

# INFORMED CONSENT:

## Mission (im)possible, and other risk remedies in data processing

# Democracy versus autocracy. Why the democratic system is superior and how it can defeat autocracy

Informed consent: mission (im)possible, and other risk remedies in data processing

**Author: Liubomir NIKIFOROV**

**Brussels, October 2022**

© Institute of European Democrats, 2022  
Rue Montoyer 25 1000 Brussels Belgium  
**[www.iedonline.eu](http://www.iedonline.eu)**



This Research Paper was elaborated on the basis of independent research. The opinions expressed here are those of the Contractor and do not represent the point of view of the Institute of European Democrats. With the financial support of the European Parliament

## EXECUTIVE SUMMARY

The European General Data Protection Regulation (GDPR) has been a recurrent target of academic and policy analysis even before its entering into force in 2018. This policy paper continues further those discussions by studying the mechanism of informed consent, in particular, for automated data processing. We review briefly consent's history and draw a parallel with consent for medical purposes. Next, we describe current legal framework underpinning consent-based automated data processing in order to point out the challenges thereof. Those include the moment and magnitude of human intervention, users' understanding of the automated decision-making process as well as the externalities of increased transparency. Based on this paper, we recommend that a revision of the Arts 15 and 22 of the Regulation and further development of the guidelines on the design of consent notices.

## Social Media summary

GDPR needs precision and improved consent mechanism, ensuring transparency and algorithm understanding.

## Keywords

#digitaldemocracy, #consent, #AI, #dataprotection, #privacy, #GDPR, #transparency, #explainability

## Short bio

For the past couple of years, Liubomir Nikiforov has been a PhD candidate researching on data protection, transparency and digital rights for a more transparent, fair and accountable digital society. Before that, he graduated from the European Master in Law and Economics, where he has awarded the Deutschlandstipendium. He is an ICANN fellow and active member of the University of Barcelona PhD community.



*This Research Paper was elaborated on the basis of independent research. The opinions expressed here are those of the Contractor and do not represent the point of view of the Institute of European Democrats.*

## TABLE OF CONTENTS

<b>I. INTRODUCTION</b>	<b>6</b>
<b>II. BRIEF HISTORY</b>	<b>7</b>
2.1. Consent for medical purposes	7
2.2. Consent for data processing	8
<b>III. LEGAL FRAMEWORK</b>	<b>10</b>
3.1. Elements of a valid consent. GDPR.	10
3.1.1. Free	10
3.1.2. Specific	11
3.1.3. Unambiguous	11
3.1.4. Informed	12
3.2. Types of consent	12
3.3. Consent for automated decision-making. Art. 22, GDPR	13
3.3.1. "Solely on automated processing"	13
3.3.2. "Legal" effects or similar	14
3.4. Information as transparency measure	15
<b>IV. CHALLENGES</b>	<b>16</b>
4.1. Human intervention as the Schrödinger's cat	16
4.2. We don't understand it	17
4.3. All that glitters is not gold	19
<b>V. CONCLUSION</b>	<b>21</b>
<b>VI. POLICY RECOMMENDATIONS</b>	<b>22</b>
<b>BIBLIOGRAPHY</b>	<b>24</b>

## TABLE OF ACRONYMS

<b>AI</b>	Artificial intelligence
<b>CJEU</b>	Court of Justice of the European Union
<b>CoE</b>	Council of Europe
<b>EDPB</b>	European Data Protection Board
<b>EU</b>	European Union
<b>GDPR</b>	General Data Protection Regulation
<b>IP</b>	Intellectual Property
<b>OCDE</b>	Organisation for Economic Co-operation and Development
<b>WP 29</b>	Article 29 Working party
<b>XAI</b>	Explainable Artificial Intelligence

## I. INTRODUCTION

The entering into force of the General Data Protection Regulation (GDPR)<sup>1</sup> in 2018 has marked a milestone in European data protection history. It has built upon the old Data Protection Directive (Directive 95/46/EC)<sup>2</sup>, and it has updated its provisions. Despite the endemic delay of our legislation in responding to technological progress and the challenges thereof, EU data protection law answers to citizens' concerns about their rights by preserving freedom of choice online, and ensuring democratic participation in the digital public space<sup>3</sup>.

Some decades ago, we considered it far-fetched that our digital footprint might be conceived as a prolongation of our physical personality producing unique consequences. However, what seemed inspired in a cyberpunk movie, today is a reality. This paper addresses some of the concerns related to the automated processing of our personal data, conceived as a form of citizens' democratic participation in the digital age. With this objective, we analyse the mechanism of informed consent as a legitimate data processing basis in the private sector. We do it on the premise that consent is an imperfect, but effective mechanism ensuring users' dignity and autonomy through transparency, fairness and accountability in automated decision-making processes. This is why we consider informed consent as one of the democratic guarantees of our digital rights and dignity on the Internet contributing to the prevention of a future where our autonomy and democratic rights are reduced to formality.

We conduct an interdisciplinary analysis of the current data protection state on the matter of consent, including its required elements for validity. We build upon this initial picture by adding up an analysis of the transparency and information challenges related to the informed consent for automated data processing. This research paper concludes with suggestions of concrete policy recommendations to the issues raised.

The conclusions of this paper are founded on the analysis of previous research papers, academic literature, existing legislation and jurisprudence as well as the opinions and guidelines of the former WP29, and current EDPB. The structure of this research paper includes an introduction to the topic (I.), followed by a brief history of consent (II.), and legal framework (III). Next, we discuss the challenges (IV.) thereof, coupled with concrete policy recommendations (VI.).

---

<sup>1</sup> 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), 4 May 2016, OJ L 119/1, pp. 1–88

<sup>2</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 23 October 1995, OJ L 281/31, pp. 1-20

<sup>3</sup> European Commission, May 4, 2022, European Digital Rights and Principles. *Shaping Europe's Digital Future*, <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>, last accessed 12.08.2022

Before proceeding to the description and analysis of the legal framework, we consider illustrative for the sake of this paper to provide a brief overview of the historical development and main conceptual sources of informed consent in order to complete the context in which the object of our study evolves.

