Artificial Intelligence and Neuroscience: The impact on Data Protection and Privacy

Nicola FABIANO
Studio Legale Fabiano
Rome, 00179, (Italy)
Affiliation: *International Institute of Informatics and Systemics (IIIS)* - USA
email: *info@fabiano.law*

ABSTRACT [1]

Starting from a multidisciplinary approach, we want to investigate the kind of impact of high technologies used in neuroscience on humans to analyse the effects on data privacy and protection domain. It is still a field under a due course of deepening, and probably there are few scientific pieces of evidence, but it certainly is one of the most relevant challenges of our times although some people think this is a topic of the future. Neuroscience, data protection and privacy are current aspects, and we should deal with them now to avoid unrecoverable consequences or distorted findings. What will be the destiny of privacy and data protection in the neuroscience domain? Our approach is not technical, and thus we will not describe or propose specific technical solutions. Still, our goal is to warn about the possible effects on data protection and privacy, essentially on human dignity, hoping scientists would consider the principles laid down by the current laws and Ethics. Indeed, here comes into play also another fundamental aspect which is exactly Ethics. There is some very innovative research on the human brain in the neuroscience field, where scientists decided to use high-technologies and artificial intelligence to investigate and deepen the effects on human behaviour. We are facing a challenge, and we already heard about "neuroprivacy". This new term entails examining another privacy sector to deal with, and it led us to create a neologism which we defined as "neuroprivacy rights". Hence, there is needing to investigate all the legal effects on data protection and privacy derived from applied technologies in the neuroscience field to clarify whether we have a new category of rights. We think it is crucial to apply the Data Protection and Privacy Relationships Model (its acronym is DAPPREMO) in this deepening path .

[1]The author acknowledges that this final version of the paper has been reviewed by the peer-editor.

Keywords: Data Protection, Privacy, Ethics, Artificial Intelligence, Neuroscience

1. ARTIFICIAL INTELLIGENCE AND EUROPE: AN OVERVIEW

In Europe, Artificial Intelligence's topic concerning data protection and privacy started sparking interest at an institutional level from 2016. In fact, at the 38th International Conference of Data Protection and Privacy Commissioners (ICDPPC, now Global Privacy Assembly - GPA) issued a "Room document" by the European Data Protection Supervisor - EDPS entitled "*Artificial Intelligence, Robotics, Privacy and Data Protection*" [1].

Successively, the European Group on Ethics in Science and New Technologies of the European Commission on 9 March 2018 issued the "*Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*" [2].

On 25 April 2018, the European Commission issued the "*Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe - COM(2018) 237 final*" [3]. At a later time, in June 2018, the European Commission appointed 52 independent experts to the High-level Expert Group on Artificial Intelligence to address AI.

The 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC, now Global Privacy Assembly - GPA), held in Brussels, 22-26 October 2018, issued a document titled "*Declaration on Ethics and Data Protection in Artificial Intelligence*" [4].

Later, on 18 December 2018 the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG) published (in the first version,

then updated on 8 April 2019) the document entitled "*Draft Ethics Guidelines for trustworthy AI*" [5].

Therefore, from 2019 some European Institutions started publishing documents on Artificial Intelligence. Thus, institutional production gradually intensified in 2020, demonstrating both what kind of interest in that important topic and the European Institutions' attention.

On 25 January 2019, the Council of Europe published the *Guidelines on artificial intelligence and data protection* adopted by the Committee of the Convention for the Protection of Individuals with regards to Processing of Personal Data (Convention 108) [6].

On 8 April 2019, the European Commission High-Level Expert Group on AI (AI HLEG) presented "*Ethics Guidelines for Trustworthy Artificial Intelligence*" [7].

In June 2019, The European Union Agency for Fundamental Rights (FRA) published the document entitled "*Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*" [8].

In February 2020 the European Commission published the "*White paper on Artificial Intelligence: a European 2020 approach to excellence and trust*" [9].

