IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 17, 2021, accepted April 1, 2021, date of publication April 12, 2021, date of current version April 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3072782

AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach

MARIA MILOSSI, EUGENIA ALEXANDROPOULOU-EGYPTIADOU, AND KONSTANTINOS E. PSANNIS, (Member, IEEE)
Department of Applied Informatics, School of Information Sciences, University of Macedonia, 546 36 Thessaloniki, Greece
Corresponding author: Konstantinos E. Psannis (kpsannis@uom.edu.gr)

ABSTRACT Artificial Intelligence (AI) refers to systems designed by humans, interpreting the already collected data and deciding the best action to take, according to the pre-defined parameters, in order to achieve the given goal. Designing, trial and error while using AI, brought ethics to the center of the dialogue between tech giants, enterprises, academic institutions as well as policymakers. Ethical challenges in AI brought ethical AI framework in place in an attempt to regulate people's lives and interactions, used for the benefit of society, for the human rights' protection as well as for the respect of individual's privacy and autonomy. The paper aims to summarize and critically evaluate the basic principles for the use of AI, with emphasis to the General Data Protection Regulation's (GDPR) approach, concerning data subject's consent, data protection principles and data subject's rights in a context of 'privacy by design' architecture.

INDEX TERMS AI, privacy, data protection, ethics, GDPR.

I. INTRODUCTION

Artificial Intelligence is said to be a new form of ''smart agency'', which is already reshaping our lives, our interactions and our environments [1]. The term AI contains an explicit reference to the notion of intelligence,[1] however, since intelligence is a vague concept, AI researchers use mostly the notion of rationality, in order to explain the ability to choose the best action to take in order to achieve a certain goal, given certain criteria to be optimized and the available resources [2]. However, ensuring the best action in order to achieve a certain goal doesn't always mean that this will be done for ethical purposes. According to the European Commission's WHITE PAPER on Artificial Intelligence [3], as digital technology becomes an ever more central part of every aspect of people's lives, people should be able to trust it. Trustworthiness is a prerequisite for AI uptake, while it can be used wisely, by highlighting potentialities and by creating opportunities.

The ubiquitous artificial intelligence despite its promise of being helpful, raises numerous ethical issues. In the healthcare sector for instance, robots are taught to help workers lift patients, monitor their wellbeing, interconnect the patient with the health unit and his physician, inform the closest pharmacy and prescribe medication if necessary [4]. But what happens if an AI system recommends the wrong drug for a patient or fails to notice a tumor on a radiological scan? The extensive use of AI is currently implemented or planned to be in many national judicial systems. The involvement of AI can vary greatly according to the applications, such as advanced case-law search engines, online dispute resolution, assistance in drafting deeds, analysis (predictive, scales), categorization of contracts according to different criteria and detection of divergent or incompatible contractual clauses, ''chatbots'' to inform litigants or support them in their legal proceedings [5]. What happens when a biased predictive judicial tool causes a wrongful conviction?

In the field of agriculture and food chain, the implementation of AI is already used for optimization of irrigation and application of pesticides and herbicides [6]. The agricultural

[1] 'Artificial intelligence (AI) systems' are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems). [Refer, High-Level Expert Group on Artificial Intelligence, [2]]

The associate editor coordinating the review of this manuscript and approving it for publication was Anandakumar Haldorai.

tasks such as harvesting crops will be easier, at a higher volume and faster pace than human laborers, certainly by developing predictive analytics to track and predict various environmental impacts on crop yield such as weather changes. But what happens if algorithmic systems provide inaccurate data to farmers or give inaccurate recommendations that may lead to lost harvests, earnings and cause negative impacts on their business [7]?

The intelligent transportation systems (ITS) and the assistance of ubiquitous sensors installed in a smart city may, among others, prevent high accident rates, traffic congestion and air pollution from traffic and carbon emissions [8], however, the parallel use of facial-recognition cameras, the license plate readers, the mobile phone data and other technologies used to track people either on the roadways or public transportation raises privacy concerns. The use of autonomous cars may diminish car accidents but it is extremely difficult to answer the ethical question of how self-driving cars should be programmed to 'behave' [9].

Moreover, AI recruiting tool may be a phenomenal technological innovation, for a fast and accurate candidate choice, but the mining of his/her personal data due to the machine learning may lead to discrimination. Bots for scraping social media postings, linguistic analysis of candidates' writing samples, algorithms' analyzing tone of voice, emotional states, nonverbal behaviors are recruitment methods [10] for which the candidate has not been lawfully, fairly and transparently informed or has not necessarily previously given his/her consent, according to the General Data Protection Regulation 2016/679 (hereafter GDPR) [11].