## II. BRIEF HISTORY

The 2017 movie “Ghost in Shell” depicts a future where a robotics company develops a cyborg soldier, Major Mira Killian, with human mind, but synthetic body. After successfully reducing a group of cyber-terrorists, she decides to penetrate the system of an AI geisha in order to trace back the attack perpetrator. After the operation, the Major’s synthetic body designer, Dr. Ouelet demands the soldier’s consent to access and analyse her body algorithm for possible damages. Mira Kilian consents ...

### 2.1. Consent for medical purposes

Consent is an expression of someone’s autonomy through his/her knowledge and will<sup>4</sup>. In the recent decades with the development of technology and massive personal data collection, consent has emerged as one of the bases for lawful data processing. However, its history as a tool, which reflects an individual’s autonomy to decide, dates back to Antiquity. Plato referred to consent as an attribute of a free person, while Hippocrates saw a connection between the disease and the patient’s agreement to the treatment<sup>5</sup>.

In more recent times, and within the context of ever more complex and intertwined co-dependences between different knowledge domains such as biology, philosophy and technology, among others, the interdisciplinary field of Bioethics emerged. Beauchamp and Childress (2019) establish the four main principles of Bioethics: beneficence, non-maleficence, justice, and autonomy. Within this axiological taxonomy, consent relates most closely to the notion of autonomy as an expression of human moral independence, dignity and ultimately freedom.

Consent conceived as a “power-to-decide”<sup>6</sup>, enshrined within this principle, portrays a gradual shift in the historical relationship between a healthcare professional and a patient. Traditional doctor-patient relationship is inherently paternalistic. The patient is the receiver of a treatment prescribed by a professional, vested with the authority of his expertise and knowledge, who decides as a *caring father* on the right treatment. This paradigm experienced a gradual shift towards a relationship where the patient is empowered to his/her own decisions and bears

<sup>4</sup> Beauchamp, T. and Childress, J., 2019. *Principles of biomedical ethics*. 8th ed. New York, NY: Oxford University Press.

<sup>5</sup> Dalla-Vorgia, P., 2001. Is consent in medicine a concept only of modern times? *Journal of Medical Ethics*, 27(1), pp.59–61.

<sup>6</sup> Floridi, L. & Cowls, J., 2019. A unified framework of five principles for AI in society. *Harvard Data Science Review*. 1(1)



the consequences thereof. Thus, current medical consent stems from the ethical and legal premises that health professionals should approach pathogens' treatment, not only from a technical standpoint, i.e. with the pertinent knowledge of the human body, but they should also take into consideration patients' understanding, opinion and will.

This brief overview of consent for medical purposes is illustrative for our discussion because it lays down the background, which inspires consent mechanisms in other domains such as data processing.

## 2.2. Consent for data processing

The core idea behind consent as a tool empowering individuals in a power-asymmetric relation remains the same for data processing. Its principles parallel those of consent for medical purposes. We cannot comprehensively explore them in this paper. However, while asserting that bioethical principles respond to the challenges posed by artificial intelligence (AI), Floridi L. et al. (2018) propose to introduce an additional "explainability principle"<sup>7</sup> to the original four. Thus, explainability would act as a mechanism to ensure an intelligible and accountable AI<sup>8</sup>. We deal in detail with the problem of explainability in the part dedicated to the informed consent challenges.

Consent as a lawful basis for data processing should be regarded as a component of the development of data protection and privacy policies.<sup>9</sup> In 1968, the Council of Europe (CoE) adopted Recommendation 509 on Human rights and modern scientific and technological developments, which is considered to have inspired later European data protection legislation. Although the notion of privacy as a separate right was already being discussed in the 19<sup>th</sup> century<sup>10</sup>, it was not until

---

<sup>7</sup> Floridi, L. et al., 2018. AI4People—an ethical framework for a good AI Society: Opportunities, Risks, principles, and recommendations. *Minds and Machines*, 28(4), pp.689–707.

<sup>8</sup> Floridi, L. et al., 2018. AI4People—an ethical framework for a good AI Society: Opportunities, Risks, principles, and recommendations. *Minds and Machines*, 28(4), pp.689–707.

<sup>9</sup> Murillo de la Cueva, P.L. & Piñar Mañas, J.L., 2009. *El derecho a la autodeterminación informativa*, Madrid: Fundacion Coloquio Jurídico Europeo.

<sup>10</sup> Warren, S.D. & Brandeis, L.D., 1891. The right to privacy. *Harvard Law Review*, 4(5), pp.193–220.



the late 70-80s of the last century when in some European countries<sup>11</sup> privacy and data protection acts were first adopted.<sup>12</sup>

Of specific interest for the topic of this research is the German data protection legislation development. The Hessian Data Protection Act adopted in 1970 is the European and the world oldest data protection law. A decade later in 1983 the German Constitutional court adopted a landmark decision establishing a right of “informational self-determination”<sup>13</sup>. This decision is based on the idea that dignity, privacy and freedom to decide by oneself should be legally guaranteed in the digital environment as well<sup>14</sup>.

Next to the European national legislation of the period, we can follow similar trends within international organizations’ work such as the Council of Europe (CoE)<sup>15</sup> and OECD<sup>16</sup>. However, the most influential legal document remains the Directive 95/46/EC. Finally, we can mention the Charter of Fundamental Rights of the European Union<sup>17</sup>. This primary<sup>18</sup> EU piece of legislation established the right to privacy (Art.7), and the right to data protection (Art. 8) as fundamental rights for the citizens of the Union. Moreover, in the light of our study, it recognized explicitly that personal data should be “processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”<sup>19</sup>.

In this section, we have described briefly the historical background, which inspired legislators on the matter of data protection. In the next lines, we proceed with the description of the current legal framework, dominated by the GDPR.

---

<sup>11</sup> As a matter of example of the role of consent as a lawful ground for data processing, we can mention the 1973 Swedish data act, Datalag (1973:289), and the 1978 French Data Protection Act, Loi N° 78-17, the 1978 Danish Private Registers Act (LBK nr 622 af 02/10/1987) and the Public Authorities’ Registers Act (LOV nr 294 af 08/06/1978), the 1978 Norwegian Personal Data Registers Act, the 1979 Austrian data protection act (BGBl I Nr. 565/1978).

<sup>12</sup> van der Sloot, B., 2014. Do data protection rules protect the individual and should they? an assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, 4(4), pp.307–325.