In April 2020 the Council of Europe published the "*Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*" [10].

In June 2020 the European Parliament published the "*Study on Opportunities of Artificial Intelligence*" [11] and the European Data Protection Supervisor (EDPS) the "*Opinion on the European Commission's White paper on Artificial Intelligence - A European approach to excellence and trust*" [12].

In July 2020 the European Parliament published the document entitled "*Artificial Intelligence and Civil Liability*" [13], while the European Commission High-Level Expert Group on Artificial Intelligence (AI HLEG) published the document entitled "*Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*" [14].

In September 2020 the European Parliament published the document entitled "*Civil liability regime for artificial intelligence - European added value assessment*" [15].

On 20 October 2020, the European Parliament published the document entitled "*Framework of ethical aspects of artificial intelligence, robotics and related technologies*" [16].

On 14 December 2020 the European Union Agency for Fundamental Rights (FRA) published the report entitled "*Getting the future right – Artificial intelligence and fundamental rights*" [17].

On 15 December 2020 the European Union Agency for Cybersecurity (ENISA) published the report entitled "*Artificial Intelligence Cybersecurity Challenges*" [18].

The aforementioned detailed list demonstrates and confirms how increased the interest in Artificial Intelligence's topic. Actually, that interest does not mean only particular attention to Artificial Intelligence, but it fundamentally shows how Europe, by its European Institutions, expresses sovereignty on this topic. Europe knows and realizes that AI is a crucial topic and a challenge.

Indeed, from our view, apart from some Artificial Intelligence criticality aspects such as biases, the strong position of European Institutions has the aim of controlling the matter.

On 21 April 2021 the European Commission proposed "*new rules and actions aiming to turn Europe into the global hub for trustworthy Artificial Intelligence (AI)*" [19]. Indeed, the European Commission published 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***" and the **Annexes** [20].

Before the mentioned proposal, it was a challenge to define Artificial Intelligence. Indeed, from all over the world, there was difficulty in defining Artificial Intelligence. Now the proposal lays down a definition of "**artificial intelligent system (AI system)**" as follows: "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".

Currently, the quoted definition is the first one to being laid down by law.

On this point, we mention what authoritative authors (Stuart Russel and Peter Norvig [21] in the book entitled "Artificial Intelligence. A Modern Approach - Fourth Edition") stated about the tentative of finding an Artificial definition: "*Historically, researchers have pursued several different versions of AI. Some have defined intelligence in terms fidelity to human performance, while others prefer an abstract, formal definition of intelligence called rationality–loosely speaking, doing the 'right thing'. The subject maYer itself also varies: some consider intelligence to be a property of internal thought processes and reasoning, while others focus on intelligent behavior, an external characteriza-*

tion. From these two dimensions – human vs. rational and thought vs behavior – there are four possible combinations, and there have been adherents and research programs for all four.".

Undoubtedly, the definition of an AI system as "software that is developed with one or more of the techniques and approaches" reveals how this is the results of very general research. It seems a highly vague definition.

What does it specifically mean "software developed with one or more of the techniques and approaches"? In our opinion, the definition seems too vague to define both Artificial Intelligence and an AI system.

Furthermore, the mentioned proposal on AI is based on the classification of AI systems as high-risk.

Before the final version, we hope that the legislator amends the proposal by providing a definition more adherent to the current status of the art considering adopting a scientific approach.

2. ARTIFICIAL INTELLIGENCE AND THE VOICE OF THE GLOBAL PRIVACY ASSEMBLY (GPA)

The Global Privacy Assembly, former International Conference of Data Protection and Privacy Commissioners (ICDPPC), "has been the premier global forum for data protection and privacy authorities for more than four decades.".

The GPA, recognizing Artificial Intelligence as a relevant topic, dealt with it issuing some documents and resolutions. Indeed, Artificial Intelligence has also been the main topic of the "Resolution on Accountability in the Development and Use of Artificial Intelligence" adopted in October 2020 by the 42nd Global Privacy Assembly (GPA) 2020 – At your desk.

