https://www.ai4europe.eu/. Last Visited 01.12.2021,

the Internet of Things, and Robotics was released alongside the White Paper, providing more information on the gaps in existing laws found by the Commission.[74]

On December 14, 2020, the European Union Agency for Fundamental Rights published the report "Getting the Future Right-Artificial intelligence and Fundamental Rights." In the related report, artificial intelligence has been examined in the dimension of fundamental rights. It has been stated that special protections against discrimination originating from artificial intelligence are required and the necessity of legal protections related to these has been emphasized.[75]

As can be seen, many studies have been conducted by the Council of Europe in the field of artificial intelligence. Another effort is the establishment of an ad hoc committee called "CAHAI".[76] The aim of CAHAI is to develop artificial intelligence based on human rights, democracy, and rule of law standards.[77] In addition, the report titled "Towards Regulation of AI Systems", to which many people from the committee contributed, was published at the end of 2020. In the related report, global developments in the regulation of artificial intelligence were evaluated within the scope of human rights, democracy, and the rule of law.[78]

[74] Rechtsanwälte, L., "Regulation of Artificial Intelligence in Europe - What's in the pipeline?" (2020), Available At: https://www.lexology.com/library/detail.aspx?g=d9f74ab9-139c-49e1-9d82-70de718af80f Last Visited 04.12.2021

[75] Çetin S., op.cit. P. (21-75)

[76] CAHAI, "CAHAI - Ad hoc Committee on Artificial Intelligence", (n.d.), Available At: https://www.coe.int/en/web/artificial-intelligence/cahai. Last Visited 05.12.2021

[77] Ibid.,

[78] CAHAI - Ad hoc Committee on Artificial Intelligence, *Towards regulation of AI systems, (2020)*, Available At. https://edoc.coe.int/en/artificial-intelligence/9656-towards-regulation-of-ai-systems.html. Last Visited 06.12.2021

III.BIOMETRIC DATA

A. DEFINITION OF BIOMETRICS

Biometry is the use of distinctive biological or behavioral characteristics to identify people.[79] It derives from the ancient Greek words "bios" (life) and “metrics” (to measure).[80]

According to the World Intellectual Property Organization (WIPO), biometrics deals with the recognition of people based on physiological characteristics such as face, fingerprint, vascular structure or iris, and behavioral characteristics such as gait or speech.[81]

Biometry refers to the recognition of people based on physical or behavioral characteristics. Biometrics is physical features such as face, fingerprint, retina, vascular structure or behavioral characteristics, psychological characteristics, or features such as a person's learning throughout his life (handwriting, signature, walking, writing, speaking).[82]

The 7 basic features of biometrics can be defined as follows. Biometrics are: Universal (This is a quality that everyone should possess); Unique (In terms of that characteristic, no two people ought to be identical); Permanent (invariant with time); (It's possible to quantify it); Reliable (must be safe and operate at a high level of performance); Acceptable (non-invasive and socially acceptable); and (non-circumventable).[83]

---

[79] Dunstone, T., & Yager, N. (2008). *Biometric system and data analysis: Design, evaluation, and data mining.* Springer Science & Business Media. P.3

[80] Maguire, M. (2009). “The birth of biometric security”. Anthropology today, 25(2), 9-14. P.9

[81] WIPO, W. Technology trends 2019: Artificial intelligence. Geneva: World Intellectual Property Organization, (2019), P.147, Available At: www.wipo.int/publications/en/details.jsp?id=4386. Last Visited 27.12.2021,

[82] Tuncay, M., (2019), Biyometrik Verileri Korunnması.”, Master Thesis L.L.M Bahçesehir University Social Sciences Institute

[83] Wang, P. S., & Yanushkevich, S. N. (2007). “Biometric technologies and applications. In *Artificial Intelligence and Applications”* (pp. 249-254). P.249

Biometric technologies play a leading role in the security, migration, and border control policies of the European Union, especially in large-scale systems such as Eurodac, VIS, and planned SIS II.[84] However, recently, biometric technology has also increased its use in the private sector. Biometric systems for access and time and attendance control of employees are preferred by employers due to the increased security needs promised by the biometric system. For instance, facial recognition technology, which is one of the main topics of our study, has been in use on the internet environment since 2009. As it can be seen, the main reason why biometric data is important is the solution that biometric data brings to increasing security problems.[85]

B. DEFINITION OF BIOMETRIC DATA

The biometric features of a person are distinctive, measurable characteristics that can be used as a template to identify and define that person. Directive 95/46/EC, which is the basis of the Union on the regulation of the processing of personal data, and most national data protection legislation in the Union does not explicitly mention biometric data.[86] However the GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[87]

In another definition, biometric data can be defined as any data record that comprises a biometric sample of any modality or many modalities, whether or not it has been processed. EU data privacy law defines biometric data as special categories of personal data and prohibits their processing. Biometric Data includes physical such as fingerprints, voice prints, hand scans, face geometry recognition, and iris or retina

[84] Eurodac, VIS and planned SIS II will be examined in detail later in the thesis in "Border Control arrangements".
[85] Kindt, E. J. (2016). *Privacy and data protection issues of biometric applications* (Vol. 1). Springer.P.2
[86] Kindt, E. J. (2013). *Privacy and data protection issues of biometric applications* (Vol. 1). Springer. P.2
[87] GDPR, supra note 2, art. 4 (14).

recognition.[88] It also includes biometric Data, behavioral data such as walking and typing style. It can be said that behavioral data is more comprehensive. Any behavioral characteristic that could allow a person to be uniquely identified will be considered biometric data. However, it is unclear how narrowly regulators will interpret this category, or what limiting principles, if any, will guide their analysis.[89] For instance in the GDPR it appears that biometric data is conceived broadly. In this context, it seems to be implicitly accepted that biometric technology is relatively new and will continue to evolve.[90]

C. HISTORY OF BIOMETRIC TECHNOLOGY

How old is the history of biometric identifiers? The answer to this question goes back 36 thousand years. Discovered by the Chauvet group in Lascaux, France, handprints in cave paintings by prehistoric artists are cited as the oldest of the biometric identifiers.[91]

Biometric methods were used for the first time in the criminal justice system for processing fingerprints. It was compared manually whether the suspect had been seen before at the place where the crime was committed. In the early 20th century, the number of fingerprints held by police increased drastically. Therefore, the manual classification of fingerprints was costly at that time. In 1979, the first fingerprint recognition system prototype was tested at the US Federal Bureau of Investigation. In 1983, Automatic Fingerprint Identification Systems (AFIS) began to be used. "AFIS" was a very important step for fingerprint recognition systems. In addition, in the method called vascular recognition, the individual pattern of the veins in the fingers, wrist,

[88]Thalesgroup, "Biometric data and privacy laws (GDPR, CCPA/CPRA)." (2021, June 16), Available At: thalesgroup.com/en/markets/digital-identity-and security/government/biometrics/biometric-data. Last Visited 07.01.2022

[89] Ross, D. op.cit.,

[90] Danny Ross, "Processing biometric data? Be careful, under the GDPR." (2017, December 31), Available At: https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-GDPR Last Visited 22.08.2022

[91] Kindt, E. J. (2013). *Privacy and data protection issues of biometric applications* op.cit. P.15

hands, or face can be mapped using infrared cameras. This technology has been increasing in use especially in Japan since 2005.[92]

With regard to the history of face recognition technologies, in the 1960s, semi-automatic facial recognition methods began to be developed. The earliest published work on facial recognition methods was by Helen Chan and Charles Bisson in 1965.[93] By 1969, fingerprint and facial recognition were widely used in law enforcement in the USA. In 1988, artificial intelligence was developed to improve previously used theoretical tools that had numerous flaws. Linear algebra was used to interpret images in new ways and find a way to simplify and manipulate them without the use of human markers.[94] This development was an important step for face recognition via artificial intelligence. In 1991, face recognition technology was developed, which enables real-time recognition.[95] Turk and Pentland presented a new face recognition method with the new technology, using the PCA method as one of the first successful examples of face recognition technology.[96] In 2014, face recognition algorithm called Deepface was developed by Facebook. It has been announced that the success rate of Deepface is about 97%.[97] On November 2, 2021, Facebook announced that it would delete its entire database of face templates used for automatic photo tagging in the Facebook app by the end of the year.[98] However, it will not eliminate the software that powers the system, which is an advanced algorithm called DeepFace. As it is known, Facebook has been notorious lately for a major whistleblowing scandal and subsequent renaming of the company to "Meta". For this reason, there have been many reactions, especially from

[92] Dunstone, T., & Yager, N. op.cit. P.6-8

[93] Dunstone, T., & Yager, N. op.cit. P.8

[94] Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). "Past, present, and future of face recognition". A review. Electronics, 9(8), 1188., 1-52 P.4

[95] BioConnect, "A Brief History of Biometrics", (2021, December 8), Available At: https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/. Last Visited 03.01.2022,

[96] Turk, M., & Pentland, A. (1991)." Eigenfaces for recognition." Journal of cognitive neuroscience, 3(1), 71-86. P.71

[97] Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). "Deepface: Closing the gap to human-level performance in face verification." In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1701-1708). P.1701

[98] Jakubowska, E. "Facebook deleting facial recognition: Five reasons to take it with a pinch of salt.", (2021, November 4), Available At: https://reclaimyourface.eu/facebook-deleting-facial-recognition-five-reasons-to-take-it-with-a-pinch-of-salt. Last Visited 07.01.2022,

the EU, regarding the sharing of biometric data, which is one of the sensitive data, by Facebook. The last 10 years, the use of facial recognition technologies has gradually increased with the development of artificial intelligence. Smartphone companies started using fingerprint technology to unlock phones that made biometrics widespread in the world as an authentication tool. Facial recognition systems were installed at the entrances to workplaces and gyms. Law enforcement also made use of facial recognition systems to combat crime and criminals.

In recent years, the use of iris layer systems has become widespread in many areas. It is estimated that the concept of iris recognition, recognizing people from their irises, has a history of 80 years. Frank Burch has suggested that iris tissue, not eye color, may be an important human identifier.[99] Two ophthalmologists, Dr. Leonard Flom and Dr. Aran Safir already received the first patent for this idea in 1987. In 1994, Prof. John Daugman developed an iris recognition program and received a patent.[100]

Keystroke dynamics was first used as a biometric identifier during the Second World War. Allied powers were able to identify other operators, friend and foe, with a dialing rhythm called "The Fist of the Sender", a telegraph operator. It also appears to continue to develop new methodologies for biometrics field recognition. For example, a patent called “Method and system for smell- print recognition biometrics on a smart-card” was even granted in 2008.[101]

Voice verification and identification activities date back to the 1960s. [102] The first scientific study on this subject was done by Sandra Pruzansky in 1963 with the study named Pattern-matching procedure for automatic talker recognition.[103] By the year 2000, voice recognition technology had achieved close to 80% accuracy. Big tech

[99] Trokielewicz, M., Czajka, A., & Maciejewicz, P. (2018). “Iris recognition in cases of eye pathology.” ArXiv, abs/1809.01040. P.2

[100] Dunstone, T., & Yager, N. op.cit.. P.6-8

[101] Dunstone, T., & Yager, N. op.cit. P.6-8

[102] Gish, H. (2005). Elements of Speaker Verification. In: Wayman, J., Jain, A., Maltoni, D., Maio, D. (eds) *Biometric Systems.* Springer, London. P.115

[103] For more detailed information, see: Pruzansky, S. (1963). “Pattern-Matching Procedure for Automatic Talker Recognition.” The Journal of the Acoustical Society of America, 35(3), 354-358.

companies have invested heavily in speech recognition. (Apple- Siri, Google- Google Voice Search ,etc.)

Two renowned studies confirmed the uniqueness of the retina's blood vessel pattern. Dr. Carleton Simon and Isodore Goldstein revealed their discovery that each retina has a unique blood vessel pattern in a paper they published in 1935. The second study was conducted by Dr. Paul Tower in the 1950s. According to this study, Dr. Paul Tower found that the retina's blood vessel patterns differ even between identical twins.[104] In 1976, Robert Buzz Hill established a corporation called EyeDentify Inc.[105] This company was the first commercial example of retinal recognition.

As for DNA, James Watson and Francis Crick discovered the structure of DNA in 1953. Although this is known in textbooks, DNA had already been discovered years before the 1950s.[106] Before the 1950s, Gregor Mendel, Friedrich Miescher, Albrecht Kossel, Theodor Boveri, Walter Sutton, Erwin Chargaff, Roslind Franklin and Oswald Avery conducted studies on DNA.[107]

[104] Zibran, M. F. (2009). *Eye based authentication: Iris and retina recognition.* Technical Report#2011-04, University of Saskatchewan.P25-26

[105] For more detailed information, see: Hill, R. (1996). "*Retina identification. In Biometrics"* (pp. 123-141). Springer, Boston, MA.

[106] Dai, P., & Rudge, D. (2018). "Using the discovery of the structure of DNA to illustrate cultural aspects of science." The American Biology Teacher, 80(4), 256-262. P. 253

[107]Lunapbc,"https://www.lunadna.com/history-of-dna/", (Aprıl 24 2019), Available At: https://www.lunadna.com/history-of-dna. Last Visited: 18.08.2022

Technology	Approximate date of an early major paper or relevant patent	Approximate date of an early commercial implementation
Fingerprint (AFIS)	1962 paper	1979, 1985 Identix
Retina	1978	1984, EyeDentify, Inc.
Speaker	1963 paper, Pruzansky	1976, Texas Instruments
Face	1965, Helen Chan and Charles Bisson	1996 Cognitec,ZN, Identics
3D Face	1992 G. Gordon	2001, A4 Vision
Hand	mid-1960s	1986, IR Recognition Systems
Iris	1987 Patent, John Daugman	1995, Iridian
Palm	1994	1997
Vascular	1992, Dr K. Shimizu	early-2000s
Finger Vein	2002	2004
Keystroke	1986 Patent J. Garcia.	2002 iMagic

Table 3 shows the progression of several biometric technologies.[108]

D. BIOMETRIC TECHNOLOGIES

Biometric technologies could be examined under 4 headings: biometric authentication, biometric identification, biometric categorisation and biometric detection. Biometric authentication, biometric identification and Biometric categorization are included in the "Artificial Intelligence Act" of the European Commission. Biometric identification and biometric authentication are two separate types of biometric technologies that have often been confused. Biometric identification answers the question of “who you are” and can be applied to both physical and digital scenarios. It has been used in many applications including law enforcement, defence and border control. Biometric authentication asks if you can prove who you are.[109] For example, fingerprint and face recognition technology used in phones is biometric authentication technology.

[108] Dunstone, T., & Yager, N. op.cit. P.6

[109] Veridiumid, “Biometric Identification or Biometric Authentication?” (2018, June 11), Available At: https://www.veridiumid.com/biometric-identification-and-biometric-authentication. Last Visited 08.01.2022,

In this context, as a definition "Biometric identification is the process of comparing an individual's biometric data to biometric templates stored in a database (i.e., a one-to-many matching process)."[110] Biometric authentication is contrariwise "the process of comparing an individual's biometric data to a single biometric template stored in a device"[111]

The definition of biometric categorization on the other hand is "the process of establishing whether the individual's biometric data belongs to a group with a predefined characteristic so as to take a specific action. In biometric categorization, the person's identity is not identified or verified, but automatically assigned to a specific category. For example, an ad may show different ads according to the person, age and gender."[112]

Biometric detection, as the fourth category, is used to detect certain human conditions, the purpose of which is anger, fear, a certain intention, or a certain illness.[113] The use of such emotion recognition systems, within the context of the type of biometric detection, has been increasing in recent years.[114]

E. BIOMETRIC TECHNOLOGY TYPES

1. Facial Recognition

Facial Recognition technology is a common process used in authentication and identification and detection. Because of its ability to distinguish between individual appearances in humans, facial recognition technology is considered a natural biometric identification.[115]

---

[110] Article 29 Data Protection Working Party, (2012) *Opinion 3/2012 On Developments In Biometric Technologies*, op.cit.P.5

[111] Ibid., P.6.

[112]Ibid., p.6

[113] Wendehorst, C., & Duller, Y. , *Biometric Recognition and Behavioural Detection. Study Requested by the JURI and PETI Committees of the European Parliament,* (2021), P.22 Available At: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2021)696968

[114] Emotion recognition systems will be examined in the legal regulations (The draft AI regulation) Last Visited 15.01.2022

[115] Asha, S., & Chellappan, C. (2012). "Biometrics: an overview of the technology, issues and applications." International Journal of Computer Applications, *39*(10), 35-52. P.39

Facial recognition technology uses the following techniques: Facial geometry, which uses the face's geometric features and multiple cameras to improve accuracy such as2D, 3D etc., skin pattern recognition and facial thermogram, which uses an infrared camera to map the temperature of the user's face or smile.[116] Face recognition technology has some challenges. There may be identification and matching problems due to the change in the appearance of the face due to various reasons.[117] It is less accurate than other biometric methods such as iris or fingerprint.[118] In addition, changes such as cosmetics, disguise and aging may affect the identification system. However, the results are tried to be improved by feeding with deep learning methods and lots of data. Computers, which can now recognize faces with an accuracy of over 97%, are almost at the same level as humans in this regard.[119]

Mobile phones, as one of the most common tools the face recognition technologies are used today, are now unlocked by recognizing people by their faces. Another common practice is for Facebook to recognize people in photos and suggest names as friend suggestions. In addition, face recognition technology is used in healthcare, retail, hotel, advertising and marketing, banking, social media, aircraft, automobiles, casinos, elections, education, taxi/uber, food industry etc.[120]

[116] Ibid., P.39

[117] Colmenarez, A. J., & Huang, T. S. (1998). "Face detection and recognition. In *Face Recognition* "(Springer, Berlin, Heidelberg. pp. (174-185). P.180

[118] Dantcheva, A.; Chen, C.; Ross, A. Can facial cosmetics a ect the matching accuracy of face recognition systems? In Proceedings of the 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 23–27 September 2012; pp. 391–398. As cited in Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). "Past, present, and future of face recognition: A review." *Electronics*, *9*(8), 1188. P.2

[119] Jason Brownlee," How to Classify Photos of Dogs and Cats (with 97% accuracy)" (December 8, 2021), Avaialble At: https://machinelearningmastery.com/how-to-develop-a-convolutional-neural-network-to-classify-photos-of-dogs-and-cats/. Last Visited 23.08.2022

[120] Ibid.,

2. Fingerprint Technology[121]

Fingerprint technology is the oldest of the biometric technologies and the most used technology. Fingerprints are imprints formed by frictional projections of the skin and thumbs.[122] Fingerprint technology work by capturing the pattern of ridges and valleys on a finger. The data is then processed by the device's pattern matching software, which compares it to the list of registered fingerprints in the file. A successful match indicates that an identity has been verified and thus access has been granted.[123]

There are three sub-categories of fingerprint systems. First, some systems store and compare complete fingerprint images. Secondly, a subset of the characteristics extracted from fingerprint images is referred to as minutiae. The third category is the set of systems that works with individual patterns extracted from fingerprint images. Storing the entire fingerprint facilitates interoperability but increases the amount of personal data stored and thus the risk of identity theft in the event of a data leak.[124]

The 4 most important characteristics of a fingerprint are its uniqueness, immutability, permanent and universal. No two identical fingerprints are the same in studies done so far. Also, a person's fingerprint stays the same until he/she dies.[125]

Fingerprint technology has been used in office entrance and exit control, Police systems, Banks and Public institutions and organizations, etc. Also, nowadays mobile phones use fingerprint technology to unlock.