<sup>13</sup> Bundesverfassungsgericht (BVerfG). Urteil des Ersten Senats vom 15. Dezember 1983 (Judgement of the first senate of 15 December 1983) -1 BvR 209/83, Rn. 1-215 - ECLI:DE:BVerfG:1983:rs19831215.1bvr020983

<sup>14</sup> Eberle, E.J., 2012, Observations on the development of human dignity and personality in German constitutional law: An overview. *Liverpool Law Review*, 33(3), pp.201–233.

<sup>15</sup> Council of Europe, 1981, “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (Convention 108), ETS No. 108, Council of Europe.

<sup>16</sup> OECD, 2002, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris.

<sup>17</sup> Charter of Fundamental Rights of the European Union, 2000, OJ C 364/1

<sup>18</sup> It was enacted in 2000, and since the entry into force of the Lisbon Treaty in 2009, it has the status of primary EU law.

<sup>19</sup> Art. 8 EU Charter of Fundamental Rights.

### III. LEGAL FRAMEWORK

Within this section, we discuss the mechanism of consent as a tool for lawful data processing, along with the requirements for its validity within the framework of the European data protection regulation. We define consent and identify the context in which it applies.

#### 3.1. Elements of a valid consent. GDPR.

The GDPR establishes in its Art. 6 different grounds for lawful data processing, among which we find consent (Art. 6 (1)(a)). The specific context and conditions to be met for a valid consent could be found in Article 4 and Articles 7 to 9. Article 22 gives additional guidance in those cases where automated data processing applies. We discuss those dispositions in the following lines.

Whenever data controllers rely on consent for the processing of personal data they should make sure that it is obtained through clear manifestation of the data subject's will. As put by the European Data Protection Board (EDPB) "merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation."<sup>20</sup> In other words, data controller should have an undoubted proof that the data subject has taken deliberate action to consent for the collection of his/her data.

The Regulation contains a definition of consent in its Art. 4 (11), where it is described as "any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"<sup>21</sup>. Given this framework, we discuss the different tokens of this definition, and their intended objective below.

##### 3.1.1. Free

Drawing on the Guidelines of the EDPB on consent<sup>22</sup>, we can conclude that consent cannot be esteemed "freely given", if no other alternatives were available to the users within the services of the same provider<sup>23</sup>, nor if an individual was forced to consent. Neither can we refer to a "free" consent in those cases where the lack of data subject's consent would suggest a refusal to access the service in question, or would entail any type of detriment for the user.

The existence of a vertical relationship between the data subject, and the data controller or processor puts serious doubts on the freedom of consent. For

<sup>20</sup> EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12, para. 84

<sup>21</sup> Art. 4 (11) GDPR

<sup>22</sup> EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12

<sup>23</sup> EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12, para. 38

example, in the case of citizens' data processing by the public administration for tax collection purposes, we cannot speak about a "free" consent. This is so, because data subjects do not have real choice whether to provide or not information about their income. This imbalance of powers is recognized throughout the whole text of the Regulation, namely, in Recitals 42 and 43, and most importantly, in Art. 6 (1)(e). Aware of those issues, the legislator prescribed expressly that EU and national administrations would not need to obtain consent from data subjects.

Also, in hierarchical relations such as employer-employee, where there is a clear power imbalance, we cannot expect a consent to be "freely given". Not only because the data subject may suffer negative consequences of his/her refusal to consent, but also because other bases, more appropriate for the processing of data, may apply such as those necessary for the performance of a contract (Art. 6 (1)(b)) or for the compliance with a legal obligation (Art. 6 (1)(c)).

### 3.1.2. Specific

One of the cornerstones of the EU data protection legislation is the principle of "purpose limitation" (Art. 5 (b)). From a formal point of view, a consent notice should include controllers'/'s identity and a detailed list of all the purposes of the processing<sup>24</sup> as well as information about any further data management, and related data subject's rights<sup>25</sup>. A valid consent should be as "specific" as possible in order to "ensure a degree of user control and transparency for the data subject"<sup>26</sup>. For that reason, the data controller has to tailor it so that it reflects in a clear and understandable way the specific "legitimate"<sup>27</sup> purposes for which consent is required as well as the intended use of the collected data.

### 3.1.3. Unambiguous

One of the novelties of the GDPR compared to the derogated Directive 95/46/EC<sup>28</sup> is the introduction of a new element in the definition of consent. The requisite that consent has to be "unambiguous" entails a requirement to the data controller to obtain a clear statement and/or affirmative act that the data subject "have taken a deliberate action to consent to the particular processing"<sup>29</sup>. This is why consent should be worded in a clear and understandable language, void of technical expressions, and in the format considered most appropriate for the

<sup>24</sup> Recital 42, GDPR

<sup>25</sup> EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12, para. 64

<sup>26</sup> EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12, para. 55

<sup>27</sup> EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12, para. 58

<sup>28</sup> Directive 95/46/EC, Art. 2 (h) "the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

<sup>29</sup> EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12, para. 77

occasion, including written, oral, and/or electronic form<sup>30</sup>. An important caveat is that any pre-filled in boxes, or “opt-out” buttons within the consent notice are not considered valid consent, as confirmed by the CJEU recent case law<sup>31</sup>.

### 3.1.4. Informed

The Art. 5 (1)(a), GDPR, lawfulness, fairness and transparency principle finds embodiment in the requirement for a detailed description of the intended purposes for the data collection (3.1.2. Specific). However, it is in the requirement for a consent to be informed where it finds its full application.

This is a pivotal requirement for the validity of the consent, because no consent is possible without clear and comprehensive information about what the data subject is consenting for. This means that the information has to be in a plain, adapted and easily understandable language, avoiding technical terms.<sup>32</sup> There should be no misunderstanding about the place of the informed consent within the privacy notice so that data subject can easily distinguish it from other provisions.<sup>33</sup> Moreover, when it comes to processing, which involves algorithm-based software (art. 22), data controllers should put extra efforts in explaining the process of data management as well as the consequences thereof (Art.15 (h)).

We advance that this requirement caused a lot of debate in the academic community, because of the much-debated existence of a “right to explanation”. We discuss those issues further in this paper. However, before doing that, we need to explore what types of consent there are and when they apply.