The GPA adopted two resolutions and specifically "*Resolution on Accountability in the Development and Use of Artificial Intelligence*" [22] and "*Resolution on facial recognition technology*" [23].

In the first part of the "**Resolution on accountability in the development and use of artificial intelligence**" we read some statements, among which we highlight the following ones:

"*Affirming that the responsibility for the operation and effects of AI systems remains with human actors*";

"*Emphasising that the principle of accountability encompasses accountability to the people affected by the decisions made by or with AI systems, as well as to supervisory authorities and, where appropriate, to other third parties, and that beyond the compliance element, accountability should also be demonstrated in order to build trust with the stakeholders*";

"*Recognising that AI systems may affect human rights in different ways, the application of specific obligations should take into account the risks for human rights as well as the importance of the principle of human accountability.*".

In the second part, the GPA takes a position and resolves to declare five points of which we report the first two:

"*1. urge organisations that develop or use AI systems to consider implementing twelve accountability measures there precisely listed among which the first one is "Assess the potential impact to human rights (including data protection and privacy rights) before the development and/or use of AI. 2. urge organisations that develop or use AI systems to implement accountability measures which are appropriate regarding the risks of interference with human rights.*".

From the parts of the resolution we quoted, it emerges, specific attention to human rights that must never be compromised.

Regarding the "**Resolution on facial recognition technology**" the GPA arising some concerns, highlights "*that facial recognition technology has the capability to enable widespread surveillance, to be highly intrusive, provide biased results, and erode data protection, privacy and human rights, which in turn reduces trust and confidence in its use.*".

Thus, in this resolution, the GPA reiterates the importance of "data protection by design and by default" principles, pointing on some general statements to take into account.

3. THE EUROPEAN LEGAL FRAMEWORK ON DATA PROTECTION AND PRIVACY

It is necessary to briefly describe the European legal framework on the protection of natural persons with regard to the processing of personal data.

In Europe, firstly, we mention the Charter of Fundamental Rights of the European Union [24] which state the right to privacy (Article 7) and the right to the protection of personal data concerning him or her (Article 8).

Furthermore, we mention the Convention 108 [25], which has been modernized in 2018 [26].

Finally, we mention the EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [27].

The legislations, as mentioned above, are the main three pillars in Europe.

4. THE DATA PROTECTION AND PRIVACY RELATIONSHIPS MODEL (DAPPREMO)

In our latest book [29], we described the Data Protection and Privacy Relationships Model (**DAPPREMO**).

The proposed model is based on set theory, where each area (e.g. privacy, personal data protection, Internet of Things, Public Administration sectors, private sectors, etc.) constitutes a set, and that is a domain. In everyday activities, there are always relationships between areas or domains. Indeed, the "protection of personal data" (which is a domain) has a relationship - for example - with that of a specific Publica Administration sector, or an IoT ecosystem, or a private sector. The model assumes greater complexity where the relationships between domains increase and may even tend to infinity.

The aim is to demonstrate that the application of this model, allowing a much broader view of the phenomena, allows a more precise evaluation of domains and individual relationships. As a result, there are, undoubtedly, beneficial effects for the entire system of analysis and especially concerning subjective profiles as will be illustrated later.

The activities carried out daily both for work, and personal needs are part (processes) of the system of the reality in which we live.

However, very often, activities and related processes are not correctly observed due to a short-sighted two-dimensional vision that is entirely reductive. The use of the most modern technological solutions has allowed us to see the so-called "augmented reality", i.e. multidimensional contexts. Therefore, if we observed phenomena not on a two-dimensional plane but a three-dimensional or multidimensional one, we would have the possibility to perceive with greater precision any component.

Our study observed that the system of relations we described could find some similarities with a complex structure, borrowed from advanced mathematics, known as the "fiber bundle set". In this way, that model would seem to account for the interactions and connections that occur both between individual elements and between sets of elements.