3. Voice recognition/Verification

Voice recognition techniques are generally categorized according to two approaches—Automatic Speaker Verification (ASV) and Automatic Speaker

---

[121]Fingerprint identification is also known as dactyloscopy. See. www.dictionary.com/browse/dactyloscopy, Last Visited15.01.2021

[122] Barua, K., Bhattacharya, S., & Mali, K. (2011). "Fingerprint identification." Global Journal of Computer Science and Technology. Volume 11 Issue 6, (61-63). P.61

[123] Harris, T. "How Fingerprint Scanners Work". (2020, August 3)., Available At: https://computer.howstuffworks.com/fingerprint-scanner.htm. Last Visited 15.012022

[124] C-61/22 - *Landeshauptstadt Wiesbaden*, Summary Paraf.36

[125] Kaushal, N., & Kaushal, P. (2011). "Human identification and fingerprints:" a review. J Biomet Biostat, *2*(123), 2. DOI: 10.4172/2155-6180.1000123. P.1

Identification (ASI). Voice recognition distinguishes a person by matching certain voice characteristics with templates stored in a database.[126] On the other hand the use of distinct patterns of a person's speech for recognition is known as speech verification. The physical characteristics of the vocal chords, as well as the episodic nature of the local accent, influence vocal characteristics. Besides Speech Verification has both physiological and behavioral features.[127] Voice recognition/verification can be affected by environmental factors such as background noise, stress, and colds. Voice recognition/verification systems are used in customer service, banking, electronic devices, etc.

4. Iris

Iris recognition is the most accurate of biometrics. "Primary visible characteristic is the trabecular meshwork, a tissue which gives the appearance of dividing the iris in a radial fashion" [128] By the eighth month of pregnancy, the embryo is permanently formed.[129]

The iris is the most important biometrics in many ways.[130] Among the eye-related biometrics, iris recognition is the easiest. Because the iris is easily visible from a few meters away.[131]

Twins' irises are different from each other. Right and left irises are also different from each other. A person's iris remains constant throughout a person's life. As a result,

[126] Phadke, S. (2013), op.cit.. P. 130

[127] Dunstone, T., & Yager, N. op.cit. P.61-62

[128] Deb, S. (2003). "Multimedia Systems and Content-based Retrieval." In *Face Recognition Technology* (pp. 62-101).P.67

[129] Penny K.H. (2021). "Iris Recognition Technology for Improved Authentication." Sans Security Essentials (Gsec) Practical Assignment, Version. 2021;3. P.4

[130] In Stadt Bochum & Mr. Schwarz (2013) case; The CJEU stated that the only real alternative to taking fingerprints is an iris scan. However, Court stated that iris recognition technology is not as advanced as fingerprint recognition systems. Para 51

[131] Phadke, S. op.cit. P. 130

the physical properties of the iris are not affected by age, disease or environmental conditions.[132]

Moreover, although empirical tests with the technology will expand its reliability, it appears quite promising and even practical for many applications, especially for two-factor scenarios.[133]

5. DNA

DNA is the chemical name for the molecule that carries all living things genetic instructions.[134] Human DNA samples can be obtained from Numerous sources; from hair, nails, saliva and blood samples.[135] DNA has some differences from standard biometric.

DNA matching uses a comparison of real samples rather than using templates or feature extraction. In contrast to an impression, image or recording, DNA requires a physical sample. DNA matching is not done in real time and not all stages of the comparison are automated at the moment.[136]

DNA biometric data preferred on the following grounds: DNA is unique to every individual in the world. Identical twins are the only ones who have the same DNA. It is easily acquirable from a variety of sources, easily used in forensics to match crime scene evidence to individuals and remains constant throughout one's life without change.[137] On the other hand, DNA matching is high-priced and time consuming and so is not yet suitable for civilian use in large - scale biometrics applications.[138]

---

[132] Yadav, A. K., & Tadisetty, S. (2012).” Iris based de-duplication technology.” *IJERA*, *2*(1), (164-167). P.164

[133] Phadke, S.op.cit. P. 130

[134] DNA is the chemical name for the molecule that carries genetic instructions in all living things.

[135] Phadke, S. op.cit.. P.13

[136] Suvarnsing B., & Sangramsing K., N. & Raju M., & Jaypalsing K., & Charansing K.. (2015). “DNA Biometric”., IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 5, Issue 5, Ver. I (Sep - Oct. 2015), PP 82-84, P.83

[137] Balaji, P. (2010). “An Overview-DNA as a Biometric Data Identifier.” Available at SSRN: https://ssrn.com/abstract=1572236 or *http://dx.doi.org/10.2139/ssrn.1572236*. Last Visited15.02.2022

[138] Phadke, S. op.cit. P.131

6. Keystroke

The process of measuring and assessing a typing rhythm on digital devices, such as computer keyboards, mobile phones, and touch screen panels[139] is known as keystroke.[140] Keystroke is a behavioral biometric. Keystroke dynamics identify people based on their typing pattern, rhythm and speed using a unique biometric template. "Dwell time" and "flight time" are the raw measurements used to describe keystroke dynamics. The dwell time is the time of pressing a key, while the flight time is the time between keystrokes. So, keystroke dynamics can be defined as a software-based algorithm that measures both the "dwell time" and the "flight time" to verify the identity.[141]

7. Signature

Signature verification technology relies on the unique characteristics of a person's signature to verify their identity. Rather than comparing the images of the signature, this technology examines the behavioral components of the signature, such as stroke order, speed and pressure.[142]

FEATURES	Facial Recognition	Iris Recognition	Fingerprint Recognition	Voice Recognition
Accuracy	Medium-Low	High	High	Medium
Attack's Precaution	Medium	Very High	High	Medium
Verification time	About 3 seconds	Less than 5 seconds	Less than 3 second	About 5 second
Devices Required	Camera	Camera	Scanner	Microphone

[139] Bartlow N. (2009) "Keystroke Recognition." In: Li S.Z., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA.

[140] Rawlson King, Explainer: "Keystroke recognition.", (2018, March 12), Available At: https://www.biometricupdate.com/201612/explainer-keystroke-recognition. Last Visited 16.02.2022,

[141] Ibid.,

[142] Asha, S., & Chellappan, op.cit. P.43

Interference	Lighting, Glasses, Hair, Moving, Age	Lighting, Inaccurate eye positioning in relation to device	Dryness, Dirt, Deep injury, age	Noise, Cold symptoms

The table 4 shows the characteristics of the types of biometric technology.[143]

[143] Evgeniy Krasnokutsky., " AI Biometric Authentication for Enterprise Security". (2021), Available At: https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security. Last Visited 22.08.2022

IV. LEGAL REGULATIONS

Although both biometric data and artificial intelligence have been developing issues in recent years, important steps have been taken on this issue, especially in the EU legal order. However, it would be appropriate to say that these regulations are still insufficient. With the developing technology, it continues to be made in regulations.

There are international, supranational and national regulations regarding the matter as examined below.

A. INTERNATIONAL REGULATIONS

1. Universal Declaration of Human Rights

According to Article 12 of the UN Universal Declaration of Human Rights According to this article, everyone has the right to respect for his or her private and family life. Member states should not interfere with these rights of individuals. If the person is exposed to such interference or attacks, he or she must has the right to be protected by law.[144]

Another important issue is the various Resolutions of the United Nations Security Council on the collection and sharing of biometric data for counter-terrorism purposes. The United Nations Security Council in its resolution 2014 (2160)[145] encourages all Member States to submit to INTERPOL the biometric data of individuals, groups, enterprises and organizations that support the Taliban. In Resolution 2322 (2016),[146] it extended the recommendation on biometrics data sharing with terrorists and terrorist organizations. In Resolution 2396 (2017),[147] it emphasized to identify terrorists, including foreign terrorist fighters, responsibly and properly with the help of biometric data, in accordance with national and international law, including human rights law.

[144] Ibid., Article 12
[145] United Nations Security Council Resolution (2014). 2160. Para (38).
[146] United Nations Security Council Resolution (2016). 2322 Para (3).
[147] United Nations Security Council Resolution (2017). 2396. Article 38

The UN Counter-Terrorism Committee Executive Directorate (CTED) published the CTED Analytical Summary on 10 December 2021. The report included information on the use of biometrics in the fight against terrorism. The report emphasized that 118 out of 193 member states of the United Nations made at least marginal progress in implementing biometrics for counter-terrorism purposes. It was emphasized that especially African, Central, Southeast Asian countries and South American countries needed technical assistance from expert countries.[148] The fight against terrorism is undoubtedly very important in terms of security. But given the universally binding nature of the Security Council resolution, all 193 UN Member States need detailed human rights guidance to implement biometric data systems, many of which lack adequate privacy and data protection frameworks under domestic law.[149]

2. European Convention on Human Rights

The European Convention on Human Rights regulates respect for private and family life. According to this article, everyone has the right to respect for his private and family life. Private life refers to the non-public life that one does not share with others. Private life is a very broad concept. Private life, family life, home immunity, freedom of communication, protection of personal data is also evaluated within this scope.

Within the scope of this article, some exceptions have been introduced. These exceptions are: in accordance with the law, necessary in a democratic society, national security, public safety or the economic well-being of the country, the prevention of order or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

Protection of personal data is essential for a person to enjoy the right to respect for private and family life guaranteed by Article 8. In fact, Article 8 does not directly

[148]United Nations, "CTED publishes Analytical Brief on the use of biometrics in counter-terrorism ". Available At: https://www.un.org/securitycouncil/ctc/news/cted-publishes-analytical-brief-use-biometrics-counter-terrorism. Last Visited: 18.02.2022

[149] The University of Minnesota Human Rights Center," Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" (2020), Available At: https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Summary.pdf. Last Visited Date:20.02.2022, P.2

refer to personal data. However, personal data took place in the judicial decisions of the European Court of Human Rights. For example, the ECtHR has decided in the cases of personal data breach.[150]The European Court of Human Rights first extended the concept of private life in Article 8 of the Convention in cases involving wiretapping (Klass[151] in 1978 and Malone[152] in 1984). It also expanded the scope of Article 8 in cases involving data stored in computers, video surveillance at Peck,[153] or the storage of such data in confidential records in *Leander* in 1987[154] and in *Rotaru*[155] in 2000. The expansion of the scope of right to respect for private life and family life by the European Court of Human Rights has encouraged the protection of personal data in Europe. As a result of this encouragement, many legal regulations entered into force within the member states and the EU.[156]

In *Peck* v. *the United Kingdom* the depressed applicant was filmed by the CCTV system while he was attempting to commit suicide by slitting his wrists, holding a kitchen knife in his hand. These images appeared on television and in the local press. The applicant's complaint regarding the breach of his privacy was dismissed by the Press Complaints Commission. He then appealed to the court of appeal. However, this application was also rejected. Thereupon, the applicant applied to the ECtHR. ECtHR found that the domestic authorities' disclosure of CCTV footage of the applicant's suicide attempt violated her right to private life under Article 8 of the Convention. [157]

In another case[158] Mr. S. was charged with attempted robbery and arrested on January 19, 2001, at the age of eleven. Fingerprints and DNA samples were taken

[150] European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights". (2021), Available At: https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Last Visited22.02.2022

[151] See. Klass And Others V. Germany,(1978), (Application No. 5029/71)

[152] In Malone v Metropolitan case , it was decided that the telephone tapping was unlawful as the applicant's private life was not respected. See. Malone v Metropolitan Police Commissioner [1984] (Application no. 8691/79)

[153] Peck v. the United Kingdom, (2003), (Application no. 44647/98).

[154] Leander V. Sweden, (1987), (Application No. 9248/81)

[155] Rotaru V. Romania, (2000), (Application no. 28341/95)

[156] Bourcha, C., Deftou, M. L., & Koskina, A. op.cit.. P.45

[157] Case Of Peck V. The United Kingdom, (2003), (Application No. 44647/98)

[158] S. and Marper v. the United Kingdom (2008), ECHR Judgment No. 30562/04

during the trial. However, Mr S. was acquitted on 14 June 2001. Michael Marper was accused and arrested of abusing his partner on March 13, 2001. Fingerprints and DNA samples of Michael Marper were taken during the trial. No criminal prosecution was filed, as Marper and his partner had reconciled before an investigation was held. The ECtHR has ruled that the UK police's indefinite retention of DNA and fingerprint data obtained at the time of the suspects' trial after their acquittal is contrary to Article 8 of the European Convention on Human Rights (right to respect for private and family life). The Court stated that The capacity of the DNA profile to provide a way to identify genetic contacts between individuals is in itself adequate to conclude that their concealment interferes with the privacy rights of the individuals concerned.[159]

Following this decision, the Draft Protection of Freedoms Bill in England was presented to the Parliament on February 11, 2011. This Act introduced a new framework for police to keep fingerprints, in line with the case of *S and Marper* v. *the United Kingdom*.[160]

Wrong and unfair practices to be made due to biometric methods may hinder the freedom of people to travel freely in border and visa controls. This situation is a practice that restricts the freedom to travel internationally, which is included in the Universal Declaration of Human Rights of 1948 and Protocol No. 4 to the European Convention on Human Rights.[161]

The EU is not a party to the European Convention on Human Rights yet. The EU's accession to the European Convention on Human Rights (ECHR), which has been debated since the late 1970s, is now a legal obligation under Article 6(2) of the Lisbon Treaty. The purpose of the EU's accession to the ECHR is to contribute to the creation

[159] Ibid., Para.75

[160] Justice.org.uk, *Protection of Freedoms Bill* Available At: https://justice.org.uk/protection-of-freedoms-bill. Last Visited 13.03.2022

[161] Özkorul, G. (2021). "Uluslararası göç ve güvenlik perspektifinde biyometrik verilerin önemi" Master's thesis, Sosyal Bilimler Enstitüsü.P.50

of a single European legal space by achieving a coherent Europe-wide framework of human rights protection.[162]

As a result, the European human rights convention is very important for both EU and EU law. The European Commission's Vice-President for Values and Transparency, Věra Jourová, and the Secretary General of the 47-nation Council of Europe, Marija Pejčinović Burić, have issued the following statement. “The EU's accession to the Convention, which is a legal requirement under the Lisbon Treaty, will further strengthen human rights protection in Europe. Accession will help to guarantee coherence and consistency between EU law and the Convention system. It will also ensure that the EU is subjected to the same international oversight on human rights as its 27 member states and 20 other Council of Europe countries, which are not members of the EU. It means that citizens will be able to challenge the EU's actions before the European Court of Human Rights. The EU will also be able to join its member states in proceedings at the European Court of Human Rights concerning alleged violations resulting from EU law.”[163]

B. REGULATION OF BIOMETRIC DATA IN THE EU LEVEL

1. The Charter of Fundamental Rights of the EU

The protection of fundamental rights is one of the basic principles of European structuring after the Second World War. The fundamental rights, democracy, and rule of law are the cornerstones of the European Union. Article 2 of the Treaty on European Union regulates "Union Values". “According to relevant article The Union should respect, among other values, human rights, including the rights of persons belonging to

[162] European parliament, “Completion Of Eu Accession To The European Convention On Human Rights”, (2021) Available At: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-completion-of-eu. Last Visited 27.02.2022
accession-to-the-echr, P.1

[163] European Commission,"The EU's accession to the European Convention on Human Rights: Joint statement on behalf of the Council of Europe and the European Commission", (2020), Avaiable At: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_1748. Last Visited 22.08.2022

minorities. These values include pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men.[164]

The Charter also enshrines the fundamental rights people enjoy in the EU. In light of societal changes, social advancement, and scientific and technological advancements, the Charter is a contemporary and comprehensive document that safeguards and advances the rights and freedoms of all people.[165]

The protection of fundamental rights is a horizontal issue, that touches all areas of EU activity. This means that, regardless of their level or the subjects they cover, they must be taken into account by all EU institutions, bodies and agencies in their work. Additionally, there is a specialized organization that handles all matters directly related to fundamental rights: the Working Party on Fundamental Rights, Citizens' Rights and Free Movement of Persons (FREMP).[166] One of the main areas of (FREMP) is the implementation of the EU Charter of Fundamental Rights.

Article 51 regulates Field of application of Charter. The provisions of this Charter are addressed to the institutions, organs, offices and agencies of the Union, in accordance with the principle of subsidiarity, and to the Member States only when implementing the law of the Union.[167] As can be seen, the relevant article is quite clear. Provisions of Charter are addressed to the institutions and bodies of the Union, and to the member states when they are implementing European Union law.

Article 52 regulates Scope and interpretation. The conditions under which the limitation can be made are specified in this article. First, the limitation must be provided by law. Secondly, the essence of rights and freedoms must be respected. Third, the limitation must be subject to the principle of proportionality. Further, the limitation must be necessary and may be made only if it genuinely meets the objectives of general

[164] TEU Article 2
[165] European Commission, "Why do we need the Charter?" Available At: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en. Last Visited 22.08.2022
[166] European Council,"Protection and promotion of human rights", (2022), Available At https://www.consilium.europa.eu/en/policies/human-rights/: . Last Visited 23.08.2022
[167] ECHR Article 51

interest recognized by the Union or the need to protect the rights and freedoms of others. [168]

Stadt Bochum, Mr. *The Schwarz* case is related to Article 52. In *Schwarz & Stadt Bochum* case; Mr. Schwarz applied to the Stadt Bochum for a passport. Mr. Schwarz didn't ask for his fingerprints to be taken. Thereupon the Stadt rejected Bochum's application. Mr. Schwarz appealed to the court, demanding that he be given a passport without fingerprints. There upon the ECJ was asked whether the imposition of the requirement to store fingerprints of Article 1(2) of Regulation (ECTHR) no 2252/2004 regulating the issuance of passports by member states was contrary to the "Right to respect for private life" and “Right to the protection of personal data”. In this decision, the CJEU recognized fingerprints as personal data because they contain objectively unique information about individuals and allow for the precise identification of these people. [169]

As explained in detail in the EU Charter of Fundamental Rights above, the general reasons for limitation of rights are listed in Article 52 of the EU Charter of Fundamental. Accordingly, the limitation on the exercise of rights should be provided by law and the essence of these rights and freedoms should be respected. Also, the limitation can be made in accordance with the principle of proportionality and only if it is necessary and really meets the general goals recognized by the Union or the need to protect the rights and freedoms of others.[170] Taking and keeping the fingerprints while issuing the passport is done with Regulation No. 2252/2004. In other words, the requirement to be regulated by law has been fulfilled. Regarding the public interest purpose underlying the limitation, firstly, it is to prevent falsification of passports and secondly, to prevent forgery, i.e., use by persons other than their real holders. As regards the essence of the right in the case, the limitations placed on the exercise of the rights recognized by Articles 7 and 8 of the Charter do not respect the essence of those rights. It is clear from the evidence available to the Court. It has not even been claimed. The Court must also determine whether the restrictions placed on these rights are

[168] ECHR Article 52
[169] Case C-291/12 Schwarz v Stadt Bochum , (2013), Para 27
[170] ECHR Article 52(1)

proportionate to the aims pursued by Regulation 2252/2004, as well as the aim of preventing illegal entry into the European Union. The taking and storage of fingerprints referred to in Article 1(2) of Regulation No 2252/2004 is appropriate for the purposes pursued in this Regulation, in addition to the purpose of preventing illegal entry. As for necessity, the CJEU finds that the combination of two operations designed to identify persons may not a priori be regarded as giving rise in itself to a greater threat to the fundamental rights at stake than if each of those two operations were to be considered in isolation.[171]

In terms of the protection of biometric data, "Respect for private and family life" regulated in Article 7 of ECFR and "Protection of personal data" regulated in Article 8 are important. According to Article 7; Everyone has the right to respect for his private and family life.[172]

Technological developments have made it easy to intervene in fundamental rights and freedoms. For this reason, the need to make legal regulations on personal data has arisen. In this respect, Articles 7 and 8 of the Charter are regulated for this purpose in the protection of personal data. According to Article 8; Everyone has the right to the protection of their personal data. Certain conditions have been introduced in the second paragraph. These; Personal data must be processed fairly for specified purposes, based on the consent of the person concerned or on any other legitimate basis provided for by law. Moreover, in the 3rd paragraph; compliance with the rules is subject to the control of an independent authority.[173]

C-61/22 Landeshauptstadt Wiesbaden & Digitalcourage[174] case is related to Article 7 and Article 8. The case stems from the applicant's request to be given an identity card without taking fingerprints. Defendant rejected the applicant's request on the grounds that fingerprinting is mandatory under the article 3(5) of Regulation (EU) 2019/1157. As a result, Digital Course argued that the inclusion of sensitive biometric

[171] Case C-291/12 Schwarz v Stadt Bochum , (2013), Para 34,36,39,40,41,49,64
[172] ECHR Article 7
[173] ECHR Article 8
[174] C-61/22 (Landeshauptstadt Wiesbaden) Digitalcourage, (2022), Para 2

data in identities is incompatible with fundamental rights. and asks for an ID card without fingerprints.