### 3.2. Types of consent

Generally, the GDPR requires a free, specific, informed and unambiguous indication of will for the collection, processing and storage of personal data. However, for processing of certain categories of personal data, which present a significant risk for the data subject’s rights, the required level of protection is higher. Therefore, the GDPR establishes in practice two types of consent. We will call the first one, which we have already explored (in 3.1.), “ordinary”. The second one receives its name from the wording of the Regulation, namely, “explicit consent”. Although the GDPR does not establish formally such taxonomy, neither provides a definition of “explicit consent”, we find it illustrative to draw such a separation, moreover, because the Article 29 Data protection working party (WP29), and later the EDPB in their documents, adopt the same approach.

Thus, while a free, specific, informed and unambiguous act of will qualifies as an “ordinary” consent for the processing of personal data, “explicit” consent is

---

<sup>30</sup> Recital 32, GDPR

<sup>31</sup> Judgement of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901; and Judgement of the Court of 1 October 2019, *Planet49*, C-673/17 ECLI:EU:C:2019:801

<sup>32</sup> EDPB, “Guidelines 05/2020 on consent under Regulation 2016/679”, 4 May 2020 (Version 1.1.), pp.1-12, para. 67

<sup>33</sup> EDPB, “Guidelines 05/2020 on consent under Regulation 2016/679”, 4 May 2020 (Version 1.1.), pp.1-12, para. 67

required in specific contexts of data collection where highly sensitive data is at stake. The term “explicit” refers not only to the data category, but also to the way the data subject expresses his/her will. The most straightforward way to achieve an undoubted expression of consent is to obtain a written and signed declaration<sup>34</sup>. In theory, “explicit” consent might be obtained by other means such as oral statements, electronic forms or by telephone. However, forms of providing consent, which do not leave lasting proof of the data subject’s wishes, such as any oral expression of consent, risk falling short in terms of *explicitness*<sup>35</sup>.

That being said, those cases where explicit consent is required are mentioned in Art. 9 (2)(a) for special categories of data, Art. 22 (1)(c) for decisions based solely on automated processing, including profiling, and in Art. 49 for data transfers lacking appropriate safeguards.

After having laid down briefly the elements and types of valid consent as designated by the current European data protection regulation, in the following section we focus on consent as a lawful ground for automated decision-making (Art. 22).

### 3.3. Consent for automated decision-making. Art. 22, GDPR

According to the GDPR digital services users have the right not be an object of a decision based exclusively on automated data processing, when it supposes a significant impact and/or produces legal effect on them<sup>36</sup>, unless applies one of the provisions in the Paragraph 2 of the same Article 22<sup>37</sup>. Following the WP29<sup>38</sup> interpretation, the Art. 22 establishes rather a prohibition, than a separate right<sup>39</sup>. For the sake of this paper, we will focus exclusively on the provision of Art. 22 (2)(c) of the GDPR, concerning explicit consent as a lawful ground for automated decision-making.

#### 3.3.1. “Solely on automated processing”

Art. 22(1) refers to a decision where there is no human intervention in the decision process. At first glance, this text suggests that, if *any* human intervention is

<sup>34</sup> EDPB, “Guidelines 05/2020 on consent under Regulation 2016/679”, 4 May 2020 (Version 1.1.), pp.1-12, para. 93

<sup>35</sup> EDPB, “Guidelines 05/2020 on consent under Regulation 2016/679”, 4 May 2020 (Version 1.1.), pp.1-12, para. 94; and WP29 “Opinion 15/2011 on the definition of consent”, 13 July 2011, pp. 1-38, p. 25

<sup>36</sup> Art.22 (1) and Recital 71

<sup>37</sup> Art. 22 (2)(a) automated processing “is necessary for entering into, or performance of, a contract”

(b) “authorized by Union or Member State law”

(c) “based on the data subject’s explicit consent”

<sup>38</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37

<sup>39</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37, p. 20

ensured, then the decision involving AI does not qualify as one “based solely on automated data processing”. The Guidelines on Automated individual decision-making are very instructive, because their authors describe the minimum threshold for the human element in the automated decision-making. Thus, to qualify as such, this involvement must be “meaningful”, and not merely a formal one. Moreover, someone empowered to influence the decision-making process should oversight the data processing<sup>40</sup>.

Nevertheless, the same Article 22 and Recital 71 of the GDPR do not provide an answer to the question of *when* and *where* this human intervention should happen and to what extent. Current technological development allows plenty of techniques and layers of human intervention, which could happen in different stages of the algorithmic decision-making<sup>41</sup>, making this disposition easily surmountable in practice. We discuss those challenges in detail in part IV. of this paper.

### 3.3.2. “Legal” effects or similar

The GDPR contains no description of the “legal” effects, nor the consequences that “similarly significantly” affect the data subject. The authors of the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 interpret the requirement for a “legal” effect as a measure of the impact of the decision on someone’s legally recognized civil and political rights<sup>42</sup>.

A decision-making process may not affect a data subject’s legal rights, but may equally affect him/her in a comparable manner. In the words of the authors of the Guidelines, “the threshold for significance must be similar to that of a decision producing a legal effect.”<sup>43</sup> This means that “significantly” important consequence for someone would translate into a long-term and serious negative impact on individual’s preferences related to his/her participation in society<sup>44</sup>.

Until here, we have briefly explored the requisites for consent when no human intervention could be ensured in an automated data processing. In the next section we explore the safeguards data controllers have to implement in order to ensure data subjects rights. We focus on the human role and explainability

<sup>40</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), p. 21

<sup>41</sup> Adadi A., Berrada M., 2018, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), *IEEE Access*, vol. 6.

<sup>42</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37, p. 21

<sup>43</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37, p. 21

<sup>44</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37, p. 21-22



challenges as pivotal for a transparent, and ultimately, democratic automated data processing.