We consider the model like a first and innovative approach, still under development, to a mathematical interpretation of the multidimensional interrelational framework. However, our model seems to have the merit of providing a unifying and abstract vision to a scenario of high complexity, such as the one on which we intend to focus our study investigation.

The complexity of the "fiber bundle" makes its description not simple. Still, we can illustrate it as a brush (see figure below) where the shaft represents, in our case, the data protection set, and the individual bristles constitute the relationships and connections between sets and objects of each other set.

The complexity of the model, at times, can make the dynamic aspect escape and lose sight of it, leaving space to focus only on the static part of the core that corresponds to the regulations in force. The regulatory discipline is not and cannot be an end in itself. Still, we must evaluate it as a contributing element to analysing a complex and dynamic context.

The ecosystem data protection attributes are numerous and, some precise and identified, and others indefinite and indeterminable. There is undoubtedly ethics among the specific fundamental objects, which is a crucial and essential element for the analysis of every single scenario. Ethics can seem an exogenous factor, extraneous to the set of rules governing the matter of the protection of personal data. In reality, this is not the case because the reference to ethics emerges from the principles of the whole body of rules. Thus, ethics is very close to the effects of the other elements of the whole (the legal norms) in terms of the same characteristic property that unites them.

The proposed model, which is called DAPPREMO, acronym of Data Protection Relationships Model, can be expressed mathematically through the concept of equivalence relationships.

5. THE RELATIONSHIP BETWEEN NEUROSCIENCE AND PRIVACY

The field of neuroscience is vast and complex.

We do not intend to delve into neuroscience, but only to assess, according to the Regulation UE 2016/679 (GDPR) [27] and the legislation as mentioned above, what impact the technologies used have on personal data and thus on individuals.

There is copious scientific literature on neuroscience and privacy, but our approach also intends to consider some aspects deriving from the analysis of people's behavior.

We know that sometimes scientists are using Artificial Intelligence and high-level technologies to deepen the effects of their studies on humans and their brains in the neuroscience domain. We also know that some laboratory carried out experiments on animals using high-level technologies and artificial intelligence to deepen the brain reaction [28].

Thus, it is clear that scientific research into the neuroscience domain is making use more and more artifi-

cial intelligence and the most innovative technologies to carry out experiments aiming to discover something of the most profound and intimate of the human being.

What are the human brain's reactions?

Do we know, or can we forecast the human brain's reactions?

These questions are both crucial and eloquent at the same time, also without any answer. Is there a limit to the science (in this case, neuroscience) to the use of artificial intelligence and high-technologies when the purposes are private investigations?

Undoubtedly, an approach only technological-based does not consider other aspects especially related to the human being.

It is fundamental always to guarantee a natural person his or her right to have full control over any possible decision, especially in data protection, underlining that the consent has to be freely and unconditionally given.

People should know in advance what are the purposes for which in researches scientists use high-technologies to carry out results and especially whether there are analysis and investigations (more or less deep) on intimate human aspects. People should take into account the impact on data protection and privacy of technologies used in the neuroscience to analyze human behavior in general, considering different degrees of invasiveness and hence how much they can affect human behavior and decisions.

What about human dignity when technologies compromise people's decisions and consents?

In fact, the DAPPREMO approach effectively allows us to achieve the necessary instrument-keys to qualify the scenario and find the most valuable legal solution.

Indeed, it is well-known that privacy and the protection of personal data are two different aspects, so much so that, in Europe, each one constitutes fundamental rights.

Therefore, technologies used in neuroscience may affect both privacy and the protection of individuals with regard to the processing of personal data.

In their daily lives, human beings communicate and behave differently depending on the situations they find themselves in.

Hence, considering people's everyday context, it emerges that the brain induces a particular type of verbal communication in each person depending on the context in which they find themselves. Similarly, non-verbal communication, i.e., which each individual expresses with his or her body, should not be underestimated.