The Wiesbaden Administrative Court, following Digital courage argument, pointed to three reasons why the EU Regulation requiring the retention of fingerprints could be unlawful.

- The legislative process had some formal errors.
- The regulation in question is not compatible with Articles 7 and 8 of the European Charter of Fundamental Rights.
- The legislator has not conducted a privacy impact assessment, which may be necessary due to the high risk involved.[175]

The case has been referred to the CJEU for an opinion on whether Article 3(5) of the Regulation (EU) No. 2019/1175 is compatible with EU law. legitimate legal basis is required, in accordance with Article 52(1) of the Charter. It has been enacted by law in Article 3(5) of the Regulation (EU) 2019/1157 on the inclusion of fingerprints on identity cards. Within the European Union, identity cards can be used as part of a border crossing. Identity cards are also used, at least as travel documents, and as a result, it seems that the regime also serves the purpose of preventing illegal entry from these countries. This will constitute a general interest goal recognized by the Union. However, there are doubts about whether Article 3(5) of the Regulation (EU) No. 2019/1157 is proportionate, even if the regime is intended for a public interest purpose. The CJEU will make a decision by taking into account the reasons such as " In violation of fundamental rights and No impact assessment".[176]

[175] EDRİ, "ID-Fingerprint obligation to be reviewed by European Court of Justice", (2022), Available At: https://edri.org/our-work/id-fingerprint-obligation-to-be-reviewed-by-european-court-of-justice. Last Visited 04.05.2022

[176]Julia Witte., "Fingerprint obligation to be reviewed by European Court of Justice",(2022), Available At: https://digitalcourage.de/blog/2022/fingerprint-obligation-to-be-reviewed-by-ecj. Last Visited 20.03.2022

2. General Data Protection Regulation

2.1 Basic Principles of Processing Biometric Data

The processing of personal data must be done in accordance with fundamental rights and freedoms. For this, a number of principles are regulated by the legislator. The first of these principles is "lawfulness, fairness and transparency". This principle is regulated in Article 5(1)(a) of the GDPR. The principle of legality is the basic principle of personal data protection law. The purpose of the principle of legality is to ensure that personal data is processed in accordance with legal regulations.[177]

In addition, the fairness principle, which is another principle, should be followed when processing personal data. According to the principle of Fairness, controllers must process data in a lawful and transparent manner and report this to data subjects and the general public and demonstrate that their processing complies with GDPR. Personal data processing should not be done confidentially, and data owners should be informed about potential risks.[178]

Another important principle is transparency. According to the principle of transparency, the data controller should inform the data owner about the way their data is processed, risks, rules, safeguards and rights during the processing of the data.

The principle of purpose limitation simply means that you need to be clear from the very beginning about why you are collecting and processing personal data and your intention behind it.[179] According to this principle, regulated by Article 5(1)(b) of the GDPR, Personal data is collected for specific, clear and legitimate purposes and is not processed further in a way that is incompatible with these purposes.

According to the data minimization principle regulated in Article 5(1)(c) of GDPR; It is necessary to collect and process personal data that is sufficient, appropriate

[177] Küzeci, E. (2010). *Kişisel verilerin korunması,.* Ankara: Turhan Kitabevi,P.206

[178] Giakoumopoulos, C.- Buttarelli F.- O'Flaherty.M. (2018). *Handbook on European data protection law:* 2018 Edition. European Union Agency for Fundamental Rights and Council of Europe, P.120

[179] Dataprivacymanager, ,"What are the 7 principles of GDPR", (2020), Available At: https://dataprivacymanager.net/what-are-the-7-gdpr-principles/. Last Visited 23.02.2022

and limited to what is necessary for the purposes for which they are processed. That is important, because not keeping personal data correctly may harm the fundamental rights and freedoms, economic interests and personal rights of the data owner. Collecting the minimum amount of data, two questions should come to mind:

- Can you reach the goal without collecting the data?
- And is your data collection limited to information that is absolutely necessary for you to provide your service or fulfill a purpose? [180]

According to the Accuracy principle regulated in Article 5(1)(d) of GDPR; The purposes for which personal data are processed should be evaluated and all reasonable steps should be taken to promptly delete or rectify inaccurate personal data. Unlawful processing of personal data may cause the data owner to violate fundamental rights and freedoms, economic interests and personal rights. The right to truth, the right of access and the right to rectification are directly related. The right to rectification gives an individual the right to request the deletion, correction or replacement of inaccurate personal data.

According to the Storage Limitation principle regulated in Article 5(1)(e) of GDPR; Data owners should not keep personal data for longer than necessary for the purposes of processing. In the light of this principle; Personal data should not be kept longer than necessary. In addition, retained data should be periodically reviewed and deleted or anonymized when no longer needed. Personal data may only be retained for a longer period if it is stored for public interest archiving, scientific or historical research or statistical purposes.[181] There are many decisions given by the ECtHR where it has decided that keeping biometric data longer than necessary for the purposes of processing violates the person's "right to respect for privacy".

In the M.K. V. France case, as part of the investigation, fingerprints were taken of the suspect due to the theft of a book. However, the Prosecutor decided not to

[180] Ibid.,

[181]Ombudsmanky, Fifth Data Protection Principle - Storage limitation, Available At: https://ombudsman.ky/images/pdf/guide/56-fifth-data-protection-principle-storage-limitation.pdf. Last Visited 23.08.2022,p.2

prosecute. Later, M.K requested the deregistration of his fingerprints from the competent authority. Evaluating the applicant's application, the ECtHR decided that the storage of fingerprint data violated the "right to respect to privacy".[182]

In Gaughran v. The United Kingdom case; A British citizen was charged with driving with excessive alcohol in Northern Ireland in 2008. As a result of this trial, he was fined £50 and disqualified from driving for 12 months. Fingerprints and DNA samples were taken by the Northern Ireland Police as part of the investigation. After the end of the conviction, the applicant requested the deletion of the retained DNA sample and fingerprint records, but this request was denied. Evaluating the applicant's application, the ECtHR decided that the storage of fingerprint and DNA data violated the "right to respect to privacy" in accordance with Article 8 of the European Convention on Human Rights. [183]

According to the integrity and Confidentiality principle regulated in Article 5(1)(f) of GDPR; The data processor must take appropriate security measures to ensure the security of the data. This principle is strictly connected with information security. This principle not only regulates the prevention of malicious attacks and data breaches; but is also important for ensuring personal security.[184]

The last principle is the principle of accountability. According to the Accountability principle regulated in Article 5(2) of GDPR a data controller must be responsible for complying with the measures acting on the principles set out above. This principle is presented together with the reformed rules of the European Union on data protection, as recommended by the Working Group under Article 29 of Directive 95/46/EC.

[182]M.K. V. France (2013), (Application no. 19522/09), Available At: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-7567%22]} , Para 1-4

[183]Gaughran V. The United Kingdom, (2020), (Application No. 45245/15), Available At: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12731%22]}, Para1-9

[184] Dataprivacymanager, op.cit.

2.2 Lawfulness Requirements of Processing Personal Data

The European Data Protection regulation regulates the lawfulness grounds that legitimize personal data. In Article 6 of the GDPR, the lawfulness Of Processing Personal Data is listed[185] as follows: Consent of the individual concern, contractual obligation, legal obligation, vital interests, public interest and public task and legitimate interest. In Article 9 of the GDPR "processing of special categories of personal data" is regulated. In this context, both articles will be discussed in order to understand the differences between "Lawfulness of Processing Personal Data" regulated in Article 6 and "Processing of special categories of personal data" regulated in Article 9

2.2.1. Consent of the individual concerned

The first point is the consent of the data owner. The processing of personal data for one or more specific purposes is possible with the consent of the data owner. In terms of Directive 95/46 EC, only consent is sufficient for the processing of personal data of a general nature, while explicit consent is required for the processing of personal data of special nature. With the GDPR, explicit consent is required for both data categories.

The definition of consent is regulated in the article 4(11) of the GDPR. Similar to this article, the definition of consent is as follows. Consent is the declaration that the person expressly, freely and specifically accepts the processing of personal data about herself/himself."[186]

2.2.2. Contractual Obligation

According to the contractual obligation regulated in Article 6(b) of GDPR, data processing is lawful if the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before

[185] Since biometric data, (Sensitive biometric data) which is the subject of our study, is a category of personal data, this subject has been examined in a limited way.
[186] GDPR Article 4, paraf 11

entering into a contract. Contractual obligation is not however regulated in the Processing of special categories of personal data regulated in Article 9 of the GDPR.

2.2.3. Legal Obligation

According to the legal obligation regulated in Article 6(c) of GDPR, having a valid legal basis can be said to be a fundamental requirement under GDPR. The legal obligation, which is the reason for compliance with the law, applies to data controllers in both the private and public sectors.[187] People living in the EU have a fundamental right to privacy. It is unlawful to process personal data unless you have a valid legal reason under EU law. This legal reason for processing personal information is known as the legal basis for processing. In this context, the relevant law must be a law of the GDPR country in which you operate or the EU itself. If a country is not covered by the GDPR (for example, the USA, Canada or Australia), that country's laws will not provide a legal basis for processing.[188]

2.2.4. Vital Interests

According to the vital interest regulated in Article 6(d) of GDPR; The processing must be necessary to protect the vital interests of the data subject or another natural person. The natural person need not be the data owner, it can be another natural person. This legal basis is very limited in scope and generally only applies to matters of life and death.[189] It is similar to the "state of necessity", which is one of the reasons for compliance with the law regulated in some penal laws in the world.

2.2.5. Public Interest and Public Task

According to the public interest and public task regulated in Article 6(e) of GDPR the processing must be necessary for the performance of a task carried out in the public interest or for the exercise of the official authority vested in the controller. Public

[187] Giakoumopoulos, C.,Giovanni B.,/Michael O., op.cit.. P.151

[188] Robert Bateman "GDPR Lawful Basis: Legal Obligation",(2022), Available At: https://www.termsfeed.com/blog/gdpr-lawful-basis-legal-obligation. Last Visited 27.02.2022

[189] Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation:* A Commentary. Oxford University Press.P.378

interest and public task should be based on a legal regulation as in article 6(c). The legal basis must be clear, unambiguous and predictable.[190] Necessity and proportionality should be taken into account in terms of the reason for compliance with the law in question and should be interpreted narrowly.[191]

In *Huber* v. *Bundesrepublik Deutschland*[192] case Huber, an Austrian citizen, moved to Germany in 1996 to continue his job as a self-employed insurance agent. Since Mr. Huber felt that the processing of the data concerning him had been discriminated against, in particular nationals, due to the absence of such a database for German citizens, Mr. Huber requested that this data be deleted. This request was rejected by the authorities. Personal data can be legally processed, according to Article 7 (e) of Directive 95/46.386, if it is necessary for the performance of a task carried out in the public interest or for the performance of an official authority, according to the CJEU. In conclusion, the CJEU stated that the right of a Union citizen to free movement in the territory of a Member State of which he or she is not a national is not unconditional and may be subject to limitations and conditions imposed by the European regulations.[193]

2.2.6. Legitimate Interest

The legitimate interests could be your own interests or the interests of third parties. The existence of a legitimate interest in question should be carefully examined on a case-by-case basis.[194] If the legitimate interests of the controller are identified, a balancing should be carried out between these interests and the interests or fundamental rights and freedoms of the data subject.[195] Necessity and proportionality, like other

[190]. Voigt, P., B., (2017) The EU GDPR: A Practi cal Guide, Springer, Heidelberg, 2017. P.108 As Cited İn: Dülger, M. V. (2019). "Protection of Personal Data in the Context of the European Union General Data Protection Regulation". Yaşar University Law Journal, 1(2), 71-174 P.118

[191] Paslı, A., Kaya, A., Engin, B. İ., Aşıkoğlu, Ş. İ., & Oğuz, E. (2020). *Türk Hukukunun Avrupa Birliği Hukukuna Uyumu Özel Hukuk*. İstanbul University Press P.1067

[192] CJEU, C-524/06, Heinz Huber v. Bundesrepublik Deutschland [GC], (2008), Para 49,54

[193] Giakoumopoulos, C.,Giovanni B.,/Michael O., op.cit.P.154

[194] General Data Protection Regulation, Preamble, Recital 47.

[195] Article 29 Working Party (2014), "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", Available At:

reasons for compliance with the law, are important for the legitimate interest. Necessity and proportionality should be taken into account and interpreted narrowly in terms of the reason for complying with this law.

2.3. Processing of Special Categories of Personal Data

The importance of sensitive data after the second world war is very critical in terms of data related to race or religion. During the war years, it has been seen that the abuse of data can lead to human rights violations. A high level of protection is required for sensitive data. Because they are related to fundamental rights and freedoms by their very nature.[196]

In Article 9 of the GDPR "processing of special categories of personal data" is regulated. Racial or ethnic origin, political views, religious beliefs or other beliefs of a similar or philosophical nature, physical or mental health, sexual life or orientation, genetic and biometric data are special personal data. The processing of special categories of personal data is prohibited. However, there are some exceptions. Article 9 of the GDPR has replaced Article 8 of Directive 95/46/EC. Article 9 adds new types of sensitive data that were not listed in Directive 95/46/EC such as biometric and genetic data. In the processing of sensitive personal data, it may be processed within the scope of the cases specified in Article 9(2) of the GDPR. Explicit consent means that there is no doubt about consent of the data controller for the processing of his or her data.[197]

2.3.1. (9/a) Explicit consent:

The explicit consent of the data owner makes the processing of private data lawful. Directive 95/46 defined explicit consent within the scope of definitions. According to the relevant definition: Consent of the data subject means any freely given specific and informed indication of their request, in which the data subject indicates that

---

https://www.fia.org/sites/default/files/2019-11/Excerpts%20-%20Opinion%2006-2014%20on%20the%20notion%20of%20legitimate%20interests%20of%20the%20....pdf. Last Visited 03.04.2022

[196] Kuner, C., Docksey, C., & Bygrave, L. op.cit.P.369

[197] Giakoumopoulos, C.,Giovanni B.,/Michael O., op.cit. P.149

he accepts the personal data relating to him being processed.[198] According to Article 9(2) of the GDPR, Union or Member State law may regulate that the prohibition on the processing of special categories of data cannot be lifted by the individual.

The definition of consent is regulated article 7 of the GDPR. In a nutshell:

- Consent must be given of free will.
- The purpose of consent must be specific.
- Consent must be informed.
- The confirmation must be a clear indication.
- Consent must be given with a statement or an explicit act.
- Consent must be distinguishable from other considerations.

Another important point is that withdrawing consent should be as easy as giving consent. In addition, the data processor should refrain from any intervention that would make it difficult to withdraw consent.

Another innovation brought by GDPR is Conditions applicable to the child's consent regulated in article 8. Within the scope of this article, it is obligatory to obtain the permission of the child's parent in cases where the child is under the age of sixteen.[199]

2.3.2. (9/b) Employment, social security and social protection.[200]

It covers situations in which employers are required to process sensitive data of employees in order to fulfill their obligations under the labor, social security and social protection law. As an example, it can be used in the case of collecting biometric data for use in access control systems in the workplace.[201]

[198] Directive 95/46/EC Article 2 Paraf H
[199] GDPR Article 8
[200] This condition will usually also satisfy the condition in Article 6(1)(c) for the legal obligation. See. Legal İnterest P.37
[201] Kuner, C., Docksey, C., & Bygrave, L. op.cit. P.377

2.3.3. (9/c) Vital interests

The natural person need not be the data owner, it can be another natural person. This legal basis is very limited in scope and generally only applies to matters of life and death.[202] It is similar to the "state of necessity", which is one of the reasons for compliance with the law regulated in some penal laws in the world. This would be useful in an emergency where a person cannot consent (for example, is unconscious), is underage or legally incapacitated, or cannot be found.[203]

2.3.4. (9/d) Not-for-profit bodies:

Not every non-profit organization is covered by this exception. Because, according to GDPR, these organizations must have the purpose of allowing the exercise of fundamental freedoms. In addition, the Organization should be organized without profit. This article applies only to data processing carried out in connection with the purposes of organizations. In another important issue, disclosure to a controller other than the organization requires the consent of the data subject.[204] If the processing requires the data to be shared to third parties, the relevant organization will still require the explicit consent of the data subjects.[205]

2.3.5. (9/e) Made public by the data subject:

Article 9(2)(e) was one of the least discussed provisions in the enactment of the GDPR. This article is a word for word repetition of Article 8(2)(e) of Directive 95/46/EC.[206] This condition does not apply to all public domain special category data. It only applies to personal data that the individual has made public. What matters is not

[202] Kuner, C., Docksey, C., & Bygrave, L. op.cit.. P.378

[203] Carey, P. (2018). *Data protection: a practical guide to UK and EU law*. Oxford University Press, Inc..P.73

[204] Kuner, C., Docksey, C., & Bygrave, L. op.cit. P.378

[205] Carey, P. (2018). Op.cit.P.73

[206] Common Position (EC) No 1/95 Adopted By The Council On 20 February 1995 With A View To Adopting Directive 95/. . ./EC Of The European Parliament And Of The Council Of. On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (95/C 93/01 ,The Council Of The European Communities. Official Journal L, No C 93/1, Available At: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51995AG0413(01)&from=EN. Last Visited 08.03.2022,

whether, in theory, "mentioned in a publication in a specialist library, or in court" is in the public domain, but whether it is actually in the public domain in practice.[207] This condition does not cover all special category data in the public domain. It covers only the personal data that the individual himself has publicly disclosed.[208]

2.3.6. (9/f) Legal claims or judicial acts:

This article has been regulated to protect the right of the EU charter of fundamental rights under Article 47 the Charter, the effective remedy under Article 13 of the ECHR and the right to a fair trial in Article 6 of the ECHR. [209] For example.

- for the establishment of legal claims;
- for the implementation or defense of legal claims; or
- when the courts act according to their own judicial capacity.[210]

2.3.7. (9/g) Reasons of substantial public interest:

In contrast to the conditions for the processing of personal data based on a task set out in the general processing conditions in Article 6(1)(e), the public interest must be 'important' when processing sensitive data. So, what is this important public good? The Data Protection Act of 2018 in the UK defines an important public interest as follows: Substantial public interest means the public interest needs to be real and of substance. [211] The Data Protection Act also regulates "What important public interest conditions exist". The conditions are listed in article 6 to 28, such as “statutory and government purposes, suspicion of terrorist financing or money ,equality of opportunity or treatment, racial and ethnic diversity at senior levels.[212]

---

[207] Edward S., Jiahong C., (2021) What does it mean for a data subject to make their personal data ‘manifestly public’? An analysis of GDPR Article 9(2)(e), International Data Privacy Law, Volume 11, Issue 2, Pages 107-124, https://doi.org/10.1093/idpl/ipab005 P.117

[208] ICO," What are the conditions for processing?", (n.d) ,Available At. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing. Last Visited 10.03.2022

[209] Kuner, C., Docksey, C., & Bygrave, L. op.cit. P.379

[210] Carey, P. op.cit P.74

[211] ICO, op.cit.,

[212]ICO, op.cit.