### 3.4. Information as transparency measure

The requirement for additional information to be provided, when processing personal data by automated means such as AI, implies a much higher level of transparency of the decision-making process. In Art. 12 (1) we find the form in which the information to be provided pursuant Arts. 13 and 14 should take. Data controllers should tailor their consent “in a concise, transparent, intelligible and easily accessible form, using clear and plain language”.<sup>45</sup> In the light of the transparency principle in Art. 5(1)(a), data controllers should communicate the information in question in a way it does not overcharge users with complex technical information, and in a fashion that is clearly distinguishable from other parts of the privacy notice.<sup>46</sup> In addition, this information should be effortlessly accessible for the users.<sup>47</sup>

Thus, data controllers have to ensure their consent notices comply first with the general requirements for informed consent in Arts 12, 13, and 14, and in case of automated data processing with additional ones contained in Arts. 13(2)(f), and 14(2)(g) in terms of information to be provided to the data subject.

Pursuant to Arts. 13 (2)(f), 14 (2)(g) and 15 (1)(h) data controllers have to inform data subjects, whose data is about to be collected for the purposes of Art. 22(1) and (4), about “the existence of automated decision-making, including profiling” and provide “meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.” Those requisites constitute the data protection transparency and accountability architecture conceived by the legislator. This is why unsurprisingly the WP29 have chosen to designate commonly those Articles as a “right to be informed”<sup>48</sup>.

As far as the meaningfulness of the information related to the logic involved in the automated data processing provided to the user, data controllers should aim to provide an easy to understand, but comprehensive, explanation of the algorithm applied. Also, the user should be delivered a tentative list of expected results and the impact thereof.

---

<sup>45</sup> Art. 12 (1)

<sup>46</sup> WP29, “Guidelines on transparency under Regulation 2016/679”, 29 November 2017, (revised and adopted on 11 April 2018), pp. 1-40, para. 7

<sup>47</sup> WP29, “Guidelines on transparency under Regulation 2016/679”, 29 November 2017, (revised and adopted on 11 April 2018), pp. 1-40, para. 7

<sup>48</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37, p. 16



## IV. CHALLENGES

Having outlined the history, and the current consent mechanism within the EU data protection architecture, in this part, we highlight the challenges, which may undermine its validity, application and functioning. For the purposes of this paper, we focus on the information problem by identifying three challenges for an “informed” consent.

### 4.1. Human intervention as the Schrödinger’s cat

The first challenge we identify is contained in the Art 22(1), which establishes a general prohibition for users to be subjected to “a decision based solely on automated processing”. This is problematic because it suggests that, if *any* human intervention is ensured, then the algorithmic decision would not qualify as “solely based” on automated processing, and Art. 22 would not apply, together with its safeguards.

Article 22 and Recital 71 of the GDPR do not provide an answer to the question of *when* and *where* human intervention should happen and to what extent. Given the variety of techniques and layers of possible human involvement in the process, the lack of clear milestones of human participation blurs the difference between a completely algorithm-based system and one supervised by a human.

As pointed out in the section dedicated to consent for automated processing (3.3.), the WP29 Guidelines<sup>49</sup> define human involvement as an active participation through an “actual” and “meaningful” influence on the data management process. This definition is no less abstract than the one contained in the text of the Regulation. However, based on the general wording of the GDPR and the intended meaning of the Guidelines, we should understand human involvement as an active participation in the process, defined by precise steps, performed by an individual with the authority to introduce changes, and take decisions about the data processing and its product.

Human intervention could happen in the beginning of the data collection, when data is being recorded, or during the multiple and complex stages of data processing. Human participation could also take place in the moment of assembling the data in a form of a “result”, product of multiple overlapping factors, or in the final part, when the “result” is provided and a decision upon the same is made. Despite this uncertainty, we admit that indicating clearly on which stage of processing human intervention should occur, may be reasonable in some cases, but nonsensical in others. Thus, we suppose that the EU data protection legislation is silent on those questions due to the diversity of algorithmic processing techniques currently available, which allow human participation in every step of the data management.

Nevertheless, we consider it reasonable that human involvement should occur in the final stages of automated data processing for three main reasons. First,

<sup>49</sup> WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37

automated processes are applied in order to spare burdensome, routine and tedious initial work such as manual data collection, selection and classification. This stage is time-consuming and requires little cognitive power, creativity and empathy. Second, the algorithms are designed as a technology capable of establishing inferences and correlations based on huge amounts of data, and seemingly unrelated factors, which often are impossible for humans to perform, process and understand. Third, the most important and “significant” part happens at the final stage of the data processing. The result provided by the algorithm determines the decision to be made afterwards, which may entail potentially important negative consequences for the user such as a loan denial or a job application rejection<sup>50</sup>.

This is why external involvement should ensure that human considerations of the context of the situation are included. AI draws on historical data about the factors and the way decisions were made in the past. Thus, empathy, creativity, awareness of the particular social code and situation as well as the ability to spot possible technical errors and biases are essential for the data processing accountability and the fairness of the decision-making.

#### 4.2. We don't understand it

The second challenge relates to the exception of the prohibition of decision-making based uniquely on automated data processing. Informed consent is one of the grounds contained in Paragraph 2 of the Art. 22 on which an exception of this rule may be applied.

Data subjects should be informed beforehand that their data is used in an automated decision-making process according to Arts. 13 (2)(f), 14 (2)(g) as well as about the possibility to withdraw their consent pursuant to Art. 7 (3). As discussed above, users also have to receive information about the “logic involved”, and “the envisaged consequences of such processing”<sup>51</sup>. The so-called “right to be informed”<sup>52</sup>, contained in Arts. 13-15 implies multiple challenges both for data controllers and for users. Providing an understandable information for the purposes, functioning and outcomes expected of an algorithmic data processing is often a fiction.

This is so, first, because in some cases it is very difficult to describe the purposes of the collection. Data might be collected for one reason, but later may result useful for different, previously unspecified, reasons<sup>53</sup>, which may contradict the initial purposes, and potentially clash with the principles in Art 5 of the GDPR for

---

<sup>50</sup> Recital 71 GDPR

<sup>51</sup> Arts. 13 (2)(f), 14 (2)(g), 15 (h)

<sup>52</sup> In words of the WP29 in, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37

<sup>53</sup> Rhoen M., Yi Feng Q., 2018, Why the ‘Computer says no’: illustrating big data’s discrimination risk through complex systems science, *International Data Privacy Law*, Volume 8, Issue 2, pp. 140–159

“purpose limitation” (Art. 5(1)(b)), “data minimization” (Art. 5(1)(c))<sup>54</sup>, and “accountability” (Art. 5 (2)).