These brief considerations are well-known in the field of neurolinguistic programming (NLP).

We believe that there might be severe impacts on the privacy and protection of individuals' personal data only from the analysis of their behavior according to the NLP. However, apart from the NLP, there are other aspects related to clinical or laboratory investigations such as, for instance, magnetic resonance (MRI) and functional magnetic resonance imaging (MRIf) which are much more invasive for privacy and personal data protection.

With NLP, for example, it would be possible to analyze the behavior of people who, if affected by a disease, would act differently from those who are not affected. The mentioned scenario poses privacy and data protection problems for sensitive information that needs to be adequately protected, even outside the medical context.

In essence, the human brain's impulses would be useful for identifying intimate aspects belonging to the human person.

In the light of this, it is clear that high technologies in neuroscience can lead to the not tricky situation of interfering with the most intimate aspects of a human being and even influencing their behavior or even revealing what a person is thinking.

We know that experiments have been done on some animals basically to understand their thinking, but it is extraordinarily worrying if scientists were applying those researches to humans.

We should also consider that neuroscience is not exempt from Ethics, one of the crucial aspects not expressly mentioned in the European legislation.

We also have to take into account the relationships between Ethics and Artificial Intelligence. Indeed, it is challenging (impossible?) to develop an algorithm with instructions with ethical connotations.

We also have to take into account the relationships between Ethics and Artificial Intelligence. Indeed, it is challenging (impossible?) to develop an algorithm to execute ethics instructions (good or bad) and produce a correct output without any biases.

Indeed, it is well-known that one of the main risks in Artificial Intelligence is bias because it is an unpredictable and uncontrollable element and also strictly related to the human being: it is a variable. For these reasons, it does not allow to have a final secure and specific result.

We could have consequences by compromising intimate human components and, undoubtedly, the infringement of the data protection and privacy laws for unlawful processing.

The above brief considerations, for which we reserve

the right to go into further detail, constitute a minimum requirement for assessing European data protection legislation compliance.

The European legislation (the GDPR, Convention 108 and the Charter of Fundamental Rights of the European Union) protects natural persons with regard to the processing of personal data and consequently human dignity.

It is not allowed to compromise human dignity as the highest value, also when - albeit for scientific reasons - investigations are conducted that may present risks to data subjects' fundamental rights and freedoms.

6. CONCLUSIONS

It would be a mistake to impede technological evolution and interfere with the development of technical solutions.

It is not even possible to think of separating technologies from our daily lives. We live in symbiosis with technologies and cannot do without them.

Real-life is almost overlapping with virtual life, especially since the COVID19 pandemic was declared, as we have been forced to make greater use of the available technologies.

Indeed, the supply of digital services has increased.

Nevertheless, we cannot disregard data protection rules.

As we have made clear, there are other aspects that we very often do not take into account when analyzing reality, and that is why we have proposed an approach based on the model called DAPPREMO.

In conclusion, the technologies used in neuroscience and the scientific studies that are carried out must not disregard privacy and the protection of individuals with regard to the processing of personal data.

Neural data are personal data and, as they are biometric data, subject to a specific legal framework.

We should not allow too invasive investigations into the human brain, which cannot be controlled by the person concerned, and which even have an impact on thinking.

The results would be dramatic if we only thought of artificial intelligence-based systems that could understand what a human being is thinking.