Ethics guidelines for trustworthy AI according to the European Commission's High-level expert group on AI, are based on human-centric and trust worthy AI. From the texts of the EU Treaties and the Charter of Fundamental Rights [12] to the Oviedo Convention [13] and the GDPR, the respect for human dignity is of top priority. While the value of human being is non-negotiable, then we talk about the principle of autonomy (either on individuals' everyday life or especially concerning the use of technology in their lives), which means that individuals are free to make their own choices for their own lives. That is because, they have firstly been informed and then they have given their free consent[2] [14] from which they can withdraw or not.[3] Every human being possesses an ''intrinsic worth'', which cannot be diminished, compromised or repressed by others, even by technology. In this context, individuals must have the control of their own lives, enjoy autonomy and thus enjoy democracy, justice and equality in every field of their social interaction, like work, science and participation in democratic processes [15]. Being an active member of social life can undoubtedly offer possibilities of reinventing and redesigning society, using the algorithmic solutions of AI for common goals like medical research or climate change.

It is true that there is a critical need to closely examine how AI technologies are being used in society and to recognize the many harms and human rights violations that may be caused by them, especially where those AI technologies are used unlawfully or unethically. Principles can provide a useful starting point to develop more formal standards and regulation and can help to identify priority issues on which both research and policy should focus, examining the basic tensions on how taking a decision using the AI technology [16]. Agreeing that the use of data-driven algorithms, helps to improve the quality and the efficiency of services, predict accurately, offer personalized services and make people's lives more convenient, we also accept that all the above, can be efficiently managed only if human rights are not undermined. That means that data are being processed lawfully, fairly and in a transparent way in relation to the data subject, promoting his/her self-actualization.

II. THE BASIC PRINCIPLES FOR THE USE OF AI

Fundamental rights' reference was the inspiration for many public, private and civil organizations to produce an ethical framework for AI. The AI4People's project[4] after a deep research to the commonalities and noteworthy differences from the existing set of principles already proposed [17], has surveyed and subsumed five overarching principles. These include: i. beneficence (defined as 'do good'), ii. nonmaleficence (defined as 'do no harm'), iii. autonomy (defined as 'respect for self-determination and choice of individuals'), iv. justice (defined as 'fair and equitable treatment for all') and v. explicability. The application of the AI ethical principles follows a cohesive cyclic flow during the data processing.

While the AI approach is not maleficent, the data processing is done beneficently, permitting to the data subject deciding for him or her in the context of a transparent AI logic, thus ensuring the justice and vice versa.[5]

A. THE PRINCIPLE OF BENEFICENCE: "DO GOOD"

AI systems should be designed and developed to be human centric and serve people. A significant approach is to apply humancentric AI (HAI) in IoT systems, so that IoT systems cannot only learn from users but also provide easy-to-understand explanations about decisions or estimations [18].

Beneficent AI systems can contribute to wellbeing by seeking achievement of a fair, inclusive and peaceful society by

[2] 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's 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 [Refer GDPR article 4(11)].

[3] 'The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent [Refer GDPR article 7(3)].

[4] AI4People, an Atomium—EISMD initiative designed to lay the foundations for a ''Good AI Society'', [1]

[5] Figure 6

helping to increase citizen's mental autonomy, with equal distribution of economic, social and political opportunity. According to a Stanford Research on how AI might affect urban life in 2030 [19], we can see, that all the fields of everyday life can result to a better way of living. For example, monitoring personal health and robot-assisted surgery are hints of things to come if AI is developed in ways that gain the trust of doctors, nurses, patients and regulators. Thus, machine learning can predict the risk of early death due to chronic disease in a large middle-aged population [20], can shorten the behavioral diagnosis of autism [21], can develop tools to interpret and quantify lung images [22] or use the artificial Intelligence in suicide prevention and mental health (Canada Protocol) [23]. In this context, European Commission has already invested in the use of Artificial Intelligence to speed up the diagnosis of COVID-19 and improve the future treatment of patients [24].