2.3.8. (9/h) Health or social care:

It includes exceptions for the following purposes in the processing of sensitive data for health care purposes for preventive or occupational medicine, assessment of worker's work capacity, medical diagnosis, provision of health or social care or treatment, management of health or social care systems and services.[213] In addition, with regard to the processing of health data, Member States may provide or impose other conditions, including limitations on the processing of genetic data, biometric data or health-related data. This article coincides with the public interest in Article 6(1)-(E).

2.3.9. (9/i) Public health:

This paragraph covers the processing of sensitive data for the public interest in the field of public health. For data processed under this exception, the right to erasure in accordance with the article "(17) (1). (c)" does not apply.[214] One of the most important issues of today, Covid 19, which started in March 2020 and was declared as a pandemic by the World Health Organization, is directly related to this paragraph. The processing of all health-related personal data must comply with the data protection principles set out in Article 5 of the GDPR. One of the legal grounds set out in Articles 6 and 9 of the GDPR. [215] First, the consent of the data subject pursuant to Article 6 (1) (a) and Article 9 (2) (a) GDPR can provide a legal basis for the processing of health-related data under COVID-19. Furthermore, Article 9 (2) (j) or Article 9 (2) (i) GDPR may provide a legal basis for the processing of personal health data for scientific research. However, it should be emphasized that the processing of such data for other purposes is prohibited. It cannot be used for other purposes or by third parties.

---

[213]HRB, "Special category personal data", (n.d), Available At: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-overview/special-category-personal-data. Last Visited 15.03.2022

[214] GDPR Article 17 paraf 2.(c) " Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);"

[215] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, Adopted on 21 April 2020, Available At: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf. Last Visited 19.03.2022, P.6

2.3.10. (9/j) Archiving, research and statistics:

According to this condition, the archiving purposes of processing should be in accordance with the public interest. Data Processing must also be proportionate, respect the essence of the right to data protection and provide appropriate and specific safeguards. However, Proportionality will generally require data to be processed only as far as absolutely necessary.[216] . Moreover, according to the GDPR, this condition must comply with Article 89(1) of the Regulation.[217]

Processing of special categories of personal data may only be processed when processed by or under the responsibility of a professional subject to professional secrecy under Union or Member State law, or for the purposes referred to in paragraph 2(h).[218]

However, Member States may impose new conditions, including limitations on the processing of genetic data, biometric data or health-related data.[219] In this context, legal regulations that will be introduced in such a way as to exceed the GDPR framework are prohibited. In addition, the arrangements made by the member states should not contradict the fundamental rights and freedoms at the same time.

2.4. Processing of Biometric Data

According to Article 4(2) of the GDPR, the processing of personal data consists of the following: "Collection", "recording", "organization", structuring, "storage", "adaptation" or "alteration", "retrieval", "consultation", "use", "disclosure by transmission", "dissemination or otherwise making available", "alignment or combination", "restriction", "erasure or destruction".[220] As can be seen, these actions are counted as limited. In some country legislations, these actions can be broad or narrow. For example, more acts are included in the Turkish Personal Data Protection Law.

---

[216] Kuner, C., Docksey, C., & Bygrave, L. op.cit. P.379

[217] Article 89 regulates " Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".

[218] GDPR Article 9 paraf 3

[219] GDPR Article 9 paraf 4.

[220] GDPR Article 4 paraf 2

Just as important as with which action the Biometric data is processed, it is very important by whom it is processed. Biometric data can be processed by automation systems as well as manually.

Artificial intelligence systems can process personal data. Because personal data can contribute to the data sets used to train machine learning systems, that is, to create their algorithmic models. In addition, artificial intelligence systems, from personal data; can generate information, make predictions and use the data obtained.[221] Thanks to artificial intelligence, all kinds of personal data (including biometric data and other sensitive data) can be used to analyze, predict and influence human behavior.[222]

2.5. Automated Individual Decision-Making, Including Profiling

Automatic decision making, which has been used in recent years, is used in the fields of law, health, bots, autonomous vehicles, transportation, media, education, social media, etc. Automated decision-making mechanisms have social concerns as well as benefits. For example, while big data analytics can help drive business decisions, it can also anonymize social media data, compromising users' privacy.[223]

However, the potential benefits may outweigh the societal concerns they pose. This mechanism is used in areas such as evaluation, monitoring and recognition by processing computer programs, natural language processing and machine learning databases, which are types of artificial intelligence.

Working Party 29 defined automatic decision-making as the ability to make decisions with technological tools without human intervention based on any kind of data. In addition, Working Party 29 gave the following examples. Data provided directly by relevant persons (such as responses to a survey), observed data about

[221] Gibson, A., Tessa, M., "Artificial Intelligence In The Public Sector – Inference And Collection" (2020), Available At:https://ovic.vic.gov.au/blog/artificial-intelligence-in-the-public-sector-inference-and-collection. Last Visited 19.03.2022

[222] Giovanni Sartor; Francesca Lagioia, (2020), op.cit. P.1

[223] Wouters, N., Kelly, R., Velloso, E., Wolf, K., Ferdous, H. S., Newn, J., ... & Vetere, F. (2019, June). Biometric mirror: Exploring ethical opinions towards facial analysis and automated decision-making. In Proceedings of the 2019 on Designing Interactive Systems Conference (pp. 447-461) P. 447

individuals (such as location data collected through an app), derived or inferred data such as a previously created person's profile such as a credit score.[224]

The GDPR limits the use of automated individual decision-making. According to Article 22 "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"[225]

Article 22 Paragraph (2) sets out 3 exceptions as follows: In these cases, article 1 shall not apply.

1-) In case a contract is concluded between the data subject and the data controller or the performance of the contract is necessary for the automatic decision

2-) In case the automatic decision is authorized by Union or Member State law to which the controller is subject and which also determines appropriate measures to protect the rights and freedoms and legitimate interests of the data subject

3-) In case the decision is based on the explicit consent of the data subject.

A data system, when processed through a data acquisition method, attempts to predict the behavior and character of individuals. This situation emerges as profiling and segmentation in the doctrine.[226] Artificial intelligence systems usually aim to provide inferences (classifications, predictions or decisions) when applied to data about individuals. Artificial intelligence and big data, along with the availability of extensive computing resources, have greatly increased profiling opportunities. For example, the probability of heart disease for insurance applicants can be estimated based on their health records, as well as on their habits (eating, physical exercise, etc.) or social conditions. The probability of condemned to re-offend can be estimated based on their

[224] Party, A. D W, *Article 29 data protection working party guidelines on automated individual decision-making and profiling for the purposes of regulation*, 2016/679, (2017), Available At: https://ec.europa.eu/newsroom/article29/redirection/document/49826.Last Visited 28.03.2022 P.8

[225] GDPR Article 22

[226] Aliyev, A. I., Rzayeva, G. A., & Ibrahimova, A. N. (2021). "Artificial Intelligence and Personal Data: International and National Framework". Peace Human Rights Governance, 5(1). 97-123 P.112

criminal history, as well as their personality traits and backgrounds. These estimates can cause automatic determinations of the price of a health insurance or parole, respectively.

Automated decisions can be made with or without profiling, and profiling can be done before or after automated decisions are made. Profiling and automated decision-making, on the other hand, are not always distinct activities. Depending on how the data is used, something that starts out as a simple automated decision-making process could evolve into one based on profiling.[227] For instance, applying speeding fines based merely on data from speed cameras is an automated decision-making process that does not need profiling. However, monitoring of the individual's driving habits over time and whether it is the result of an assessment that includes factors such as the amount of fine imposed will become a profiling decision. [228]

Decisions that are not solely automated might also include profiling. For example, before granting a mortgage, a bank may consider the credit score of the borrower, with additional meaningful intervention carried out by humans before any decision is applied to an individual. [229]

Automated decision mechanisms and profiling are increasingly used by companies and countries around the world, especially to predict behaviour and needs. A study conducted by the AI Now Institute[230] in the United States has identified the uses of automated decision-making systems. The usage areas of automatic decision-making systems in this research are as follows. Child Welfare, Criminal Justice, Education, Fire, Healthcare, Housing: Used for multiple purposes, but most importantly for "Residential Face Authentication, Immigration and Policing.[231] However, banking

[227] Party, A. D. W. op.cit. .P.2
[228] Ibid., P.8
[229] AI Now, *Automated Decision Systems Examples Of Government Use Cases Issue:* (n.d), Available At: https://ainowinstitute.org/nycadschart.pdf. Last Visited 25.03.2022 P.1-6.
[230] The AI Now Institute at New York University is an organization that seeks interdisciplinary research and public engagement to help ensure AI systems are accountable to the communities and contexts in which they are applied. See. https://ainowinstitute.org/
[231] The AI Now Institute, op.cit. P.1-6

and finance, healthcare, tax, insurance, marketing and advertising are just a few of the areas where profiling is performed more regularly to aid decision making. [232]

2.5.1. Use of Automated Decision-making Systems in the Public Sector

The use of automated decision-making systems in public sector is increasing. It is likely to increase further in the coming years. Automated Decision-Making Systems are used for a variety of purposes, including processing social benefit requests, detecting welfare fraud risks, profiling unemployed people, law enforcement predictive policing, tax evasion, and terrorist activities and assessing parolee recidivism risks.[233]

While Automated Decision-Making Systems bring many conveniences and benefits to the public, it also carries significant concerns. Some of the more prominent concerns mentioned in response to open-ended questions include the following: First is privacy. The highest personal finance score is given as an example for privacy. Second fairness. People worry about the personal finance score scenario, job interview, and automatic screening of job applicants, because people think they are unfair. The third concern is removing the human element from important decisions. It is a prominent concern among those who are particularly concerned about the use of video business call analytics. Finally, people have stated that "humans are complex, and these systems are incapable of capturing nuance." This is especially prominent for those who find the use of criminal risk scores to be unacceptably high.[234]

Governments today have access to a great deal of data collected by public institutions for record keeping. Advances in automated decision making in data processing and analysis can help unlock the value of data, automate repetitive tasks, understand citizen needs, and therefore fuel innovative services. Artificial intelligence can help the public sector automate many highly labour-intensive data processing and

[232] Party, A. D. W. op.cit. P.1

[233] Loi, m. in collaboration with Mätzener A., Müller A., and Spielkamp M., "Automated Decision-Making Systems in the Public Sector – An Impact Assessment Tool for Public Authorities, (2021), Available At: https://algorithmwatch.org/en/wp-content/uploads/2021/06/ADMS-in-the-Public-Sector-Impact-Assessment-Tool-AlgorithmWatch-June-2021.pdf. Last Visited 26.03.2022

[234] Pew Research Center, "Public attitudes toward computer algorithms, (2018), USA, Available At: http://refhub.elsevier.com/S0308-5961(20)30068-9/sref45. Last Visited 25.03.2022

analysis activities, thereby increasing the efficiency and speed of government services and actions, thanks to its powerful data processing capabilities. Another important element of the use of artificial intelligence in the public sector is predictive power. Countries resort to comparing similar policies abroad, conducting policy trials, or developing statistical models that help predict possible outcomes.[235] For example, after the spread of the Corona virus, an algorithmic system was implemented in Qatar to estimate the impact of the quarantine policy on COVID-19 cases, which helped create the social restraint policy.[236] As a result, it is seen that automated decision-making systems have benefits in public use and can help solve problems. But it has a long way to go in use and reliability. The use of algorithms is not only a matter of whether they are fair and safe to use, but also whether they comply with the law and whether they actually work.[237] This will determine the future of automated decision-making systems in public use in the next century.

2.5.2. Use of Automated Decision-making Systems in the Private Sector

The private sector is one of the areas where automated decision-making services are used a lot. Profiling and automated decision-making systems could be useful for the private sector. Moreover, automated decision-making systems benefit in many sectors, including healthcare, education, financial services and marketing. Especially in cases where a very large amount of data needs to be analyzed and decisions to be made very quickly, they can make faster and more consistent decisions.[238]

---

[235] Pi, Y. (2021). "Machine learning in Governments: Benefits, Challenges and Future Directions". JeDEM-eJournal of eDemocracy and Open Government, 13(1), 203-219. P.205-206

[236] Said, A. B., Erradi, A., Aly, H., & Mohamed, A. (2020). "A deep-learning model for evaluating and predicting the impact of lockdown policies on COVID-19 cases". arXiv preprint arXiv:2009.05481. As Cited in: Pi, Y. (2021). "Machine learning in Governments: Benefits, Challenges and Future Directions" JeDEM-eJournal of eDemocracy and Open Government, 13(1), 203-219. P.206

[237] Waller, M., & Waller, P. (2020). "Why Predictive Algorithms are So Risky for Public Sector Bodies." Available at SSRN: https://ssrn.com/abstract=3716166 or http://dx.doi.org/10.2139/ssrn.3716166 Last Visited 27.03.2022, P.2

[238] ICO,"What is automated individual decision-making and profiling?", (n.d), Available At https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/: . Last Visited 23.08.2022

Automated decision-making systems help businesses run more efficiently. The automatic processing of data and other information causes companies to work faster, make fewer mistakes and run their business effectively. For example, GiniMachine increased loan portfolio return by over 30% while reducing bad loans by up to 50% using automated decision-making support systems powered by artificial intelligence technology.[239]

2.5.3. Use of Automated decision-making systems for individuals

Automated decision-making systems is increasingly used by state and private actors. However, it raises many concerns, especially for individuals.[240] Automated decision-making systems can undermine fundamental principles such as equality, privacy, dignity, autonomy and free will and also pose risks to health and quality of life. Another major concern is that automated decision-making systems may discriminate in many areas, including the judicial system, credit scoring, targeted advertising and employment. [241] Automated decision-making systems are used to determine the allocation of loans and jobs, the treatment of incarcerated people, the investigation of taxpayer fraud, and the prioritization of health treatments, either with or without human input.[242]

Article 22 of GDPR prohibits automated processing (including profiling) that produces legal or other material effects, with three legal exceptions. In this context, it can be said that "Profiling" is one of the most basic topics that should be examined in terms of the effects of algorithms on individuals.[243] For example, profiling a person's actions, behavior, or opinions and making various decisions based on the results will

[239] For more details, See: https://ginimachine.com/blog/how-automated-decision-making-revolutionizes-business/ Last Visited 22.08.2022

[240] Binns, R. (2019). "Human Judgment in algorithmic loops: Individual justice and automated decision-making". Regulation & Governance. P.1

[241] Castelluccia, C., & Le Métayer, D. *Understanding algorithmic decision-making: Opportunities and challenges,* (2019), *European Parliament.* Available At: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)624261. Last Visited 01.04.2022, P.II

[242] Binns, R. op.cit. P.1

[243] Dülger, M. V., Çetin, S , Aydınlı C, (2021)." Algoritmik Karar Verme ve Veri Koruması (Algorithmic Decision Making and Data Protection)." Available at SSRN: https://ssrn.com/abstract=3792207 or http://dx.doi.org/10.2139/ssrn.3792207 . Last Visited 03.04.2022 P.5

lead to an impact in many areas, such as whether the person should be hired, whether they can withdraw loans from banks, and determining insurance premiums.[244]

In this context when profiling is evaluated in terms of individuals, profiling not only leads to new pervasive and continuous forms of control and monitoring over individuals, but can also lead to increased prejudice and discrimination, leading to social exclusion or marginalization.[245]

3. Directive 95/46/EC

Directive 95/46/EC is also known as the Data Protection Directive. It entered into force in October 1995. With the entry into force of the general data protection regulation on 25 May 2018, Directive 95/46/EC has been repealed. Directive 95/46/EC can be considered the first piece of legislation to harmonize data protection laws within the European Union.[246] The purpose of "Directive 95/46/EC" is to protect the fundamental rights and freedoms and privacy rights of persons related to the processing of personal data.

Article 6 of Directive 95/46/EC regulates the principle of Transparency and information of the data subject. According to the principle of fair processing, data subjects should be aware of the collection and/or use of their biometric data. [247] Biometrics data are defined as sensitive data within the scope of Article 8 of Directive 95/46/EC. Processing of biometric data, the legality of data processing is listed in

[244] Arslan, Z., "Yapay Zeka Ve Over The Top Hizmetler Araciliğiyla Profilleme", (2019), Available At: https://www.rskveri.com/yapay-zeka-ve-over-the-top-hizmetler-araciligiyla-profilleme. Last Visited 05.04.2022

[245] Del Gamba, G.,"Machine learning, risks and benefits of automated decisions". (2020), Available At. https://www.insuranceup.it/en/opinions/machine-learning-risks-and-benefits-of-automated-decisions. Last Visited January 25, 2022

[246] Wong, R. (2012). "The data protection directive 95/46/EC: idealisms and realisms. International Review of Law, Computers & Technology, 26(2-3), 229-244. P.229

[247] Article 29 Data Protection Working Party, (2012) *Opinion 3/2012 On Developments In Biometric Technologies*, op.cit. P.14

Article 7 Grounds of legitimacy "Consent, Contract, Legal obligation, Legitimate interests of the data controller". specified as.[248]

As for what has changed by the GDPR compared to the previous Data Protection Directive: There was no "extra-territoriality" principle in the directive. But the GDPR stipulates that any entity that processes the personal data of EU residents around the world is liable to the provisions of the GDPR. There was no obligatory report of data breaches in the directive. But it is regulated with GDPR. In this context, Each data controller must notify the Supervisory Authority in case of potential or real leakage of personal data without undue delay (max. 72 hours). [249]

GDPR has extended definition of personal information to include new forms of protected personal data like IP addresses, mobile device identifiers, geolocation, biometric data. Another difference between the DPD and the GDPR is the addition of regulation of data processors. Under the directive, only data controllers were held accountable for anything wrong. Processors will also be responsible for the security of personal data.[250]

GDPR builds on the core principles of the DPD, with more specific data protection requirements, a global scope, and stricter sanctions, as well as non-compliance penalties. As a result, citizens will have more control over their personal data and more recourse in the event of personal data violation, while data controllers and processers will be required to protect sensitive personal data by design. Finally, GDPR provides a much understandable and simpler regulatory environment for businesses that collect or process the personal data of EU citizens and residents. [251]

---

[248] Directive 95/46/EC Article 7

[249]Ivan Klekovic,"EU GDPR vs. European data protection directive", (2017), Available At https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/: . Last Visited 30.08.2022

[250] Seeunity, “The main differences between the DPD and the GDPR and how to address those moving forward”, (2017), Available At: https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf. Last Visited26.07.2022

[251]Nate Lord, “What is the Data Protection Directive? The Predecessor to the GDPR”, (2018), Available At:https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr. Last Visited 08.04.2022

4. Law Enforcement Directive (LED)

Parallel to the GDPR, the Law Enforcement Directive is a piece of EU legislation that went into effect in May 2018. LED regulates the processing of personal data (including biometric data) by data controllers for law enforcement purposes that fall outside the scope of the GDPR.[252] The LED only provides law enforcement with general guidelines in Article 4(1).

Article 10 of LED regulates Processing of special categories of personal data. The processing of biometric data, which is sensitive personal data, is permitted only in cases where it is absolutely necessary and subject to appropriate safeguards for the rights and freedoms of the data subject. Other processing conditions within the scope of Article 10 are as follows. Where authorised by Union or Member State law, protect the vital interests of the data subject or any other natural person; or where such processing relates to data that has been expressly made public by the data subject.

Paragraph 3 regulates that profiling that discriminates against natural persons based on sensitive data is prohibited. The LED also regulates that the Member States require appropriate security measures, including privacy and current status, especially in relation to special categories of personal data, such as biometric data. These cover measures like user control, storage control, access control and integrity.[253]

When it comes to concerns at law enforcement directive; Transparency is not required in data processing in the Law Enforcement Directive (LED). In this context, provisions on transparency could have been included. In addition, the obligation to minimize the amount of personal data collected in the Law Enforcement Directive (LED) is weaker compared to the GDPR. In this context, it can be at least equivalent to GDPR.