REFERENCES

[1] 38th International Conference of Data Protection and Privacy Commissioners, European Data Protection Supervisor - EDPS, "Artificial Intelligence, Robotics, Privacy and Data Protection" https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf [retrieved: May, 2021]

[2] European Group on Ethics in Science and New Technologies (2018). Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems. https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf#view=fit&pagemode=none [retrieved: May, 2021]

[3] European Commission (2018). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe - COM(2018) 237 final. https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe [retrieved: May, 2021]

[4] 40th International Conference of Data Protection and Privacy Commissioners, Declaration on Ethics and Data Protection in Artificial Intelligence, 2018 https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf [retrieved: May, 2021]

[5] European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), Draft Ethics guidelines for trustworthy AI, 2018, https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai [retrieved: May, 2021]

[6] Council of Europe - Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) (2021). Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3EuropeanUnion(2012).CharterofFundamentalRightsoftheEuropeanUnion.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN [retrieved: May, 2021]

[7] European Commission (2019. Ethics Guidelines for Trustworthy AI" by the High-Level Expert Group on Artificial Intelligence (AI HLEG). https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top [retrieved: May, 2021]

[8] European Union Agency For Fundamental Rights - FRA, Data quality and artificial intelligence – mitigating bias and

error to protect fundamental rights, 2019 https://fra.europa.eu/en/publication/2019/data-quality-and-artificial-intelligence-mitigating-bias-and-error-protect [retrieved: May, 2021]

[9] European Commission, White Paper on Artificial Intelligence: a European approach to excellence and trust, 2020 https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en [retrieved: May, 2021]

[10] Council of Europe, "Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems", 2020 https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154 [retrieved: May, 2021]

[11] European Parliament, Study on Opportunities of Artificial Intelligence, 2020 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf [retrieved: May, 2021]

[12] European Data Protection Supervisor - EDPS, Opinion 4/2020 - EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, 2020 https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf [retrieved: May, 2021]

[13] European Parliament - Think Thank, Artificial Intelligence and Civil Liability, 2020 https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)621926 [retrieved: May, 2021]

[14] European Commission - High-Level Expert Group on Artificial Intelligence (AI HLEG), "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment", 2020 https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment [retrieved: May, 2021]

[15] European Parliament - Think Thank, Civil liability regime for artificial intelligence, 2020 https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)654178 [retrieved: May, 2021]

[16] European Parliament, Framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html [retrieved: May, 2021]

[17] European Union Agency For Fundamental Rights - FRA, Getting the future right – Artificial intelligence and fundamental rights, 2020 https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights [retrieved: May, 2021]

[18] European Union Agency For Cybersecurity - ENISA, Artificial Intelligence Cybersecurity Challenges, 2020 https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges [retrieved: May, 2021]

[19] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, 21 April 2021 https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 [retrieved: May, 2021]

[20] 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 - Annexes https://ec.europa.eu/newsroom/dae/items/709090 [retrieved: May, 2021]

[21] Stuart Russel, Peter Norvig, Artificial Intelligence. A modern approach. Fourth Edition, 2020, Pearson

[22] 42nd Closed Session of the Global Privacy Assembly - GPA, "Resolution on accountability in the development and use of Artificial Intelligence", 2020 https://globalprivacyassembly.org/wp-content/uploads/2020/11/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf [retrieved: May, 2021]

[23] 42nd Closed Session of the Global Privacy Assembly - GPA, "Resolution on facial recognition technology", 2020 https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Facial-Recognition-Technology-EN.pdf [retrieved: May, 2021]

[24] Charter of Fundamental Rights of the European Union, 2016 https://www.ecb.europa.eu/ecb/legal/pdf/oj_c_2016_202_full_en_txt.pdf [retrieved: May, 2021]

[25] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", 1981 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 [retrieved: May, 2021]

[26] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223", 2018 https://rm.coe.int/16808ade9d [retrieved: May, 2021]

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [retrieved: May, 2021]

[28] Elon Musk's Neuralink explains how a monkey used its brain-computer tech to play Pong https://www.cnbc.com/2021/04/09/elon-musks-neuralink-shows-video-of-monkey-using-mind-to-play-pong.html [retrieved: May, 2021]

[29] Nicola Fabiano, GDPR & Privacy. Awareness and opportunities. The approach with the Data Protection and Privacy Relationships Model (DAPPREMO), 2020, goWare

[30] Adam D. Moore, Privacy, Neuroscience, and Neuro-Surveillance, in Res Publica A Journal of Moral, Legal and Social Philosophy, 2016

[31] Sarah Richmond, Geraint Rees, and Sarah J.L. Edwards, "I Know What You're Thinking Brain imaging and mental privacy Edited", 2012

[32] Parag Chatterjee, Emmanuel Benoist, Asoke Nath, Applied Approach to Privacy and Security for the Internet of Things, 2020, IGI Global.