It is noteworthy that investments in uplifting technologies like predictive models to prevent lead poisoning or improve food distributions could spread AI benefits to the underserved. Work should start immediately on how to help people adapt as the economy undergoes rapid changes as many existing jobs are lost and new ones are created. Moreover, many researchers claim that machine learning can also increase the level of education, both for the teachers and for the students [25]. With the use of AI, education can be available from everywhere [26], with the help of virtual teachers, at any time and personalized to the users' knowledge and interests. This type of education can encourage students from all over the world, living probably in special circumstances, to have access to a new model of education that uses interactive tutoring systems.

In the field of transportation, with the use of AI, autonomous cars, trucks and, possibly, aerial delivery vehicles may alter how we commute, work, shop and create new patterns of life and leisure in cities. The conjunction of content creation tools, social networks and AI will also lead to new ways to gather, organize and deliver media in engaging, personalized and interactive ways. Cameras, drones and software to analyze crime patterns should use AI in ways that reduce human bias and enhance safety without loss of human liberty or dignity, which is the basic priority for an ethical artificial intelligence.

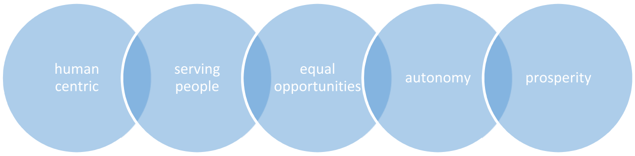


FIGURE 1. Illustration of a beneficent AI system.

B. THE PRINCIPLE OF NON MALEFICENCE: "DO NO HARM"

AI systems should be designed and developed not to undermine or harm people. Following the basic principle of privacy by design that GDPR introduced in its 25th article,[6] both at the time of the determination of the means for processing and at the time of the processing itself, appropriate technical and organizational measures have to be taken [27]. These measures are designed to implement data-protection principles, in an effective way and to integrate the necessary safeguards into the processing, in order to meet the requirements of the GDPR and protect the rights of data subject. In this context, AI systems should not be harmful for human beings, but protect the dignity, the integrity, the liberty, the privacy, the safety and the security of human beings in their social interaction. Yet the infringement of all the above, is not the only danger to be avoided in the adoption of AI. The emphasis should also be given to the misuse of AI.

In the field of health care and medicine for instance, a misuse or a malicious use of AI can lead to a fatal result to a patient's health. The machine may make a mistake; that is responsible for this? Treatment decisions may be designed depending on insurance status or the patient's ability to pay. Action is required to keep patients' data confidentiality, as well as to preserve the human approach from a doctor to a patient.

In the field of work, the use of AI can also be extremely harmful, in recruitment and promotion processes, in workplace monitoring and efficiency or productivity tests. Action is required to safeguard workers' interests and maintain a balance of human resource necessity. However, AI and its applications [28] are already displacing workers and it is expected that many more tasks done by humans today, will be done by AI and robots in the future; typical human resource tasks are being complemented or even substituted by AI.

Artificial intelligence has revolutionized information technology. To avoid harm in any field of social interaction, data collected and used for training of AI algorithms must be done in a way that avoids discrimination, manipulation or negative profiling, as it has already occurred with Amazon's recruiting engine which did not like women [29]. The Amazon resume scanning example is just one of many that show how the functional logics of a given technology echo the gender and racial dynamics of the industry that produced it [30], [31].

Of equal importance, AI systems should be developed and implemented in a way that protects societies from ideological polarization and algorithmic determinism. Thus, vulnerable demographics (e.g. children, minorities, disabled persons, elderly persons, immigrants) should receive greater attention to the prevention of harm, given their special status in society.

[6] 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'[Refer GDPR article 25(1)].

Inclusion and diversity are key ingredients for the prevention of harm to ensure suitability of these systems across cultures, genders, ages, life choices, etc., having a place in the design process (rather through testing, validating, or other) [32].

The algorithmic determinism spotlights also the challenge of the 'outcome-thinking' [33], that is the result of a work that counts and not the way that a professional (or not?) is driven to this result. While the outcome is a quick, cheap and reliable solution to a client's, a customer's or a patient's problem, then people will likely prefer machines than experts, on line medical prescription than a visit to a GP, disputes resolved via on line courts than in traditional courts by lawyers. Doctors support their patients, do a concrete human-centric diagnosis and treat them with empathy. No case is the same, while every medical treatment reflects patient's medical profile, as well as doctor's specific problem-solving skills. Even if the healthcare's improvement depends purely on digital technology, algorithms' interpretation remains still a human 'duty'. Human being cannot be treated as an experiment subject, taking for granted that healthcare is not a linear process.