[252]Data Protection Commission,, "Law Enforcement Directive,(n.d), Available At:https://www.dataprotection.ie/en/organisations/resources-organisations/law-enforcement-directive. Last Visited 08.04.2022

[253] Wendehorst, C., & Duller, Y. op.cit. P.27

5. Council Regulation No 2252/2004

On 13 December 2004, the Council adopted Regulation No 2252/2004, which stipulates the mandatory application of biometrics in EU passports. The purpose of this regulation is to integrate biometrics into European passports to strengthen the link between the passport and the person holding the passport and facilitate the verification of the authenticity of the passport.[254] According to Article 1(2) of the Regulation, Data must be protected and the storage medium must have adequate capacity and capability to ensure the integrity, authenticity and confidentiality of the data.[255] In the *Stadt Bochum, Mr. Schwarz* case; Mr. Schwarz applied to the Stadt Bochum for a passport. Mr. Schwarz didn't ask for his fingerprints to be taken. Thereupon the Stadt rejected Bochum's application. Mr. Schwarz appealed to the court, demanding that he be given a passport without fingerprints. There upon the ECJ was asked whether the imposition of the requirement to store fingerprints of Article 1-(2 of Regulation (ECTHR) no 2252/2004 regulating the issuance of passports by member states was contrary to the "Right to respect for private life" and “Right to the protection of personal data”. However, In the decision; it was concluded that the interference arising from Article 1(2) of Regulation 2252/2004, CJEU, was justified with the aim of protecting against fraudulent use of passports.[256]

In another case; Mr Willems and Ms Roest and Ms van Luijk have applied for an identity card for a passport. However, they refused to provide fingerprints and a facial image during the application. Their application was rejected on the grounds that they did not provide fingerprints. The applicants stated that it constituted a serious violation of their physical integrity and right to private life. In addition, the applicants were concerned that it was stored in three different environments, including the decentralized database. The court of first instance dismissed the case and the applicants appealed. In this context, the appeal court (Raad van State) decided to ask CJEU for

[254] Dumortier, F. (2018). “PROTECT (Pervasive and UseR Focused BiomeTrics Border Project): D2. 2 Legal framework of biometric border control.” Available At: https://researchportal.unamur.be/en/publications/protect-pervasive-and-user-focused-biometrics-border-project-d22. Last Visited 25.04.2022 P.19

[255] Council Regulation (EC) No 2252/2004 Article 1 Paragraph 2

[256] Case C-291/12 Schwarz v Stadt Bochum , (2013),Para 64

preliminary ruling. The referring court's question was whether Article 1(3) of Regulation 2252/2004 applies to identity cards, both at the domestic level and within EU law. According to Article 1(3), second sentence, Regulation 2252/2004 does not apply to identity cards or temporary passports issued by Member States to their nationals and to travel documents with a validity of 12 months or less. Consequently, the fact that identity cards such as Dutch identity cards can be used for travel purposes within the European Union and in a limited number of non-Member States do not fall within the scope of Regulation 2252/2004.[257]Public authorities are not allowed to request data, if there is no legal basis to do so to collect the data. Actions by public authorities must comply with laws that protect our fundamental rights.[258]

Article 1 regulates that only the staff of the national authority responsible for issuing passports will be authorized to collect biometric identifiers and that they will do so in accordance with the ECHR and the UN Convention on the Rights of the Child. [259] For the purposes of this regulation, biometric features in passports and travel documents will only be used to verify the authenticity of the document and the identity of the holder when it is required by law to present a passport or other travel document.[260]

When the regulation came into effect, facial recognition systems were 2D. In 2-D face recognition systems, it could affect the orientation and alignment of the face (posture), changes in lighting conditions, and other skewed factors. Also, there was no proven reliable vitality detection in 2D face recognition Systems. This situation was criticized in terms of security at that time.[261] 3D face recognition systems offer improved robustness while being able to handle changes in poses and challenging lighting conditions during image acquisition by combining the geometry- and texture-channel information of the face.[262] The 3D Face project was launched in April 2006.

[257] Joined cases C-446/12 to C-449/12 Willems et al. v Burgemeester van Den Haag, (2015), Para34
[258] Katarzyna Stachyra , "ECJ: no legal basis for biometric data in ID cards",(2015), Available At: https://europensblog.wordpress.com/tag/joined-cases-c-44612-to-c-44912. Last Visited19.03.2022
[259] Wendehorst, C., & Duller, Y. op.cit. P.28
[260] Council Regulation (EC) No 2252/2004 Article 4 Paragraph 3
[261] Busch, C., Nouak, A., Zhou, X., van der Veen, M., Deravi, F., & Suchier, J. M. (2007, September). *Towards unattended and privacy protected border control.* In 2007 Biometrics symposium (pp. 1-6). P.1,5
[262] Ibid., P.1

The transition from two-dimensional to three-dimensional facial recognition systems promises a better verification procedure. [263]

6. Biometric Border Control Regulations

The European Commission gives two reasons for border management regulations. These are migrations and terror concerns. In this context, there are four systems developed by the EU for border management. I. The Schengen Information System (SIS) II. The Visa Information System (VIS), III. The Entry-Exit System (EES) IV. The EURODAC system [264]

(SIS) is a system used in the fight against crime, illegal immigration and terrorism, helping to increase security in the region by sharing information between participating countries. SIS was established in 1990 for "Border control cooperation", "Law enforcement cooperation" and Cooperation on vehicle registration.[265] Photographs (not facial images) and fingerprints are biometric data that can be processed in the SIS II database for border control management purposes.[266] In this context, facial images and fingerprints are included in the system through the Automatic Fingerprint Identification System (AFIS) regulated in the Article 22(c) and facial images regulated in the Article 28 (4), Article 22 (a) of Regulation 1987/2006 regulates " Specific rules for photographs and fingerprints". According to the Article 2(b) " photographs and fingerprints could only be used to authenticate third-country nationals located as a result of an alphanumeric search in SIS II."[267]

(VIS) connects consulates in non-EU countries with all Schengen States' external border crossing points. It processes information about applications for short-term visas to visit or transit through the Schengen Area. For identification and verification, the system can perform biometric matching, primarily of fingerprints. Ten

[263] Busch, C., Nouak, A., Zhou, X., Suchier, J. M., Kelkboom, E., & Kevenaar, T. (2008). "3D Face Recognition for Unattended Border Control". Security and Management, *8*, 350-356.P.355
[264] Dumortier, F. op.cit. P.49
[265] ETIAS, The Schengen Information System: Keeping Europe Safe, (2022Available At: https://www.etiasvisa.com/etias-news/schengen-information-system-sis). Last Visited 15.04.2022
[266] Dumortier, F. op.cit P.49
[267] Regulation 1987/2006 Article 22

fingerprints and digital photographs are taken from visa applicants. On the other hand, ten-digit finger scan is not required from children under the age of 12 or those who cannot physically provide finger scanning. After the finger scans are stored in the Vis, they can be reused for a period of 5 years for subsequent visa applications. Access to VIS data is limited to authorized personnel in the performance of their duties. In addition, any person can demand the correction of incorrect information about himself and the deletion of illegally recorded data.[268]

According to Article 1 of Entry-Exit System Regulation 2017/2226, EES has been prepared for the following purposes.

I. Prevention and investigation of terrorist crimes or other serious criminal offenses.
II. Registration of entry and exit times and places of third-country nationals entering and leaving the borders of Member States.
III. Calculation of the period of stay of third country nationals,
IV. Registration and storage of place and time of refusal of entry of citizens of third countries.
V. Issuing warnings to member States when the permitted period of stay has expired.

EEC will store biometric information of non-EU visitors traveling. Thanks to EEC, manual stamping of passports will be replaced by automatic monitoring. [269]This new system regulates the registration of non-EU citizens with data such as name, travel document, date of birth, as well as biometric data such as fingerprints and facial images when entering and leaving the Schengen area. The retained data will be stored for a period of five years for those who remain for three years or more. EES would normally

[268]European Commission,," Visa Information System (VIS)",(n.d) Available At: https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/visa-information-system_en. Last Visited 18.04.2022

[269]Edri, "Smart Borders: the challenges remain a year after its adoption", (2018), Available At: https://edri.org/our-work/smart-borders-the-challenges-remain-a-year-after-its-adoption. Last Visited 20.04.2022

come into effect in 2020. However, due to Covid, it will enter into force in October 2022.[270]

EURODAC Regulation (EU) No 603/2013 aims to receive and process asylum applications from persons who may need protection in a reasonable and transparent manner. EURODAC includes fingerprints. It does not contain any other personal information.[271]

7. EU Artificial Intelligence Act

The European Commission presented the Artificial Intelligence Act on April 21, 2021. The proposed regulation aims to codify the EU's high standards for trustworthy artificial intelligence systems. Artificial intelligence can produce socially and environmentally beneficial results by improving forecasts, optimizing operations and resource allocation, and personalizing service delivery. Thanks to artificial intelligence, companies and the European economy can also provide significant competitive advantages.[272] In the proposal of the regulation, it was emphasized that artificial intelligence rules should be people oriented. It establishes core horizontal rules that apply to all industries for the development, trade, and use of AI-driven products, services, and systems within the EU's territory. [273]

Specific objectives for the artificial intelligence regulation proposal have been set by the European Commission as follows:

[270]European Comission, "Entry/Exit System (EES)",(n.d) Available At: https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en. Last Visited 20.04.2022

[271] Eurepean Comission, EUROCAD "(European Asylum Dactloscopy Database)", (2022), Available At:https://knowledge4policy.ec.europa.eu/dataset/ds00008_en. Last Visited 20.04.2022

[272] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts P.4

[273] Kop, M. (2021, September). *EU Artificial Intelligence Act*: The European Approach to AI. Stanford-Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, Issue. P.1

I. Ensuring that artificial intelligence systems used in the borders of the European Union are safe, and that fundamental rights, values and laws of the European Union are respected

II. Ensuring legal certainty in order to encourage artificial intelligence investment and innovation

III. Improving the administration and effective enforcement of existing law on fundamental rights and security requirements that apply to artificial intelligence systems

IV. Facilitating the development of a single market for legal, safe and reliable artificial intelligence applications and preventing market fragmentation.[274]

In the title of definitions in the 3rd article of the proposal, it defines 3 types of biometric data that are only processed by artificial intelligence. These are: emotion recognition, biometric categorization and biometric identification systems.[275]

The proposal proposes restrictions and protective measures[276] for certain uses of remote biometric recognition systems for law enforcement purposes, while prohibiting some particularly harmful artificial intelligence applications as they are contrary to European Union values. Another important point is the establishment of a governance system at the Member State level with the additions to be made on existing regulations and existing structures, and the establishment of a cooperation mechanism at the Union level with the establishment of the European Artificial Intelligence Board. It is also recommended to take measures such as regulatory sandboxes for artificial intelligence to support innovation, which is one of the objectives of the proposal, and other measures to reduce the burden of administration and support Small and Medium Enterprises (SMEs) and start-ups. In conclusion, it can be said that this proposal

[274] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative P.6

[275] These definitions are listed from article 3(34) to item (38) in the artificial intelligence proposal.

[276] Restrictions and protective measures for certain uses of remote biometric recognition systems" will be examined in section 7.1.1. Real-time and Post Remote biometric identification

introduces a proportional regulatory system that does not create unnecessary restrictions on trade and focuses on a well-defined risk-based regulatory approach.[277]

7.1. Biometric techniques under AIA Proposal

7.1.1. Real-time and Post Remote biometric identification

In the proposal, the term remote biometric identification is used to discuss the regulation of certain facial recognition uses. In Article 3(36) of the proposal, the definition of "remote biometric identification system" is made by the Commission. According to this definition, remote biometric identification system refers an artificial intelligence system for identifying individuals 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 artificial intelligence system whether the person will be present and can be identified.[278] In the 29 Working party biometric identification's definition; Identifying a person by a biometric system is typically the process of comparing an person's biometric data to a set of biometric templates stored in a database.

In the proposal, the European Commission also regulated the live face recognition system under the definition of 'real-time remote biometric identification systems'. In the relevant definition; Real-time remote biometric identification system refers to a remote biometric identification system in which the capture of biometric data, comparison and identification takes place without notable delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention."[279] As it can be seen three elements were given in this definition. These are artificial intelligence systems that search for people using biometric data.[280] Real-time remote biometric identification systems can be exemplified as footage, generated

[277] Artificial Intelligence Act (Proposal). Op.cit P.6
[278] Artificial Intelligence Act (Proposal). Op.cit Article 3(36)
[279] Artificial Intelligence Act (Proposal). Op.cit Article 3(37)
[280] Fuster, G. G., & Peeters, M. A. N. (2021). *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics In The Era of Artificial Intelligence.*, Available At: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)69719. Last Visited 02.03.2022, P.14

by a camera or other device.[281] The use of real-time remote biometric identification systems in public areas for law enforcement purposes is also prohibited, unless certain limited exceptions apply, along with artificial intelligence-based social scoring for general purposes made by public authorities.[282]

In addition, the definition of "post remote biometric identification system" is also made in the proposal; the biometric data have already been captured and the comparison and identification occur only after a long period of time. This includes content, such as pictures or video footage created by closed circuit television cameras or private devices, which has been created before the use of the system in respect of the natural persons concerned.[283]

7.1.2. Biometric categorisation

In the Article 3(35) of the proposal, the definition of "biometric categorisation system" is made by the Commission. According to this definition; An AI system that assigns natural persons to particular categories based on their biometric data is referred to as a biometric categorization system.[284]

In the 29 Working Party's definition of biometric categorization; Categorization of an person by a biometric system is the process of determining whether an individual's biometric data belongs to a group with some predefined characteristics, typically to perform a particular action. In this situation, automatically classifying the person is more important than identifying or confirming them. For example, an ad screen might show different ads depending on the person that is looking at it based on age and gender.[285]

---

[281] Madiega, T. & Mildebrath, H.(2021). *Regulating facial recognition in the EU. European Parliamentary Research Service*, Available At: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. Last Visited 02.03.2022, P.25

[282] Artificial Intelligence Act (Proposal). Op.cit P.16

[283] Artificial Intelligence Act (Proposal). Op.cit Article 3-36

[284] Artificial Intelligence Act (Proposal). Op.cit Article 3-35

[285] Article 29 Data Protection Working Party, op.cit. P.6

7.1.3. Emotion Recognition

"Emotion Recognition" uses machine learning to determine the emotional state of individuals. " "Emotion Recognition" is a biometric technique that separates people's emotional states into separate categories such as anger, surprise, fear, happiness, etc. Input data includes individuals' faces, body movements, tone of voice, speech and physiological signals (e.g. heart rate, blood pressure, breathing rate).[286]

In article 3(34) of the proposal, the definition of "Emotion recognition system" is made by the Commission. According to this article; An artificial intelligence system known as a "emotion recognition system" is used for identifying or inferring the emotions and intentions of individuals based on their biometric data.

Emotion recognition, like other biometric technologies (such as facial recognition), involves the mass collection of sensitive personal data in invisible and unaccountable ways, allowing for the tracking, monitoring, and profiling of individuals, often in real time.[287]

Global companies are continuing their work on emotion recognition technology in order to teach computers how to predict human behaviour. Amazon, Microsoft and Google, such as the American technology giant offers all the basic emotion analysis, while smaller companies like HireVue and Affectiva Automotive, used to test various films, including their reactions to DisneyStar Wars. Auto companies like Ford, BMW, and Kia Motors are developing emotion recognition to assess drivers' alertness. Emotion recognition systems for public spaces have started to receive funding to be used by Lincolnshire police in England to identify suspicious people. In addition, emotion recognition system has been installed in Xinjiang, a northwestern Chinese region where about 1 million captured Uighur Muslims are being held in detention camps. According to market size research firm Markets and Markets, the money spent on emotion recognition systems is projected to almost double from $19.5 billion in 2020 to $37.1

[286] Marda, V., & Ahmed, S. (2021). *Emotional Entanglement: China's emotion recognition market and its implications for human rights*. Available At: https://www.article19.org/emotion-recognition-technology-report/. Last Visited 05.03.2022 P.10

[287] Ibid., P.10

billion in 2026. As a result, it can be said that Emotion Recognition systems will have a significant impact on the world in the future, from workplaces to schools and public places. [288]

7.2. Risk Based Approach

Artificial intelligence systems are posing significant threats to fundamental rights. Therefore, a risk-based approach is inevitable. The risk-based approach described in the white paper in 2020 was included in the Commission's proposal. The regulation proposal envisaged a risk-based approach. Accordingly, risk types are divided into 4 different categories. A risk-based approach involves determining the scale or scope of risks associated with a specific situation and a recognized threat.[289] Biometric techniques can be assigned to any of four risk levels, depending on their nature and the context in which they are used.[290]

Article 7 regulated the expansion of the scope of the list of risk-based artificial intelligence systems. In this context, the scope of unacceptable artificial intelligence systems cannot be expanded. However, High-risk artificial intelligence systems cannot be expanded by adding new categories, but they can be modified by adding subcategories to already existing ones.

7.2.1. Unacceptable risk (Title II)

Unacceptable risk (Title II) includes artificial intelligence systems that violate fundamental human rights, union values, and therefore are prohibited for use. The use of real-time remote biometric identification systems in public areas,[291] for law enforcement purposes is also prohibited, unless certain limited exceptions apply, along

[288] FT, *Emotion recognition: can AI detect human feelings from a face?*, (2021), Available At: https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452. Last Visited 06.03.2022

[289] Hidvegi, F., Leufer, D., Masse., Estelle, "The EU should regulate AI on the basis of rights, not risks", (2021), Available At: https://www.accessnow.org/eu-regulation-ai-risk-based-approach. Last Visited 08.03.2022

[290] Wendehorst, C., & Duller, Y. op.cit. P.62

[291] The definition of 'publicly accessible space' is made in Article 3-39 the proposal. "publicly accessible space' means any physical place accessible to the public, regardless of whether certain conditions for access may apply."

with artificial intelligence-based social scoring for general purposes made by public authorities.[292]

Article 5 regulates "Prohibited Artificial Intelligence Practices". In the light of this article, "real-time" remote biometric recognition systems shall be prohibited to be used in public areas for law enforcement purposes. However, In the same article, exceptions to the prohibition of using real-time remote biometric recognition systems in public areas for law enforcement purposes are regulated. These three exceptions are:

The first of these exceptions is the search to identify potential crime victims. This includes missing children. The second exception is the prevention of a significant and imminent threat to the life or physical safety of persons or a terrorist attack. It can be said that this exception was brought for the increasing terrorist attacks in Europe. Third exception: locating, identifying or prosecuting a perpetrator or suspected criminal; and punishable in the relevant Member State by a detention order or custodial sentence for a minimum of three years, as determined by that Member State's law.[293]

7.2.2. High risk (Title III)

Certain rules that pose a high risk to people's health, safety, and fundamental rights are included in the high risk (Title III) category. Accordingly, high-risk artificial intelligence systems are only permitted on the European market subject to certain mandatory conformity assessment or a preliminary conformity assessment. High risk systems are included in Annex III.

In this context, " Artificial intelligence systems used for real-time and remote biometric identification of natural people "[294] are specified as the high-risk AI systems in accordance with Article 6(2).