[33] Nicola Fabiano, European Data Protection Regulation and the Blockchain Analysis of the Critical Issues and Possible Solution Proposals, 2018

[34] Nicola Fabiano, Robotics, Big Data, Ethics and Data Protection: A Matter of Approach, In Robotics and Well-Being, 2019, Springer

[35] European Data Protection Supervisor – EDPS (2016). Artificial Intelligence, Robotics, Privacy and Data Protection. https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf [retrieved: May, 2021]

[36] European Data Protection Supervisor – EDPS (2015). Opinion 4/2015 - Towards a new digital ethics. Data, dignity and technology. https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf [retrieved: May, 2021]

[37] 38th International Conference of Data Protection and Privacy Commissioners, "Informal reflections on policy questions", 2016 https://icdppc.org/wp-content/uploads/2015/03/Robotics-and-artificial-intelligence-session-Informal-reflections-on-policy-questions.pdf [retrieved: May, 2021]

[38] Information Commissioner's Office – ICO (2017). Big data, artificial intelligence, machine learning and data protection. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [retrieved: May, 2021]

[39] European Parliament (2017). European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf?redirect [retrieved: May, 2021]

[40] European Data Protection Supervisor – EDPS (2018). Choose Humanity: Putting Dignity back into Digital. https://www.privacyconference2018.org/system/files/2018-10/Choose%20Humanity%20speech_0.pdf [retrieved: May, 2021]

[41] Council of Europe (2013). European Convention on Human Rights. https://www.echr.coe.int/Documents/Convention_ENG.pdf [retrieved: February, 2021]

[42] AI Now Institute at New York University (2018). Now Report 2018. https://ainowinstitute.org/AI_Now_2018_Report.pdf [retrieved: May, 2021]

[43] European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and Autonomous Systems, 2018 https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf#view=fit&pagemode=none [retrieved: May, 2021]

[44] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe - COM(2018) 237 final, 2018 https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe [retrieved: May, 2021]

[45] G. Buttarelli - European Data Protection Supervisor, Choose Humanity: Putting Dignity back into Digital, 2018 https://www.privacyconference2018.org/system/files/2018-10/Choose%20Humanity%20speech_0.pdf [retrieved: May, 2021]

[46] European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, 2019. https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en [retrieved: May, 2021]

[47] European Data Protection Supervisor - EDPS, Artificial Intelligence, Robotics, Privacy and Data Protection, 2016, https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf [retrieved: May, 2021]

[48] The Treaty on the functioning of the European Union (2016/C 202/01), 2016. https://www.ecb.europa.eu/ecb/legal/pdf/oj_c_2016_202_full_en_txt.pdf [retrieved: May, 2021]

[49] Information Commissioner's Office, Big data, artificial intelligence, machine learning and data protection, 2017 https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [retrieved: May, 2021]

[50] European Parliament, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)),2017 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN [retrieved: May, 2021]

[51] J. Pandya, Is The Future Of Artificial Intelligence Tied To The Future Of Blockchain? https://www.forbes.com/sites/cognitiveworld/2019/03/29/is-the-future-of-artificial-intelligence-tied-to-the-future-of-blockchain/ [retrieved: May, 2021]

[52] European Data Protection Supervisor (EDPS), Opinion 4/2015 - Towards a new digital ethics. Data dignity and technology, 2015 https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf [retrieved: May, 2021]

[53] Nicola Fabiano, "Privacy and Security in the Internet of Things", in Cutter IT Journal, Vol. 26, No. 8, August 2013