Secondly, AI frequently reaches its decisions using huge amounts of data, complex layered procedures (deep learning, for example) and/or associates data in ways humans cannot understand, nor explain. This problematics is known as the “black box”<sup>55</sup> problem and is already being studied in emerging disciplines such as XAI<sup>56</sup>. In other words, a software developer may be able to design, create and successfully launch an AI, but this does not imply an understanding of what data determined the result, nor the specific process behind it. In order to limit this problem, the EU legislator has introduced a “right to access” the information about the way users’ data is processed by an algorithm, which includes a “meaningful information about the logic involved” (Art. 15 (h)).

There has been an academic debate whether this disposition establishes a “right to an explanation”<sup>57</sup>. This “right” is supposed to provide an “explanation” of the algorithmic decision-making upon the data subject’s request. We are certain, however, that the GDPR dispositions, at least to a certain extent, entail a requirement for an “explainable” algorithm.

Thus, regarding the question of the information about the outcomes of the decision-making, some authors<sup>58</sup> have concluded that the GDPR contains, *de facto*, a “right to explanation” derived from the legally imperative safeguards foreseen (Art. 22, para. 3), the notification duties (Arts. 13-14 ) and the right to access (Art. 15) in combination with the non-binding Recital 71. Such a right may refer to two kinds of explanations, one about the general architecture of the algorithm and the other about the logic involved in the specific decision in question<sup>59</sup>.

<sup>54</sup> Zarsky, T, 2017, Incompatible: The GDPR in the Age of Big Data, *Seton Hall Law Review*, Vol. 47, No. 4(2), pp. 995-1020

<sup>55</sup> High-Level Expert Group on Artificial Intelligence, 2019, “A definition of AI: Main capabilities and scientific disciplines”, EC, pp. 1-9

<sup>56</sup> Adadi A., Berrada M., 2018, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), *IEEE Access*, vol. 6.

<sup>57</sup> Wachter, S., Mittelstadt, & B. Floridi, L., 2017, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 2, pp. 76-99; Kaminski Margot E., 2019, The Right to Explanation, Explained, *Berkeley Technology Law Journal*, Vol. 34, No. 1, pp. 189-218; Edwards Lilian and Veale Michael, 2018, Enslaving the Algorithm: From a ‘Right to an Explanation’ to a ‘Right to Better Decisions’? Vol. 16, No. 3, *IEEE Security & Privacy*, pp. 46-54; Edwards Lilian and Veale Michael, 2017, Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking For, Vol. 16, No.1, *Duke Law & Technology Review*, 2017, pp. 18-84

<sup>58</sup> Goodman Bryce and Flaxman Seth, 2017, European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”, *AI Magazine*, Vol. 38 No. 3, pp. 50-57

<sup>59</sup> Wachter, S., Mittelstadt, & B. Floridi, L., 2017, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 2, pp. 76-99

There are other authors who dismiss the connection between the binding and non-binding provisions of the GDPR, and sustain that individuals should receive only “meaningful” information, but limited *accordingly*.<sup>60</sup> Wachter et al. (2017) point out to the possible negative consequences for IP protected rights, if an explanation of the functioning and architecture of the algorithm were included. According to the same authors, individuals should be entitled to receive an explanation of the “individual circumstances of a specific automated decision”<sup>61</sup>. For that reason they propose a “right to reasonable inferences” related only to the specific individual results of the automated decision-making. Other scholars, interpreting the Regulation, advocate for the introduction of a “legibility test”, which would ensure “the capability of individuals to autonomously understand data and analytics algorithms, with a concrete comprehension of methods and data used”.<sup>62</sup>

#### 4.3. All that glitters is not gold

Certain level of understanding of the algorithm functioning is necessary for a transparent and fair data processing; two concepts, which impregnate the Regulation text.<sup>63</sup> Despite that, we should consider some of the externalities originated by the transparency commitment in the informed consent.

Firstly, the debate around the existence of a “right to an explanation” and its elements relates to the larger ethical debate about the principles on which EU data protection should be founded.<sup>64</sup> We consider the transparency, fairness and accountability principles, listed in Art. 5 of the GDPR, most closely related to the consent information problem.

Consent notice would be potentially a powerful tool to enhance transparency in automated data collection, processing and decisions by including an “explanation” thereof. A system is deemed accountable, if it is transparent, and if it is transparent, it is fair.<sup>65</sup> This logical chain is easily refutable because something fair is not necessarily transparent, neither does transparency mean fairness in judgement. Furthermore, the principle of accountability serves primarily legal notions such as responsibility and liability as long as they can be applied to

<sup>60</sup> Wachter, S., Mittelstadt, & B. Floridi, L., 2017, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 2, pp. 76-99

<sup>61</sup> Wachter, S., Mittelstadt, & B. Floridi, L., 2017, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 2, pp. 76-99

<sup>62</sup> Malgieri, G. and Comandé, G., 2017, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 4, pp. 243–265

<sup>63</sup> Art. 5 (1)(a), Art. 13 (2), Art. 14 (2), Art. 40 (2)(a)

<sup>64</sup> High-Level Expert Group on Artificial Intelligence, 8 April 2019, “Ethics Guidelines for Trustworthy AI”, EC, pp. 1-41

<sup>65</sup> Kaminski Margot E., 2019, The Right to Explanation, Explained, *Berkeley Technology Law Journal*, Vol. 34, No. 1, pp. 189-218

machines. Selbst and Barocas (2018) summarize public opinion in favour of a more transparent algorithms as a “visceral” fear to an environment where no human control over the outcome and no participation in the process thereof is guaranteed.<sup>66</sup> The authors build on this notion by incorporating the concept of “procedural justice”<sup>67</sup> as defined by Tom Tyler. This concept sheds light on the question why people are so concerned about the processes their data take part in. If procedural justice criterion is satisfied, the outcome in the proceeding may be considered more bearable, even though below optimum results are achieved.<sup>68</sup> In this way, voluntary compliance with the law is ensured.<sup>69</sup>

The danger of this rationale consists in the so-called “transparency fallacy”<sup>70</sup> which relates to the misconception and illusion plain users have about their own ability to understand explanations, or any information about the algorithm provided in the consent form. From a behavioural perspective the fact that users are asked for their consent, enhances their perception of security, empowerment, and certainty. Thus, the effective control users exercise over the processing procedure is, if not an illusionary, then, at least, manipulated.