Similarly, the purpose of the law is not to keep lawyers employed. A lawyer's duty to a client is to protect his/her interests with fairness and confidentiality, without conflict of interest, while concurrently ensuring the integrity of the justice system. The purpose that lawyers serve is to ensure that all members of society may exercise their legal rights and freedoms knowing that this exercise will be honored by all the other members of society and by society itself. Lawyers create positive social change for their clients by crafting structures that provide fair solutions to the problems that clients face or opportunities that clients wish to seize [34].

Besides its potentialities, AI can hardly replace doctors or lawyers for instance. A probable bad algorithms' use of client's or patient's personal data or algorithms' misinterpretation, could lead to ominous results for individuals' lives, certainly due to the question of the "ownership" of personal data. To realize this vision and to realize the potential of AI, especially across health systems, more fundamental issues have to be addressed: who owns health data, who is responsible for it, and who can use it? [35] Where healthcare organizations are the de-facto owners and guardians of patient data generated in the health system to share patient generated data back into the health system, there exists the need for secure, high-performance data infrastructure to make use of this data for AI applications, by creating, for example, a common data schema for storage and transfer of healthcare data. Even similar, is the case of lawyers' clients' data that are shareable in the justice system.

The principle of non-maleficence may also, according to Floridi et al,[7] may be viewed in terms of harm to the environment and animals, so the development of environmentally friendly AI may be considered part of the principle of avoiding harm. Environmental awareness will shape how we adapt to a changing world, how we preserve natural resources and the quality of life for future generations.

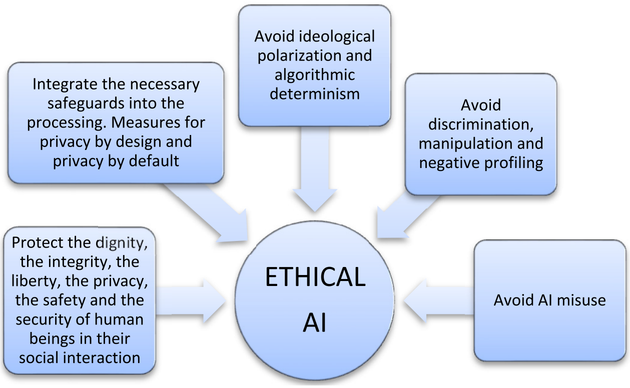

Integrate the necessary safeguards into the processing. Measures for privacy by design and privacy by default
Avoid ideological polarization and algorithmic determinism
Avoid discrimination, manipulation and negative profiling
Protect the dignity, the integrity, the liberty, the privacy, the safety and the security of human beings in their social interaction
ETHICAL AI
Avoid AI misuse

FIGURE 2. Illustration of a non maleficent AI system.

C. THE PRINCIPLE OF AUTONOMY: "PRESERVE HUMAN AGENCY"

In the context of AI development, autonomy means freedom from subordination to AI systems. Human beings interacting with AI systems have the right to decide for themselves, concerning the treatment they do, have the right not to receive a direct or indirect interaction with AI systems, the right to opt out and the right of withdrawal. Autonomy can be either helpful for a human being, when for example a disabled person uses smart glasses [36] or a smart car and harmful in the case of predictive policing methods, while not all machine learning algorithms are equally effective in crime prediction [37].

Human intervention is present in the use of algorithms, through the parameterization of the algorithm, the choice and the weighting of criteria as well as the categories of data that are taken into account in order to arrive at the desired result [38]. For example, if the user does not intervene directly in the recommendation of a restaurant through an algorithmic platform, the platform's developer role is fundamental, as he/she determines the importance of the location of a restaurant, its rating by other users or its concordance assumed (again according to criteria to be defined) with the profile of the petitioner.

The application of 'autonomous' software includes bots. Trade, finance and stock markets are largely run by algorithms and software. Without human intervention and control from outside, smart systems today conduct dialogues with customers in online call-centers; speech recognition interfaces and recommender systems of online platforms, e.g. Siri, Alexa and Cortana, make suggestions to users. Beyond the straightforward questions of data protection and privacy, the question arises whether people have the right to know whether they are dealing with a human being or with an AI artifact or whether there should be limits to what AI systems can suggest to a person, based on a construction concerning the person's own conception of their identity [39]. That is because of the fact that besides the accuracy and fairness of the automated assessments, problems of pervasive

[7] See citation [1]

surveillance, persistent evaluation, insistent influence and possible manipulation may occur.