[292] Artificial Intelligence Act (Proposal). Op.cit P.16
[293] Artificial Intelligence Act (Proposal). Op.cit Article 5-(D)
[294] Annexes To The Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, Article 1-(a)

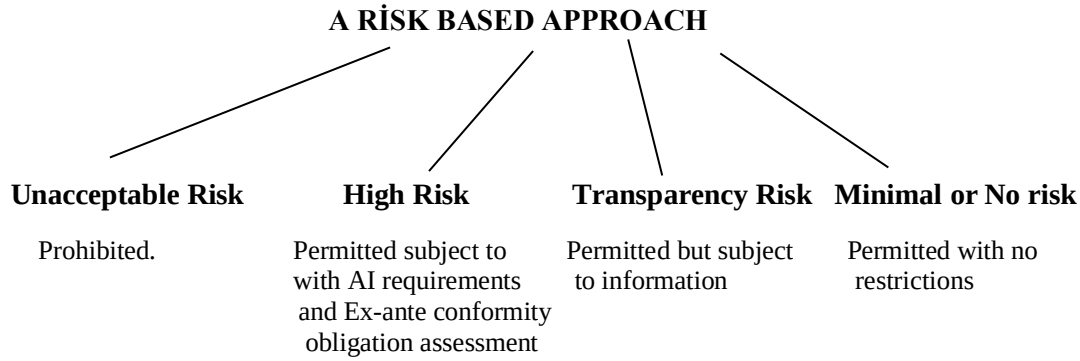
Regulated in Article 6(e) Artificial intelligence systems used for crime analytics on natural real person [295] and Artificial intelligence systems used by competent public authorities as polygraph and similar tools or to detect the emotional state of a natural person [296] regulated in article 7(a) are other high risks listed in annex III.

However, It is worth saying that emotion recognition systems are classified as high-risk only to the extent they are used by law enforcement authorities and by competent authorities in the fields of migration, asylum and border control management.[297]

7.2.3. Transparency Risk (Title IV)

In transparency risk (Title IV), a limited risk is envisaged. This limited risk is subject to the obligation of transparency. Article 52(2) of the proposal is related to emotion recognition and biometric categorization system. According to the relevant article Users of emotion recognition systems and biometric categorization systems must inform about how the systems work.[298] However, there are some exceptions. These exceptions are: artificial intelligence systems that are legally permitted for the detection, prevention, and investigation of crimes. As can be seen, the transparency requirement has been introduced in cases foreseen as limited risk.

[295] Ibid., Article 6(e)
[296] Ibid., Article 7(a)
[297] Blanca Escribano , "Biometric systems in the forthcoming EU Artificial Intelligence Act", (2021), Available At: https://www.ey.com/en_es/law/biometric-systems-in-the-forthcoming-eu-artificial-intelligence. Last Visited 11.03.2022
[298] Artificial Intelligence Act (Proposal). Op.cit. Article 52-2



Figures 1 shows the Figure Risk-based approach of the Artificial intelligence Proposal.[299]

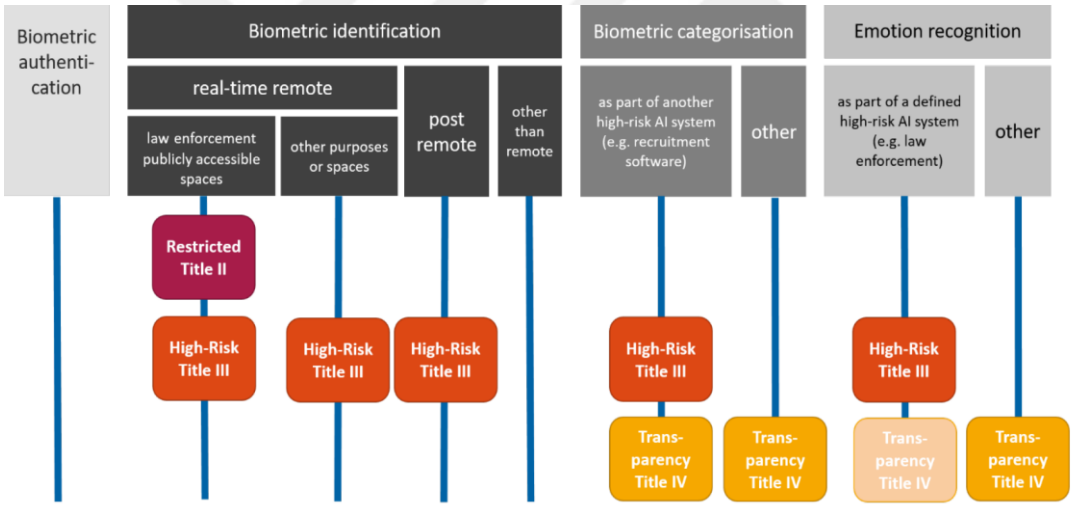


Figure 2 shows that biometric techniques under the AIA Proposal's risk levels. [300]

[299]Mazzini, G., "A European Strategy for Artificial Intelligence" , ELI webinar 'Regulating AI: A First Analysis of the European Commission's Proposal' 29 April 2021 Available At:https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/News_page/2021/Presentation_Gabriele_Mazzini.pdf. Last Visited 20.04.2022

[300]Ibıd.,

V. POSSIBLE SOLUTIONS FOR THE PROTECTION OF BIOMETRIC DATA

A. RECOMMENDATIONS FOR AI SYSTEM

1. Recommendations for Artificial Intelligence Act

In this part of the thesis, "Recommendations for Artificial Intelligence System and Biometric Data" will be examined in the light of why biometric data is important and why it should be protected. In addition, this section will include recommendations from various research and articles conducted in the EU, as well as my personal recommendations on how biometric data should be protected.

1.1. Recommendations for Risk Based Approach

1.1.1. Expanding the scope of the ban on the use of biometric artificial intelligence systems in public spaces[301]

Undoubtedly, one of the most urgent issues in democratic societies today is the regulation of the use of biometric data in public spaces. There is an important global debate on the "red lines" that should be established by the regulators to prevent individuals' freedoms from being endangered as a result of the use of biometric data. [302]

DPB President Andrea Jelinek said live facial recognition systems are interfering with fundamental rights and freedoms. A comprehensive prohibition on the use of facial recognition in public areas should be the necessary starting point if we are to protect our freedoms and create a human-centered legal framework for artificial intelligence. Moreover, the proposed regulation should also ban any use of artificial intelligence for social scoring, as it goes against the core values of the European Union and may cause discrimination. Considering the extremely high risks posed by remote

[301]Lydia Belkadi ," The Proposed Artificial Intelligence Act and Biometric Systems: A Peek Into the Conceptual Maze (Part I))" (2020), Available At: www.law.kuleuven.be /citip/blog/the-proposed-artificial-intelligence-act-and-biometric-systems-part-i/. Last Visited 24.03.2022

[302] Christakis, T., Bannelier, K., Castelluccia, C., & Le Métayer, D. (2022). "Mapping the Use of Facial Recognition in Public Spaces in Europe–Part 1: A Quest for Clarity: Unpicking the'Catch-All'Term". *Available at SSRN 4110512*. P.1

biometric identification of individuals in publicly accessible spaces, the EDPB and EDPS recommend a comprehensive prohibition on any use of Artificial intelligence for automated recognition of human features in publicly accessible spaces, such as face recognition, gait recognition, fingerprints recognition, DNA recognition, voice recognition, keystrokes dynamics and other biometric or behavioural signals, in any context. [303]

1.1.2. Recommendation of Banning Biometric Categorization

Under the current regulation, the risk category to which these systems are assigned remains unclear. Annex III appears to classify together biometric identification and categorization of natural persons, suggesting that these systems may be thought as high-risk. [304]

In 2021 annual report on The Right to Privacy in the Digital Age, it was stated "Uses of AI that inherently conflict with the prohibition of discrimination should not be allowed. For example… AI systems that categorize individuals into clusters on prohibited discriminatory grounds should be banned in line with these principles."[305]

There is no legitimate justification for the use of biometric categorisation systems to monitor or surveil people in publicly accessible, so it must be forbidden. The use of biometric categorization systems in workplaces or educational institutions can result in highly intrusive surveillance where employees, job applicants or students are already in a position of power imbalance. Moreover, Discrimination might also take

[303]EDPB," EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", (2021), Available At: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en. Last Visited 24.03.2022

[304] Belkadi, L., (2020), op.cit.

[305] Human Rights Council, (2021), *The right to privacy in the digital age* Report of the United Nations High Commissioner for Human Rights Advance Edited Version*, Available At: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx. Last Visited 23.08.2022 P.12

place in private areas if AI-based systems incorrectly categorize disabled people due to their unusual physical characteristics, movements, voices, or facial expressions. [306]

However, the EDPB and EDPS recommend the prohibition of artificial intelligence systems for both public authorities and private organizations that categorize individuals from biometrics (e.g. facial recognition) into clusters based on ethnicity, gender, and political or sexual orientation.[307]

1.1.3. Recommendations Of Banning emotion recognition systems

As ARTICLE 19 has stated that, "the use of emotion recognition involves the mass collection of sensitive personal data in invisible and unaccountable ways, enabling the tracking, monitoring, and profiling of individuals, often in real time."[308]

In the report of the AIDA committee of the European Parliament, the following statements were made regarding the prohibition of emotion recognition systems. Artificial intelligence (AI)-powered emotion recognition systems may have manipulative, risky, and highly undesirable discriminatory and dignified effects. Therefore, general prohibition might be an option to consider. Consequently, a general ban might be something to think about.[309]

The EDPB and EDPS state that using Artificial intelligence to infer a natural person's emotions is highly undesirable and ought to be prohibited. However, it has been stated that artificial intelligence systems can be allowed in the use of emotion

[306] Access Now, European Digital Rights (EDRi), *Bits of Freedom, ARTICLE19 , IT-Pol, (2021), Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorization,*Available At https://www.accessnow.org/AIAct-biometric-categorisation. Last Visited 23.08.2022 P.1-2

[307] EDPB, EDPB-EDPS 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), P.12

[308] Marda, V., & Ahmed, S. , "Emotional Entanglement: China's emotion recognition market and its implications for human rights." (2022), Available At: https://www.article19.org/emotion-recognition-technology-report. Last Visited 23.08.2022

[309] Codagnone, C., LIVA, G., & BALLELL, T. R. D. L. H. (2022). *Identification and assessment of existing and draft EU legislation in the digital field. Study for the special committee on Artificial Intelligence in a Digital Age (AIDA*), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg. P.62

recognition systems for health or research purposes. But this exception must always comply with all other data protection terms and limits, including purpose limitation.[310]

One of the biggest threats to the European Union's goal of developing an ecosystem of trust and excellence for Artificial intelligence is the development of Artificial intelligence systems intended to reveal and manipulate our most private thoughts and feelings. [311] So the use of emotion recognition systems must be banned.

1.1.4. Adding "Vulnerable Individuals" to Risk Groups in the Proposal

Another important point is that sensitive groups are not included in the proposal. There are certain groups in need of special protection who are weak and vulnerable for various reasons, or who have traditionally been victims of abuses. Generally, human rights documents regulate rights to these groups.[312]

However, these groups were not included in the proposal. In 2021 annual report on The Right to Privacy in the Digital Age, it was stated " AI-assisted content curation done by companies with enormous market power raises concerns about the impact on the capacity of the individual to form and develop opinions, as two successive holders of the mandate of Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression have pointed out".[313] Especially the bias of majority or dominant groups reflected in data from search results has been shown to affect the information shared by or about minority or vulnerable groups. For instance, studies have revealed a concerning level of racial and gender bias in Google's search results.[314] Therefore the legislator should avoid risks to individual rights in his proposal. Furthermore, the legislator should include in the proposal of the

[310] Ibid. ,P.12

[311] Access Now, op.cit. P.1-2

[312] Icelandic Human Rights Centre, " The Human Rights Protection Of Vulnerable Groups", (N.D), Available At: https://www.humanrights.is/en/human-rights-education-project/human-rights-concepts-ideas-and-fora/the-human-rights-protection-of-vulnerable-groups. Last Visited 09.08.2022

[313] Human Rights Council, (2021), *The right to privacy in the digital age* Report of the United Nations High Commissioner for Human Rights Advance Edited Version*,Avaialble At: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx. Last Visited 23.08.2022,P.8

[314] Human Rights Council, op.cit. P.8

regulation societal risks to immigrants or vulnerable individuals, including ethnic minorities.[315]

1.1.5. Inclusion of Biometric Categorization Systems in the High-Risk Group

After the proposal was published, the risk-based approach regulation in the doctrine received some positive and negative criticisms. The proposal made a distinction between real-time and post biometric identification systems, as described above, as well as between biometric categorization and biometric identification systems.

However, in this distinction, some risk groups met the expectations, while others were not. One of them is Biometric categorization systems the definition of biometric categorization systems is not clear enough in the proposal. .[316] Although the views on the prohibition of biometric categorization systems in the doctrine were given above, authors such as Gianclaudio Malgieri and Marcello Ienca emphasize that biometric categorization systems should be included in the high-risk status. Gianclaudio Malgieri and Marcello Ienca emphasize that biometric categorization meets all the conditions to be defined as high-risk systems that pose a 'risk of adverse impacts on fundamental rights' and therefore must be clearly included in the high-risk group.[317]

1.1.6. Expanding the scope of Article 7 of the proposal regulating "Amendments to Annex III"

Draft's risk-based approach needs strong changes to ensure flexibility with the quick speed of Artificial intelligence development. The draft Report has neglected to

[315]Alexandru Circiumaru,"Three proposals to strengthen the EU Artificial Intelligence Act", (2021), Available At: www.adalovelaceinstitute.org /blog/three-proposals-strengthen-eu-artificial-intelligence-act/. Last Visited 28.03.2022

[316] Gloria González Fuster and Michalina Nadolna Peeters "Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence",(2021), Available At: https://free-group.eu/2021/12/17/person-identification-human-rights-and-ethical-principles-rethinking-biometrics-in-the-era-of-artificial-intelligence. Last visited 26.03.2022

[317] Madiega, T. & Mildebrath, H. Op.cit.

add any new biometric systems to Annex III, despite the fact that systems that utilise our biometric data inherently pose a high risk to fundamental rights.

Additionally, there haven't been any amendments in Annex III to increase the number of Artificial intelligence systems that pose a high risk in migration management, such as biometric identification systems, predictive analytics, and systems used for monitoring and surveillance at borders, that pose a high risk to migration management.[318]

Moreover, the inability to expand the scope of risk systems is problematic. There is no way to Expansion of the list of High-risk Artificial intelligence systems is limited, according to article 7 of the proposal. High-risk Artificial intelligence systems cannot be expanded by adding new categories, only partially modified by adding subcategories to existing ones. Artificial intelligence is a constantly evolving technology. And these changes bring risks. Expansion of risk lists is limited in the current proposal. [319] Therefore, Expansion of risk lists in the proposal should be more flexible in my opinion.

1.1.7. The Addition of Online Spaces Along with Public Spaces to the Scope of the Ban

In their joint opinion, the EDPB and EDPS argue that the scope of the ban should be broadened by including online spaces in the definition of public spaces. For example, a facial recognition system has been created by Clearview AI to identify individuals online and get their photos on social media platforms. However, data, including biometric data, was stolen by hackers.[320] For this reason, it seems that the

[318] Coalition of civil society organisations, (2021), *Coalition of civil society organisations*, Available At:https://algorithmwatch.org/en/wp-content/uploads/2022/05/Civil-society-reacts-to-EP-AI-Act-draft-report.pdf.Last Visited 24.08.2022 , P.1-2

[319] Circiumaru, A. op.cit.

[320]Alfred Ng,"Clearview AI's entire client list stolen in data breach",(2020Available At: https://www.cnet.com/news/privacy/clearview-ai-had-entire-client-list-stolen-in-data-breach/).Last 23.03.2022

proposal does not sufficiently take into account the specific risks arising from the use of artificial intelligence systems in the online spaces. [321]

1.2. Recommendations for Definitions

There are some recommendations in the definitions of the Commission's Artificial Intelligence regulation proposal in the study, which was commissioned by the European Parliament Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURY and PETIT Committees. These definition recommendations in the proposal will contribute to the protection of biometric data.

First the report describes how the definition of real-time biometric identification systems can be. The Commission stated its proposal as follows: "'‘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."

After a crime has been committed, the police will analyze the video footage with the help of biometric identification techniques. As a result, it will try to identify the culprit by checking if the live template of the criminal matches any template in an existing database. Even where the delay between this incident and the biometric identification of the offender is minimal, it qualifies as "real time" remote identification. However, this characterization is wrong. Instead of "real-time biometric identification", "post biometric identification" should be used. [322]

Secondly, it is the addition of the concept of "biometric inferences" to the proposal. The dictionary meaning of inference is " a guess that you make or an opinion that you form based on the information that you have."[323] "Biometric inferences" are system in which all kinds of personal data, whether based on biometrics or not, are used to make inferences regarding permanent or long-term physical, physiological or

[321] Belkadi, L., op.cit.
[322] Wendehorst, C., & Duller, Y. op.cit. P.70
[323] See. https://dictionary.cambridge.org/dictionary/english/inference. Last Visited 24.08.2022

behavioral characteristics of a natural person. Biometric categorisation and biometric inferences are similar. Biometric categorization can result in biometric inferences. The conclusion that a real person suffers from depression or is very susceptible to depression is a result related to a real person's long-term physical, physiological or behavioral characteristics and therefore qualifies as an inference, not a biometric classification. In the light of what was written above, the definition of "biometric inferences " in the report is as follows. "Biometric inferences" mean conclusions with regard to permanent or long-term physical, physiological or behavioral characteristics of a natural person, on the basis of biometrics-based data or other personal data."[324]

B. RECOMMENDATIONS FOR REGULATIONS ON BIOMETRIC DATA

There is nothing in GDPR regarding biometric data processed by artificial intelligence and the use of biometric data by artificial intelligence. A number of solutions have been introduced in the doctrine regarding biometric data, which should be included in the GDPR. Controllers and data subjects should be provided with guidance on how artificial intelligence can be applied to personal data consistently with GDPR. [325]

GDPR focuses on individual rights and does not take into account the broader social implications of batch processing. On the other hand, the AIA addressed these issues. Some authors have argued that there is a need for legally binding rules on broader social transactions. Strong measures need to be adopted against companies and public authorities that intentionally abuse the trust of data subjects by misusing their personal data, to engage in applications that manipulate data subjects against their interests. [326]

Another important issue is the issue of education. It is a known fact that people are often the weakest link in security, data processing, information and content

[324] Wendehorst, C., & Duller, Y. op.cit. P.70
[325] Giovanni Sartor; Francesca Lagioia, (2020), op.cit. P.79-81
[326] Giovanni Sartor; Francesca Lagioia, op.cit., P.79-81

management, and the like.[327] In the process of processing personal data, it is of great importance to raise awareness of both the data controllers and the data processors, and to increase investments in education on this subject.

In addition, another issue is that employers should provide awareness training to their employees on the protection of personal data. It should be goal for an employee joining the team to have basic knowledge of personal data before accessing systems containing personal data. The level of awareness of employees regarding personal data should be kept at the highest level. In addition, importance should be given to the sustainability of the personal data protection culture in companies. For this reason, it is necessary not to be content with the initial training given to the employees in orientation. It is important to provide periodic training to employees at least once a year.[328]

Regulations regarding the processing of personal data (including biometric data) must be regulated in detail by separate regulations from sector to sector. For example, health regulations, banking, communications sector regulations and their updated and detailed regulation will help to protect personal data more comprehensively. In this regard, a regulation can be made for the processing of personal data, especially in banking sector and financial technology systems where biometric data is used.[329]

In addition, the establishment of specialized courts in parallel with the need for regulation in the sectoral scope above would also be beneficial for the protection of personal data. The issue of protection of personal data includes technical as well as legal

[327] Kunst Bilder,"GDPR awareness: a matter of people, culture, leadership and acting now", (n.d), Available At: https://www.i-scoop.eu/gdpr/gdpr-awareness/ . Last Visited 24.08.2022

[328] Ozbek Attorney Partnership, "Turkey: How To Increase Awareness About Personal Data Protection With Employees And Data Processors?",(2022) Available At https://www.mondaq.com/turkey/data-protection/1162058/how-to-increase-awareness-about-personal-data-protection-with-employees-and-data-processors: . Last Visited 24.08.2022

[329] Erdinç, G..H, "Bilgi Güvenliği, Kişisel Verilerin Korunmasi Ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler" Istanbul Technical University Informatics Institute, P.111

issues. For this reason, it will be important to establish specialized courts in order for the proceedings in this regard to progress more fairly and quickly.[330]

[330] Ibid., P.111

CONCLUSION

Thanks to the developing technology, we live in a world with search engines, online shopping portals, the Internet of objects, 3D printers, driverless vehicles, smart houses and offices, augmented reality applications, chat boots, personal digital assistants and robot surgeons. One of the developing areas is artificial intelligence technology. However, evolving artificial intelligence systems increasingly require the collection of biometric data.