Secondly, we should not turn a blind eye on the negative economic effects<sup>71</sup> too much transparency may have, leading to competitive loss<sup>72</sup>, strategic decision-making<sup>73</sup>, and finally to worst overall economic and social equilibria. A paradigmatic example thereof in the light of the problematics discussed is the challenge transparency poses on other legal branches and rights such as Intellectual property (IP), especially, trade secrets.<sup>74</sup>

---

<sup>66</sup> Selbst Andrew D. and Barocas Solon, 2018, The Intuitive Appeal of Explainable Machines, Vol. 87, *Fordham Law Review*, pp. 1085-1139

<sup>67</sup> Selbst and Barocas (2018) refer to the following article: Tyler Tom R., 1988, What Is Procedural Justice?: Criteria Used by Citizens to Assess the Fairness of Legal Procedures. Vol.22, no. 1, *Law & Society Review*, pp. 103-135.

<sup>68</sup> Selbst Andrew D. and Barocas Solon, 2018, The Intuitive Appeal of Explainable Machines, Vol. 87, *Fordham Law Review*, pp. 1085-1139

<sup>69</sup> Selbst Andrew D. and Barocas Solon, 2018, The Intuitive Appeal of Explainable Machines, Vol. 87, *Fordham Law Review*, pp. 1085-1139

<sup>70</sup> Edwards Lilian and Veale Michael, 2018, Enslaving the Algorithm: From a ‘Right to an Explanation’ to a ‘Right to Better Decisions’? Vol. 16, No. 3, *IEEE Security & Privacy*, pp. 46-54.

<sup>71</sup> Burt A., 2019, The AI Transparency Paradox, *Harvard Business Review*, <https://hbr.org/2019/12/the-ai-transparency-paradox>, last accessed 10.08.2022

<sup>72</sup> Burt A., 2019, The AI Transparency Paradox, *Harvard Business Review*, <https://hbr.org/2019/12/the-ai-transparency-paradox>, last accessed 10.08.2022

<sup>73</sup> Newell, S. and Marabelli, M., 2015, Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of 'Datification', *Journal of Strategic Information Systems*, *Forthcoming*

<sup>74</sup> Banisar D., 2011, The Right to Information and Privacy: Balancing Rights and Managing Conflicts. *World Bank Institute governance working paper series*; World Bank, Washington, DC. World Bank, pp. 1-56; Malgieri G., 2016, Trade Secrets v Personal Data: A Possible Solution for Balancing Rights, *International Data Privacy Law*, Vol. 6, No. 2, pp. 102– 116

Recital 63 expressly mentions IP rights and trade secrets when referring to the “right of access”, which “should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property”. The text of the Recital responds to a certain founded preoccupation of the legislator that, if data controllers disclose information about the way their algorithms function, they may end up revealing highly valuable economic information. Algorithmic inferences or specific procedures applied in the data processing such as trade secrets are part of data controller’s businesses assets. Investors would suffer significant losses, if forced to disclose specific information on the algorithm architecture, leading to reduced economic advantage and widened competitive gap. In relation to the point of connection between data protection and IP law, the analysis of some authors indicates that, although EU legislation intends to establish a balance between competing rights, slight preference towards data protection rights should be admitted.<sup>75</sup>

## V. CONCLUSION

Near the climax of the movie, Dr. Ouelet receives the order to kill Major Mira Killian. The moment Major Kilian learns about it, it is already too late, because she rests immobilized on the operation chair. She knows she has to give consent every time her AI is accessed, and as a last resort, she expressly states she does not give consent for that procedure. However, Dr. Ouelet reveals she never needed it.

Although one might not be a fan of the cyberpunk cinematographic genre, we consider that movie an illustrative extrapolation of the negative effects of an ineffective and formal consent mechanism, which while extracts data, degrades the consenting party’s dignity and autonomy. We can consider this practice a form of a digital exploitation. In this paper, we advocate for a prevention and clearer data protection rules on an EU level in order to pre-empt living in Major Kilian’s reality.

We consider the GDPR a pivotal instrument for European citizens’ privacy and data protection rights in a world where data is the new gold, and technology giants compete to get a grasp on it. In this paper, we have described the legal framework for a valid informed consent, together with the challenges it poses, and we believe that European data protection legislation needs to oil its gears and reform in order to continue serving as the legal shield Europeans deserve. With the policy recommendations made here, we aim to contribute to that objective.

---

<sup>75</sup> Malgieri, G. and Comandé, G., 2017, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 4, pp. 243–265



## VI. POLICY RECOMMENDATIONS

Based on the legal framework and challenges discussed above, we can propose the following policy recommendations, which may serve as an inspiration for the bases of future European legislation as well as for further discussions, and analysis on the matter.

- *Clarify the role of human intervention in an automated decision-making processing. Art. 22 (1)*

Future improvement of EU data protection legislation should include an answer to the question *when* and *where* human intervention should occur along the automated processing as well as the magnitude thereof. This is essential in order to mitigate possible negative impact on data subjects such as discrimination and technical errors through active human participation throughout the stages of data processing. As discussed in the part dedicated to the challenges, we consider human intervention should primarily be focused at the final stages of the automated processing, when the final *decision* is delivered. In this way, we prevent dehumanizing data processing, while ensuring users' digital rights on the premise of human dignity and autonomy as necessary elements for a non-discriminatory and democratic digital society.

- *Clarify whether data subjects have a right to an explanation of the algorithmic processing, and what information it should contain. Art. 15 (h)*

Further development towards a more sophisticated EU data protection regime needs to count with a more detailed text on the information data subject should expect prior to consenting, and in case they exercise their *right to be informed* (Art. 15). EU legislators should take a stance on the question whether users are entitled to an *explanation* of the functioning of the algorithm as a system, or they should expect information only on the specificities of the decision concerning them. Both options entail important legal, ethical and economic considerations and consequences, which have potentially significant impact on the EU digital environment.

- *Provide common guidelines on the design of consent notices.*

Currently, there are no formal requirements for the design of consent notices. This translates into a diverse landscape, where digital service providers enjoy creative freedom on the wording, position and language used in the consent formatting. Thus, a common framework based on best practices and industry experience<sup>76</sup> may contribute to a more *informed* users. Unified guidelines would

---

<sup>76</sup> Utz Ch., Degeling M, Fahl S., Schaub F., and Holz Th., 2019, (Un)informed Consent: Studying GDPR Consent Notices in the Field. *In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association for Computing Machinery, New York, NY, USA, pp. 973–990



limit nudging practices such as highlighting the “Accept” button in the notice. Moreover, shared consent notice design would make it easier for users to navigate through complex and long privacy texts. It would strengthen data subjects’ participation in the data management, and contribute to the actual control on their personal data, and thus, human autonomy in the digital.

## BIBLIOGRAPHY

### ACADEMIC REFERENCES:

1. Adadi A., Berrada M., 2018, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), *IEEE Access*, vol. 6.
2. Banisar D., 2011, The Right to Information and Privacy: Balancing Rights and Managing Conflicts. *World Bank Institute governance working paper series*; World Bank, Washington, DC. World Bank, pp. 1-56;
3. Beauchamp, T. and Childress, J., 2019. *Principles of biomedical ethics*. 8th ed. New York, NY: Oxford University Press.
4. Dalla-Vorgia, P., 2001. Is consent in medicine a concept only of modern times? *Journal of Medical Ethics*, 27(1), 59–61
5. Eberle, E.J., 2012. Observations on the development of human dignity and personality in German constitutional law: An overview. *Liverpool Law Review*, 33(3), pp.201–233.
6. Edwards Lilian and Veale Michael, 2017, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, Vol. 16, No.1, *Duke Law & Technology Review*, 2017, pp. 18-84
7. Edwards Lilian and Veale Michael, 2018, Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'? Vol. 16, No. 3, *IEEE Security & Privacy*, pp. 46-54.
8. Floridi, L. & Cows, J., 2019. A unified framework of five principles for AI in society. *Harvard Data Science Review*. 1(1)
9. Floridi, L. et al., 2018. AI4People—an ethical framework for a good AI Society: Opportunities, Risks, principles, and recommendations. *Minds and Machines*, 28(4), pp.689–707.
10. Goodman Bryce and Flaxman Seth, 2017, European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”, *AI Magazine*, Vol. 38 No. 3, pp. 50-57
11. Kaminski Margot E., 2019, The Right to Explanation, Explained, *Berkeley Technology Law Journal*, Vol. 34, No. 1, pp. 189-218
12. Malgieri G., 2016, Trade Secrets v Personal Data: A Possible Solution for Balancing Rights, *International Data Privacy Law*, Vol. 6, No. 2, pp. 102– 116
13. Malgieri, G. and Comandé, G., 2017, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 4, pp. 243–265
14. Murillo de la Cueva, P.L. & Piñar Mañas, J.L., 2009. *El derecho a la autodeterminación informativa*, Madrid: Fundacion Coloquio Jurídico Europeo.
15. Newell, S. and Marabelli, M., 2015, Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal

- Effects of 'Datification', *Journal of Strategic Information Systems, Forthcoming*
16. Rhoen M., Yi Feng Q., 2018, Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science, *International Data Privacy Law*, Volume 8, Issue 2, pp. 140–159
  17. Selbst Andrew D. and Barocas Solon, 2018, The Intuitive Appeal of Explainable Machines, Vol. 87, *Fordham Law Review*, pp. 1085-1139
  18. Tyler Tom R., 1988, What Is Procedural Justice?: Criteria Used by Citizens to Assess the Fairness of Legal Procedures. Vol.22, no. 1, *Law & Society Review*, pp. 103-135.
  19. Utz Ch., Degeling M, Fahl S., Schaub F., and Holz Th., 2019, (Un)informed Consent: Studying GDPR Consent Notices in the Field. *In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association for Computing Machinery, New York, NY, USA, pp. 973–990
  20. van der Sloot, B., 2014. Do data protection rules protect the individual and should they? an assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, 4(4), pp.307–325.
  21. Wachter, S., Mittelstadt, & B. Floridi, L., 2017, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, No. 2, pp. 76-99
  22. Warren , S.D. & Brandeis, L.D., 1891. The right to privacy. *Harvard Law Review*, 4(5), pp.193–220.
  23. Zarsky, T, 2017, Incompatible: The GDPR in the Age of Big Data, *Seton Hall Law Review*, Vol. 47, No. 4(2), pp. 995-1020

#### NORMATIVE REFERENCES:

1. Charter of Fundamental Rights of the European Union, 2000, OJ C 364/1
2. Coucil of Europe, 1981, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention 108), ETS No. 108, Council of Europe.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 23 October 1995, OJ L 281/31, p. 1–20
4. EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679", 4 May 2020 (Version 1.1.), pp.1-12
5. European Commission, May 4, 2022, European Digital Rights and Principles. *Shaping Europe's Digital Future*, <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>, last accessed 12.08.2022

6. OECD, 2002, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris.
7. 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), 4 May 2016, OJ L 119/1, p. 1–88
8. WP29 “Opinion 15/2011 on the definition of consent”, 13 July 2011, pp. 1-38
9. WP29, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 3 October 2017, (revised on 6 February 2018), pp. 1-37
10. WP29, “Guidelines on transparency under Regulation 2016/679”, 29 November 2017, (revised and adopted on 11 April 2018), pp. 1-40
11. High-Level Expert Group on Artificial Intelligence, 2019, “A definition of AI: Main capabilities and scientific disciplines”, EC, pp. 1-9
12. High-Level Expert Group on Artificial Intelligence, 8 April 2019, “Ethics Guidelines for Trustworthy AI”, EC, pp. 1-41

#### JURISPRUDENCE:

1. Bundesverfassungsgericht (BVerfG). Urteil des Ersten Senats vom 15. Dezember 1983 (Judgement of the first senate of 15 December 1983) -1 BvR 209/83, Rn. 1-215 - ECLI:DE:BVerfG:1983:rs19831215.1bvr020983
2. Judgement of the Court of 1 October 2019, *Planet49*, C-673/17 ECLI:EU:C:2019:801
3. Judgement of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901