Biometry is a promising and exciting space in which different disciplines meet and provide an opportunity for a safer and more responsible world.[331] In the first part of the thesis, why biometric data is advantageous is explained as follows:

- Biometric data is unique and cannot be copied.
- Biometric data, fraudsters' efforts to create multiple fake digital identities are blocked.
- Biometric data cannot be changed.
- Thanks to the digital identity protection of biometric data, banks aim to increase their online product offerings by opening up their digital infrastructure to third-party fintech providers.
- Biometric data; provides convenience and security. Users forget passwords and pins.
- The innate biometry does not change. A haircut and cosmetic surgery can change the contours of the face, On the other hand the innate biological data of the human beings does not change.
- The stolen biometric data may be more difficult to use than normal encryption methods.
- People can easily forget their passwords, but there is no need for this as Biometric data is precise.
- Biometric data is easy to use, requires little storage space and takes about five seconds to store.

[331] Asha, S., & Chellappan, C. op.cit. P.51

However, there are serious disadvantages as well as advantages of biometric data. These disadvantages are summarized in the first part of the thesis as follows:

- The biggest concern with biometric data is its immutability.
- Biometric data collected falls into the hands of criminal organizations and terrorist organizations is another concern.
- Another major concern is biometric data being hacked.
- Another important concern is that biometric systems violate people's privacy.
- Another concern is the use of automated decisions based on artificial intelligence algorithms in Biometric data.

The development of biometric methods is causing major problems. The development of technology will require the development of new legal regulations and ideas. There is no European legislation regarding biometric data exclusively yet. Currently, biometric data is limited in the GDPR, which is the basic regulation on personal data. In addition, there are provisions on biometric data in law enforcement and passport and border security regulations. (LED), Council Regulation No 2252/2004, (SIS), (VIS), (EES). On the other hand, a draft proposal for artificial intelligence was published by the European Commission for the first time on 21 April 2021. This draft proposal is the first example of legislation on artificial intelligence. However, there are deficiencies in this proposal regarding the protection of fundamental rights and freedoms, especially arising from the risk-based approach. In the thesis, the report prepared by the institution and the association and the recommendation from the doctrine are included. In this context, as summarized in the 5th part of the thesis, the following suggestions regarding the protection of biometric data in the light of artificial intelligence technology are given.

- The scope of the ban on the use of biometric artificial intelligence systems in public spaces must be expanded.
- Online Spaces Along with Public Spaces to The Scope of The Ban must be added.

- Artificial intelligence systems for both public authorities and private organizations that categorize individuals from biometrics into clusters based on ethnicity, gender, and political or sexual orientation must be prohibited.
- Artificial intelligence systems that categorize individuals from biometrics (e.g. facial recognition) into clusters based on ethnicity, gender, and political or sexual orientation must be prohibited.
- Legislator should include in the proposal of the regulation societal risks to immigrants or vulnerable individuals, including ethnic minorities.
- Biometric categorization systems should be included in the high-risk group.
- Expansion of risk lists in the proposal should be more flexible.
- Controllers and data subjects ought to be provided with guidance on how artificial intelligence can be applied to personal data consistently with GDPR.
- In the process of processing personal data, the parties should be made aware and education investments should be increased.
- Sectoral-based biometric data regulations should be made by lawmakers.
- Establishment of specialized courts will be beneficial in terms of protecting biometric data.

In summary, in the light of artificial intelligence, biometric data protection will be one of the most discussed areas of the future. The artificial intelligence proposal for the biometric data protection in the EU should be further strengthened and put into effect. In addition, AIA GDPR and other EU regulations should be handled in harmony, and a strong biometric data protection mechanism should be developed by implementing the above-mentioned recommendations. This will be beneficial in enhancing the protection of fundamentals and freedoms in the EU legal order.

BIBLIOGRAPHY

BOOKS:

Aşıkoğlu, Ş. İ. (2018). "*Avrupa Birliği Ve Türk Hukukunda Kişisel Verilerin Korunması Ve Büyük Veri*":. İstanbul: Oniki Levha Yayıncılık

Carey, P. (2018). *Data protection: a practical guide to UK and EU law*. Oxford University Press, Inc

Çetin S., (2021) *Gelişen Teknolojiler ve Hukuk II – Yapay Zeka: Yapay Zeka Stratejileri ve Hukuk*, Onikilevha Yayıncılık

Dunstone, T., & Yager, N. (2008). *Biometric system and data analysis: Design, evaluation, and data mining*. Springer Science & Business Media

Feyzioğlu, G, (2021*) Gelişen Teknolojiler ve Hukuk II – Dijitalleşen Dünyada Yapay Zeka*:, Onikilevha Yayıncılık

Giakoumopoulos, C.- Buttarelli F.- O'Flaherty.M. (2018). *Handbook on European data protection law:* 2018 Edition. European Union Agency for Fundamental Rights and Council of Europe,

Gish, H. (2005). Elements of Speaker Verification. In: Wayman, J., Jain, A., Maltoni, D., Maio, D. (eds) Biometric Systems. Springer, London

Hallevy, G. (2013). *When robots kill artificial intelligence under criminal law*. UPNE

Kindt, E. J. (2016). *Privacy and data protection issues of biometric applications* (Vol. 1). Springer

Kop, M. (2021, September). *EU Artificial Intelligence Act*: The European Approach to AI. Stanford-Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, Issue.

Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation:* A Commentary. Oxford University Press.

Küzeci, E. (2010). *Kişisel verilerin korunması,.* Ankara: Turhan Kitabevi

Paslı, A., Kaya, A., Engin, B. İ., Aşıkoğlu, Ş. İ., & Oğuz, E. (2020). *Türk Hukukunun Avrupa Birliği Hukukuna Uyumu Özel Hukuk*. İstanbul University Press

Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G& Teller, A. (2016). Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence. Stanford University

Zibran, M. F. (2009). Eye based authentication: Iris and retina recognition. Technical Report#2011-04, University of Saskatchewan.

Voigt, P., B., (2017) *The EU GDPR:* A Practi cal Guide, Springer, Heidelberg

ARTİCLES:

Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). "Past, present, and future of face recognition". A review. Electronics, 9(8), 1188., 1-52

Aliyev, A. I., Rzayeva, G. A., & Ibrahimova, A. N. (2021). "Artificial Intelligence and Personal Data: International and National Framework." Peace Human Rights Governance, 5(1). 97-123

Asha, S., & Chellappan, C. (2012). "Biometrics: an overview of the technology, issues and applications." International Journal of Computer Applications, *39*(10), 35-52

BAK, B (2018). "Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk". Türkiye Adalet Akademisi Dergisi, (35), 211-232.

Barua, K., Bhattacharya, S., & Mali, K. (2011). “Fingerprint identification.” Global Journal of Computer Science and Technology. Volume 11 Issue 6, (61-63)

Bartlow N. (2009) “Keystroke Recognition.” In: Li S.Z., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA.

Binns, R. (2019). “Human Judgment in algorithmic loops: Individual justice and automated decision-making”. Regulation & Governance. P.1 Available At: https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12358. Last Visited 01.04.2022

Bourcha, C., Deftou, M. L., & Koskina, A. (2017). “Data mining of biometric data: revisting the concept of private life?”. Ius et Scientia, 3 (2), (37-62).

Bozüyük, T., Yağci, C., Gökçe, İ., & Akar G. (2005). Yapay Zeka Teknolojilerinin Endüstrideki Uygulamalari., Available At: www.teknoloji.isparta.edu.tr/assets/uploads/sites/134/files/is-yeri-egitimi-6-hafta-odev-notu-08052020.pdf. Last Visited 25.10.2021

Busch, C., Nouak, A., Zhou, X., Suchier, J. M., Kelkboom, E., & Kevenaar, T. (2008). “3D Face Recognition for Unattended Border Control”. Security and Management, 8, 350-356

Calo, R. (2017). “Artificial intelligence policy: a primer and roadmap.” UCDL Rev., 51, 399-475

Carpenter, D., McLeod, A., Hicks, C, (20189. *Privacy and biometrics:* An empirical examination of employee concerns. Inf Syst Front 20, (91–110) Available At:. https://doi.org/10.1007/s10796-016-9667-5.

Christakis, T., Bannelier, K., Castelluccia, C., & Le Métayer, D. (2022). “Mapping the Use of Facial Recognition in Public Spaces in Europe–Part 1: A Quest for Clarity: Unpicking the'Catch-All'Term”. Available at SSRN 4110512

Colmenarez, A. J., & Huang, T. S. (1998). “Face detection and recognition. In *Face Recognition* “ (Springer, Berlin, Heidelberg. pp. (174-185).

Dai, P., & Rudge, D. (2018). “Using the discovery of the structure of DNA to illustrate cultural aspects of science.” The American Biology Teacher, 80(4), 256-262

Deb, S. (2003). “Multimedia Systems and Content-based Retrieval.” In Face Recognition Technology (pp. 62-101)

Down, M. P., & Sands, R. J. (2004). “Biometrics: An overview of the technology, challenges and control considerations.” Information Systems Control Journal, 4, 53-56

Dülger, M. V. (2019). “ Protection of Personal Data in the Context of the European Union General Data Protection Regulation”. Yaşar Hukuk Dergisi, 1(2), (71-174).

Dülger, M. V., Çetin, S , Aydınlı C, (2021).” Algoritmik Karar Verme ve Veri Koruması (Algorithmic Decision Making and Data Protection).” Available at SSRN: https://ssrn.com/abstract=3792207. Last Visited 03.04.2022

Ebelogu, C. & Amujo, O. & Adelaiye, O. & Silas, F. (2019). “Privacy Concerns in Biometrics”, IEEE-SEM, Volume 10, Issue 7, July-2019 ISSN 2320-9151,(45-52),

Edward S., Jiahong C., (2021) What does it mean for a data subject to make their personal data ‘manifestly public’? An analysis of GDPR Article 9(2)(e), International Data Privacy Law, Volume 11, Issue 2, Pages 107-124, https://doi.org/10.1093/idpl/ipab005

Hacker, P. (2018). “Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law.” Common Market Law Review, 55(4). Available at SSRN: https://ssrn.com/abstract=3164973, 1143-1186.

Haenlein, M., & Kaplan, A. (2019). “A brief history of artificial intelligence: On the past, present, and future of artificial intelligence.” California management review, 61(4), 5-14

Hill, R. (1996). “Retina identification. In Biometrics” (pp. 123-141). Springer, Boston, MA.

Kaushal, N., & Kaushal, P. (2011). “Human identification and fingerprints:” a review. J Biomet Biostat, *2*(123), 2. DOI: 10.4172/2155-6180.1000123. P.1

Kok, J. N., Boers, E. J., Kosters, W. A., Van der Putten, P., & Poel, M. (2009). *Artificial intelligence: definition, trends, techniques, and cases*. EOLSS Publications

Koza, J. R., Bennett, F. H., Andre, D., & Keane, M. A. (1996). “Automated design of both the topology and sizing of analog electrical circuits using genetic programming. In Artificial intelligence in design”, (pp. 151-170), Springer, Dordrecht

Maguire, M. (2009). “The birth of biometric security”. Anthropology today, 25(2), 9-14

Marda, V., & Ahmed, S. (2021). *Emotional Entanglement: China’s emotion recognition market and its implications for human rights*. Available At: https://www.article19.org/emotion-recognition-technology-report/. Last Visited 05.03.2022

Metin, Y. (2002). “Avrupa Birliği Temel Haklar Şartı. “Ankara Üniversitesi SBF Dergisi”. 57(04). (35-53)

Penny K.H.(2021). “Iris Recognition Technology for Improved Authentication.” Sans Security Essentials (Gsec) Practical Assignment, Version. 2021;3. Available At: https://www.sans.org/white-papers/132/. Last Visited 05.02.2022

Phadke, S. (2013). “The Importance of a Biometric Authentication System”. The SIJ Transactions on Computer Science Engineering & its Applications, 1 (4), 128-132

Pi, Y. (2021). “Machine learning in Governments: Benefits, Challenges and Future Directions”. JeDEM-eJournal of eDemocracy and Open Government, 13(1), 203-219.

Ploeg, I. V. D. (2012). “Security in the danger zone: Normative issues of next generation biometrics. In *Second generation biometrics: The ethical, legal and social context* “Springer, Dordrecht.(pp. 287-303).

Pruzansky, S. (1963). “Pattern-Matching Procedure for Automatic Talker Recognition.” The Journal of the Acoustical Society of America, 35(3), 354-358.

Said, A. B., Erradi, A., Aly, H., & Mohamed, A. (2020). “A deep-learning model for evaluating and predicting the impact of lockdown policies on COVID-19 cases”. arXiv preprint arXiv:2009.05481

Selçuk, E. (2014). “Lizbon Sonrasi Avrupa Birliği’nin Yenilenen Temel Haklar Sorunsali.” Marmara Üniversitesi Avrupa Topluluğu Enstitüsü Avrupa Araştırmaları Dergisi, 22(1), 121-147

Suvarnsing B., & Sangramsing K., N. & Raju M., & Jaypalsing K., & Charansing K.. (2015). “DNA Biometric”., IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 5, Issue 5, Ver. I (Sep - Oct. 2015), PP 82-84, P.83

Şahin, G. Ö., & Şahin, Ç., (2022) “Yapay Zekali Varliklara Elektronik Kişilik Modeli Taninmasina İlişkin Eurobotics Raporu Ve Fikri Mülkiyet Sorunu Bağlaminda Meseleye Yaklaşim”. İnönü Üniversitesi Hukuk Fakültesi Dergisi, 13(1), 110-128.

Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). “Deepface: Closing the gap to human-level performance in face verification.” In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1701-1708).

Temir, E. (2020). Deepfake: new era in the age of disinformation & end of reliable journalism. Selçuk İletişim, 13(2), (1009-1024).

The University of Minnesota Human Rights Center, (2020),” Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?”, P.2, Available At: https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Summary.pdf. Last Visited20.02.2022

Trokielewicz, M., Czajka, A., & Maciejewicz, P. (2018). “Iris recognition in cases of eye pathology.” ArXiv, abs/1809.01040.

Turing, A. M., & Haugeland, J. (1950). “Computing machinery and intelligence”, Cambridge, MA: MIT Press. (pp. 29-56).

Turk, M., & Pentland, A. (1991).” Eigenfaces for recognition.” Journal of cognitive neuroscience, 3(1), (71-86)

Waller, M., & Waller, P. (2020). “Why Predictive Algorithms are So Risky for Public Sector Bodies.” Available at SSRN: https://ssrn.com/abstract=3716166 or http://dx.doi.org/10.2139/ssrn.3716166. Last Vİsited 27.03.2022

Wang, P. S., & Yanushkevich, S. N. (2007). “Biometric technologies and applications. In *Artificial Intelligence and Applications”* (pp. 249-254).

Wong, R. (2012). “The data protection directive 95/46/EC: idealisms and realisms. International Review of Law”, Computers & Technology, 26(2-3), (229-244).

Wouters, N., Kelly, R., Velloso, E., Wolf, K., Ferdous, H. S., Newn, J., ... & Vetere, F. (2019, June). “Biometric mirror: Exploring ethical opinions towards facial analysis and automated decision-making.” In Proceedings of the 2019 on Designing Interactive Systems Conference (pp. 447-461)

Yadav, A. K., & Tadisetty, S. (2012).” Iris based de-duplication technology.” *IJERA, 2*(1), (164-167).

Yilmaz, İ., Sözer, C., & Elver, E. “Yapay Zeka İle İlgili Güncel Düzenlemeler: Avrupa Birliği Ve Amerika Birleşik Devletlerinde Alınan Aksiyonlar Işığında Bir Değerlendirme”. *Adalet Dergisi*, (66), (445-469)

THESES

Çabuk, E., (2020), "Avrupa Birliği Düzenlemeleri Işiğinda Türk Hukukunda Kişisel Verilerin Korunmasi", Master Thesis Bahcesehır Unıversity Social Science Institute

Erdinç, G..H, "Bilgi Güvenliği, Kişisel Verilerin Korunmasi Ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler" Master Thesis Istanbul Technical University Informatics Institute

Gürses, B. (2019). "AB Ve Türk Hukukunda kişisel Verilerin korunması-Mevzuat Uyumuna yönelik Bir değerlendirme" "PHD Thesis, Marmara Universiy.

Özkorul, G. (2021). "Uluslararası göç ve güvenlik perspektifinde biyometrik verilerin önemi" Master's thesis, Sosyal Bilimler Enstitüsü.

Tuncay, M., (2019), Biyometrik Verileri Korunnması.", Master Thesis L.L.M Bahçesehir University Social Sciences Institute

REPORTS /GUIDELINES/ OPINIONS / RECOMMENDATIONS:

Article 29 data protection working party guidelines on automated individual decision-making and profiling for the purposes of regulation, 2016/679

Article 29 Data Protection Working Party, (2012) Opinion 3/2012 On Developments In Biometric Technologies

Article 29 Working Party (2014), "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

Busch, C., Nouak, A., Zhou, X., van der Veen, M., Deravi, F., & Suchier, J. M. (2007, September). Towards unattended and privacy protected border control. In 2007 Biometrics symposium

Castelluccia, C., & Le Métayer, D. (2019). Understanding algorithmic decision-making: Opportunities and challenges. European Parliament. P.II Available At: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)624261. Last Visited 01.04.2022

Codagnone, C., LIVA, G., & BALLELL, T. R. D. L. H. (2022). Identification and assessment of existing and draft EU legislation in the digital field. Study for the special committee on Artificial Intelligence in a Digital Age (AIDA), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg. P.62

Dantcheva, A.; Chen, C.; Ross, A. Can facial cosmetics a ect the matching accuracy of face recognition systems? In Proceedings of the 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 23–27 September 2012

Dumortier, F. (2018). "PROTECT (Pervasive and UseR Focused BiomeTrics Border Project): D2. 2 Legal framework of biometric border control.", Available At: https://researchportal.unamur.be/en/publications/protect-pervasive-and-user-focused-biometrics-border-project-d22- Last Visited 25.04.2022

EDPB, EDPB-EDPS 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),

European Commission, "Why do we need the Charter?" Available At: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en. Last Visited 22.08.2022

European Commission,"The EU's accession to the European Convention on Human Rights: Joint statement on behalf of the Council of Europe and the European Commission", (2020), Avaiable At: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_1748. Last Visited 22.08.2022

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

European Council,"Protection and promotion of human rights", (2022), Available At https://www.consilium.europa.eu/en/policies/human-rights/: . Last Visited 23.08.2022

European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, Adopted on 21 April 2020, Available At: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf. Last Visited 19.03.2022

Fuster, G. G., & Peeters, M. A. N. (2021). *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics In The Era of Artificial Intelligence.*, Available At: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)697191. Last Visited : 02.03.2022

Giovanni Sartor; Francesca Lagioia, (2020), *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*,European Parliament, Available At:https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530. Last Visited : 28.03.2022

Human Rights Council, (2021), The right to privacy in the digital age* Report of the United Nations High Commissioner for Human Rights Advance Edited Version

Madiega, T. & Mildebrath, H.(2021). *Regulating facial recognition in the EU. European Parliamentary Research Service*, Available At: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. Last Visited : 02.03.2022

Wendehorst, C., & Duller, Y. (2021). Biometric Recognition and Behavioural Detection. Study Requested by the JURI and PETI Committees of the European Parliament

WIPO, W. (2019). Technology trends 2019: Artificial intelligence. Geneva: World Intellectual Property Organization

LEGISLATIONS:

Annexes To The Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts.

Charter of the United Nations

Council Regulation (EC) No 2252/2004

Common Position (EC) No 1/95 Adopted By The Council On 20 February 1995 With A View To Adopting Directive 95/. . ./EC Of The European Parliament And Of The Council Of. On The Protection of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (95/C 93/01, The Council Of The European Communities. Official Journal L, No C 93/1

Directive 95/46/EC

European Convention on Human Rights General Data Protection Regulation

Law enforcement Directive

Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts

Regulation 1987/2006

Treaty on European Union

United Nations Security Council Resolution (2014). 2160.

CASES:

C-61/22 - Landeshauptstadt Wiesbaden, Summary

C-291/12 Schwarz v Stadt Bochum , (2013)

C-524/06, Heinz Huber v. Bundesrepublik Deutschland [GC],

Joined cases C-446/12 to C-449/12 Willems et al. v Burgemeester van Den Haag, (2015

Case Of Peck V. The United Kingdom, (2003), (Application No. 44647/98)

Gaughran V. The United Kingdom, (2020), (Application No. 45245/15)

Malone v Metropolitan Police Commissioner [1984] (Application no. 8691/79)

Leander V. Sweden, (1987), (Application No. 9248/81)

M.K. V. France (2013), (Application no. 19522/09)

Peck v. the United Kingdom, (2003), (Application no. 44647/98).

Rotaru V. Romania, (2000),(Application no. 28341/95)

S. and Marper v. the United Kingdom (2008),

NEWS:

BBC, (21.08.2019), "Biostar 2: Suprema plays down fingerprint leak reports", Available At: https://www.bbc.com/news/technology-49418931 Last Visited : 02.04.2022

Bloomberg Intelligence,(2017), "Business-focus on artificial intelligence rising", Available At: https://www.bloomberg.com/professional/blog/business-focus-artificial-intelligence-rising-2/. Last Visited : 11.10.2021

FT, (2021), *Emotion recognition: can AI detect human feelings from a face?,* Available At: https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452. Last Visited :06.03.2022

www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know-about/?sh=1aec3a572404

WEBSITES / INTERNET BLOG

Access Now, European Digital Rights (EDRi), Bits of Freedom, ARTICLE19 , IT-Pol, (2021), Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorization,Available At https://www.accessnow.org/AIAct-biometric-categorisation. Last Visited 23.08.2022 P.1-2

AI Now, (n.d), *Automated Decision Systems Examples Of Government Use Cases Issue:*Last Visited .25.03.2022 Available At: https://ainowinstitute.org/nycadschart.pdf

Albayrak, B. (n.d.). "Parmak izi sistemi nedir? Nasıl çalışır? Nerelerde kullanılır?", Available At: https://www.moonwell.com.tr/parmak-izi-sistemi-nedir-nasil-calisir-nerelerde-kullanilir/. Last Visited : January 15, 2022,

Arslan, Z., (2019), “Yapay Zeka Ve Over The Top Hizmetler Araciliğiyla Profilleme”, Available At: https://www.rskveri.com/yapay-zeka-ve-over-the-top-hizmetler-araciligiyla-profilleme/. Last Visited :05.04.2022,

Balaji, P. (2010). “An Overview-DNA as a Biometric Data Identifier.” Available at SSRN: https://ssrn.com/abstract=1572236 or *http://dx.doi.org/10.2139/ssrn.1572236.* Last Visited : 15.02.2022

Bateman, R., (2022), GDPR Lawful Basis: Legal Obligation, Available At: https://www.termsfeed.com/blog/gdpr-lawful-basis-legal-obligation/. Last Visited : 27.02.2022

Belkadi, L., (2020),” The Proposed Artificial Intelligence Act and Biometric Systems: A Peek Into the Conceptual Maze (Part I))”, Available At: www.law.kuleuven.be /citip/blog/the-proposed-artificial-intelligence-act-and-biometric-systems-part-i/. Last Visited : 24.03.2022

Benjamin Kuipers, " Progress in AI" (2019, Avaialble At: https://web.eecs.umich.edu/~kuipers/opinions/AI-progress.html. Last Visited 30.08.2022

BioConnect. (2021, December 8). “A Brief History of Biometrics.”, Available At: https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/. Last Visited 03.01.2022

Blanca, E.,(2021), “ey-woman-wearing-augmented-reality-glasses-touching-screen Biometric systems in the forthcoming EU Artificial Intelligence Act”, Available At: https://www.ey.com/en_es/law/biometric-systems-in-the-forthcoming-eu-artificial-intelligence.Last Visited : 11.03.2022

Bosso, J., (2021),"The dangers of government use of biometric data", Available At: https://blog.avast.com/government-use-of-biometric-data-avast. Last Visited : 25.03.2022

CAHAI - Ad hoc Committee on Artificial Intelligence ,(2020),*Towards regulation of AI systems (2020*Available At.https://edoc.coe.int/en/artificial-intelligence/9656-towards-regulation-of-ai-systems.html*)*. Last Visited :06.12.2021

Circiumaru, A. (2021), "Three proposals to strengthen the EU Artificial Intelligence Act", Available At: www.adalovelaceinstitute.org /blog/three-proposals-strengthen-eu-artificial-intelligence-act/. Last Visited : 28.03.2022

Clifford, C. (2018, February 1). "Google CEO: A.I. is more important than fire or electricity.", Available At: https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html. Last Visited : 18.11.2021

Coalition of civil society organisations, (2021), Coalition of civil society organisations, Available At:https://algorithmwatch.org/en/wp-content/uploads/2022/05/Civil-society-reacts-to-EP-AI-Act-draft-report.pdf.Last Visited 24.08.2022

Darama, S, "Yapay Zekanin Hukuki Statüsü Hakkindaki Görüşler Üzerine Değerlendirme", (2021), Avaiable At: https://www.ozgunlaw.com/makaleler/yapay-zekanin-hukuki-statusu-hakkindaki-gorusler-uzerine-degerlendirme-744. Last Visited 19.02.2023

Data Protection Commission, (n.d), "Law Enforcement Directive, Available At:https://www.dataprotection.ie/en/organisations/resources-organisations/law-enforcement-directive. Last Visited : 08.04.2022

Del Gamba, G. (2020, May 13). "Machine learning, risks and benefits of automated decisions". Available At. https://www.insuranceup.it/en/opinions/machine-learning-risks-and-benefits-of-automated-decisions/.Last Visited 25.01.2022

Dezhic,E, "Artificial vs Natural Intelligence", (2017), Available At: https://becominghuman.ai/artificial-vs-natural-intelligence-82ccd056b212 , Last Visited 22.08.2022

ECHR, (n.d.) *European court of human rights & question and answers,* Available At: https://www.echr.coe.int/documents/questions_answers_eng.pdf. Last Visited :12.03.2022

EDPB, (2021)," EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", Available At: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en. Last Visited : 24.03.2022

Edri, (2018), "Smart Borders: the challenges remain a year after its adoption", Available At: https://edri.org/our-work/smart-borders-the-challenges-remain-a-year-after-its-adoption/. Last Visited : 20.04.2022

EDRİ, (2022) " ID-Fingerprint obligation to be reviewed by European Court of Justice", Available At: https://edri.org/our-work/id-fingerprint-obligation-to-be-reviewed-by-european-court-of-justice/. Last Visited : 04.05.2022

ETIAS, (2022), The Schengen Information System: Keeping Europe Safe, Available At: https://www.etiasvisa.com/etias-news/schengen-information-system-sis. Last Visited : 15.04.2022

Eurepean Comission, (2022), EUROCAD "(European Asylum Dactloscopy Database)", Available At: https://knowledge4policy.ec.europa.eu/dataset/ds00008_en. Last Visited :20.04.2022

European Comission, "Entry/Exit System (EES)", Available At: https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en. Last Visited : 20.04.2022

European Comission, (2019), "Ethics guidelines for trustworthy AI", Available At: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Last Visited : 02.12.2021

European Comission, (n.d), "The European AI Alliance”, Available At: https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance. Last Visited : 03.12.2021

European Commission,,” Visa Information System (VIS)”, Available At: https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/visa-information-system_en. Last Visited . 18.04.2022

European Court of Human Rights, (2021), “Guide on Article 8 of the European Convention on Human Rights”, Available At: https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Last Visited : 22.02.2022

European Parliament, (2019), *Motion For A European Parliament Resolution*, Available At: https://www.europarl.europa.eu/doceo/document/A-8-2019-0019_EN.html. Last Visited : 25.11.2021

European parliament, (2021) “Completion Of Eu Accession To The European Convention On Human Rights”, Available At: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-completion-of-eu-. Last Visited : 27.02.2022

European Parliament. (2020, September 4). “What is artificial intelligence and how is it used?" ,Available At:www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used. AccessDate,10.10:2021

European Parliament, “European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence”,(2020), Available At: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html. Last Visited 21.02.2023

Gibson, A., Tessa, M., ,(2020), “Artificial Intelligence In The Public Sector – Inference And Collection”, Available At:https://ovic.vic.gov.au/blog/artificial-intelligence-in-the-public-sector-inference-and-collection/. Last Visited :19.03.2022

Global ID Summit, (2018), “Identity in a Digital Age:A Glance At The Countries Leading the Revolution,”, Available At: https://www.idga.org/events-globalidsummit/downloads/sponsorship-information-mt. Last Visited : 23.03.2022

Gonzalaz, G., (2021), “Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence”, Available At: https://free-group.eu/2021/12/17/person-identification-human-rights-and-ethical-principles-rethinking-biometrics-in-the-era-of-artificial-intelligence/. Last Visited : 26.03.2022

Harris, T. (2020, August 3). How Fingerprint Scanners Work., Available At: https://computer.howstuffworks.com/fingerprint-scanner.htm Last Visited : 15.01.2022

Herrera ,P., (2013), “Estrella Gutiérrez: ECJ Judgment Schwarz (C-291/12) Biometric data and respect for private life Access” Date:18.03.2022 Available At: https://ecjleadingcases.wordpress.com/category/datos-biometricos-biometric-data/

Hewage, Chaminda. (2019). “Stolen Fingerprints Could Spell The End Of Biometric Security”, Available At: https://theconversation.com/stolen-fingerprints-could-spell-the-end-of-biometric-security-heres-how-to-save-it-122001. Last Visited :02.04.2022

Hidvegi, F., Leufer, D., Masse., Estelle, (2021), “The EU should regulate AI on the basis of rights, not risks”, Available At: https://www.accessnow.org/eu-regulation-ai-risk-based-approach/. Last Visited : 08.03.2022

HRB, (n.d), "Special category personal data", Available At: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-overview/special-category-personal-data/. Last Visited :15.03.2022

ICO, (n.d), " What are the conditions for processing?", Available At. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/. Last Visited .10.03.2022

ICO,"What is automated individual decision-making and profiling?", (n.d), Available At https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/: . Last Visited 23.08.2022

Ivan Klekovic,"EU GDPR vs. European data protection directive", (2017), Available At https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/: . Last Visited 30.08.2022

Jakubowska, E. (2021, November 4). “Facebook deleting facial recognition: Five reasons to take it with a pinch of salt.”, Available At: https://reclaimyourface.eu/facebook-deleting-facial-recognition-five-reasons-to-take-it-with-a-pinch-of-salt/. Last Visited : 07.01.2022

Jrc Science Hub Community, (2018*), EU Declaration on Cooperation on Artificial Intelligence, Available* At: https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence

Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, ProPublica, " Macnine Bias", (2016), Available At: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Last Visited 30.08.2022

Justice.org.uk, *Protection of Freedoms Bill*, Available At: https://justice.org.uk/protection-of-freedoms-bill/. Last Visited : 13.03.2022

Karla Lant,"Confirmed: Ai Can Predict Heart Attacks And Strokes More Accurately Than Doctors", (2017), Available At:

https://futurism.com/neoscope/confirmed-ai-can-predict-heart-attacks-and-strokes-more-accurately-than-doctors . Last Visited 30.08.2022

Kaya F , "Yapay Zeka Ve Yapay Zekanin Hukuki Kişiliği Meselesi", (2021), Available At: http://blog.ilem.org.tr/yapay-zeka-ve-yapay-zekanin-hukuki-kisiligi-meselesi. Last Visited 21.02.2023

King, R. (2018, March 12). Explainer: "Keystroke recognition.", Available At: https://www.biometricupdate.com/201612/explainer-keystroke-recognition. Last Visited : 16.02.2022

Krasnokutsky, E., (2021), " AI Biometric Authentication for Enterprise Security". Available At: https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security. Last Visited 30.08.2022

Loi, m. in collaboration with Mätzener A., Müller A., and Spielkamp M., (2021), "Automated Decision-Making Systems in the Public Sector – An Impact Assessment Tool for Public Authorities", Available At: https://algorithmwatch.org/en/wp-content/uploads/2021/06/ADMS-in-the-Public-Sector-Impact-Assessment-Tool-AlgorithmWatch-June-2021.pdf.Last Visited : 26.03.2022

Marda, V., & Ahmed, S. , "Emotional Entanglement: China's emotion recognition market and its implications for human rights." (2022), Available At: https://www.article19.org/emotion-recognition-technology-report. Last Visited 23.08.2022

Mazzini, G., (2021), "A European Strategy for Artificial Intelligence" , ELI webinar 'Regulating AI: A First Analysis of the European Commission's Proposal' 29 April 2021 Available At:https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/News_page/2021/Presentation_Gabriele_Mazzini.pdf. Last Visited :20.04.2022

Medium.com. (2018, March 16). “Yapay Zekanın Tarihçesi ve Gelişim Süreci.”, Available At: medium.com/türkiye/yapay-zekanın-tarihçesi-ve-gelişim-süreci-cb4c73deb01d. Last Visited : 5.11.2021

Mesai N, (2021), “Can the criminal justice system’s artificial intelligence ever be truly fair?”, Available At: https://massivesci.com/articles/machine-learning-compas-racism-policing-fairness/. Last Visited :20.03.2022

Mitek systems, (2019), "Looking ahead: 7 reasons why biometric security is important for digital identity", Available At: https://www.miteksystems.com/blog/looking-ahead-7-reasons-why-biometric-security-is-important-for-digital-identity. Last Visited : 21.03.2022

Ng, A., (2020),"Clearview AI's entire client list stolen in data breach", Available At: https://www.cnet.com/news/privacy/clearview-ai-had-entire-client-list-stolen-in-data-breach/.Last Visited : 23.03.2022

Nordi N., (2018), “What is the Data Protection Directive? The Predecessor to the GDPR”, Available At: https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr. Last Visited : 08.04.2022

OECD, (2021), *Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers,* Available At: https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf, Last Visited : 21.11.2021

Ombudsmanky, Fifth Data Protection Principle - Storage limitation, p.2Available At: https://ombudsman.ky/images/pdf/guide/56-fifth-data-protection-principle-storage-limitation.pdf. Last Visited 23.08.2022,

Ozbek Attorney Partnership, “Turkey: How To Increase Awareness About Personal Data Protection With Employees And Data Processors?”,(2022) Available At https://www.mondaq.com/turkey/data-protection/1162058/how-to-increase-awareness-

about-personal-data-protection-with-employees-and-data-processors: . Last Visited 24.08.2022

Pew Research Center. (2018). “Public attitudes toward computer algorithms,USA, Access Data” 25.03.2022 Available At: http://refhub.elsevier.com/S0308-5961(20)30068-9/sref45

Privacy International, (n.d), " what is privacy" , Available At: https://privacyinternational.org/explainer/56/what-privacy. Last Visited : 03.04.2022

Rechtsanwälte, L., (2020),Regulation of Artificial Intelligence in Europe - What’s in the pipeline?, Available At: https://www.lexology.com/library/detail.aspx?g=d9f74ab9-139c-49e1-9d82-70de718af80f. Last Visited : 04.12.2021

Rockcontentwriter,” Artificial Intelligence Algorithm: Everything You Need To Know About It “(2021), Available at: https://rockcontent.com/blog/artificial-intelligence-algorithm/%20efficiently, Last Visited (22.08.2022)

Ross, D. (2017, December 31). “Processing biometric data? Be careful, under the GDPR.”, Available At: https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-GDPR. Last Visited : 27.12.2021

Seeunity, “The main differences between the DPD and the GDPR and how to address those moving forward”, (2017), Available At: https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf. Last Visited26.07.2022

Signalsvc.com, (2021), "Role of Artificial Intelligence and Machine Learning in Speech Recognition", Available At: https://signalscv.com/2021/07/role-of-artificial-intelligence-and-machine-learning-in-speech-recognition/. Last Visited : 10.10.2021

Simonart, V, "Artificial Intelligence And Legal Personal", Available At: https://liedekerke.com/en/insights/artificial-intelligence-and-legal-personality. Last Visited 21.02.2023

Stachyra, K., (2015), "ECJ: no legal basis for biometric data in ID cards", Available At: https://europensblog.wordpress.com/tag/joined-cases-c-44612-to-c-44912/. Last Visited .19.03.2022

Stanford University, (2021), *CHAPTER 7: AI Policy and National Strategies* , Available At: https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf. Last Visited : 22.11.2021

Symanovich, S., (n.d)., " Biometric data breach: Database exposes fingerprints, facial recognition data of 1 million people", Available At: https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html. Last Visited : 01.04.2022

Tandoğan,Z: (2019), " Yapay Zekanın Geleceği, , Available At: https://kantin.sabanciuniv.edu/sites/kantin.sabanciuniv.edu/files/makale/yapay-zekanin-gelecegi.pdf. Last Visited : 01.11.2021

Tanya Lewis, A Brief History of Artificial Intelligence, (2014), Available At: https://www.livescience.com/49007-history-of-artificial-intelligence.html . Last Visited 30.08.2022

Thakkar , D., (2020), "Importance of Biometric Fingerprinting Technology: Does Your Organization Really Need It? This Will Help You Decide!" Available At: https://www.bayometric.com/importance-of-biometric-fingerprinting-technology/. Last Visited . 20.03.2022

Thales. (2021, June 16). "Biometric data and privacy laws (GDPR, CCPA/CPRA).", Available At: thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data. Last Visited : 07.01.2022

Thomas, M. (2021, January 21). “The Future of AI: How Artificial Intelligence Will Change the World.”, Available At: https://builtin.com/artificial-intelligence/artificial-intelligence-future. Last Visited : 18.11.2021

United Nations,(n.d). “CTED publishes Analytical Brief on the use of biometrics in counter-terrorism “,Available At: https://www.un.org/securitycouncil/ctc/news/cted-publishes-analytical-brief-use-biometrics-counter-terrorism. Last Visited : 18.02.2022

Urban, T. (2015, June 22). “The AI Revolution: The Road to Superintelligence.” , Available At: https://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html Last Visited : 08.11.2021.

Valerie Rivera,”What the Future of Data Protection Means for Your Business”, (januayr 5 2022), Available At: https://www.insight.com/en_US/content-and-resources/2022/the-future-of-data-protection.html. Last Visited 22.08.2022

Veridiumid, “Biometric Identification or Biometric Authentication?” (2018, June 11), Available At: https://www.veridiumid.com/biometric-identification-and-biometric-authentication. Last Visited 08.01.2022

Witte, j. (2022), "Fingerprint obligation to be reviewed by European Court of Justice", Available At: https://digitalcourage.de/blog/2022/fingerprint-obligation-to-be-reviewed-by-ecj. Last Visited : 20.03.2022,

Zapproved, (2019), "Importance of Biometric Data Privacy", Available At: https://zapproved.com/blog/just-how-important-is-it-to-protect-the-privacy-of-biometric-data/. Last Visited :30.08.2022