According to the Ethics Guidelines, self-determination in many cases requires assistance from government or non-governmental organizations to ensure that individuals or minorities are afforded similar opportunities and systems should be in place to ensure responsibility and accountability. To gain the potential benefit of autonomous intelligent systems, their design and development need to be aligned with fundamental values and ethical principles.

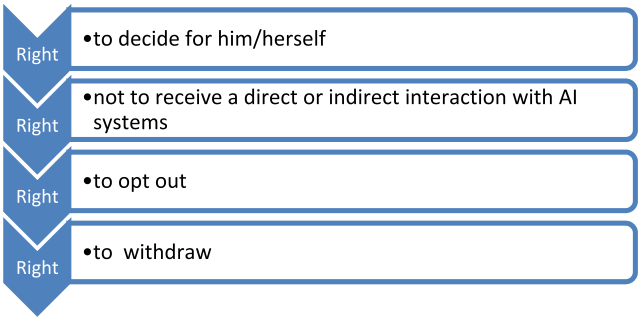

Right
•to decide for him/herself
Right
•not to receive a direct or indirect interaction with AI systems
Right
•to opt out
Right
•to withdraw

FIGURE 3. Data subject's right to autonomy.

D. THE PRINCIPLE OF JUSTICE: "BE FAIR"

The principle of justice, according to the Ethics Guideline, imparts that the development, use and regulation of AI systems must be fair and ethical. Developers and implementers need to ensure that individuals and minority groups maintain freedom from bias, stigmatization and discrimination. Additionally, the positives and negatives resulting from AI should be evenly distributed, avoiding placing vulnerable demographics in a position of greater vulnerability and striving for equal opportunity in terms of access to health, education, work, goods, services and technology amongst human beings, without discrimination.

The political and economic factors, the commercial interests as well as the influence of medical practice norms, may determine the way healthcare, with the use of AI, is delivered. For example, an algorithm trained on mostly Caucasian patients is not expected to have the same accuracy when applied to minorities and such rigorous evaluation and re-calibration must continue after implementation to track and capture those patient demographics and practice patterns which inevitably change over time [40]. Decision support systems for credit loan applications were found to favor certain socio-demographic groups in a disproportional way. As a consequence, people living in certain areas, those with a specific ethnic background or women were less likely to obtain a loan from the bank [41]. Is it fair while the sample isn't accurate or representative?

According to the AI4People research, justice variously relates to using AI to correct past wrongs such as eliminating unfair discrimination, ensuring that the use of AI creates benefits that are shared (or at least shareable) and preventing from the creation of new harms, such as the undermining of existing social structures [42]. Algorithms for a fair and ethical AI have different objectives; aiming at measuring fairness, designing fair predictions or modeling fair decisions, methods that allows practitioners to statistically quantify the level of fairness in their information systems and to monitor the effectiveness of fair AI in decision support systems over time [43]. Thus, fair AI algorithms can be derived to be fair by design.

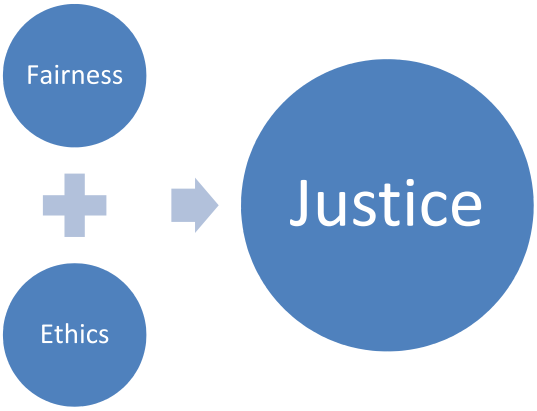


FIGURE 4. The principle of justice.

E. THE PRINCIPLE OF EXPLICABILITY: "OPERATE TRANSPARENTLY"

This principle is according to Floridi *et al.* 'the crucial missing piece of the jigsaw when we seek to apply the framework of bioethics to the ethics of AI'. The issue of transparency can come up at two points in time, when a data subject's information is inputted in an information system that includes AI algorithms (ex-ante transparency) or after the system's algorithmic model has been applied to the data subject to deliver specific outcomes concerning his or her (ex-post transparency) [44]. A central consideration of the principle of transparency outlined in the provisions of GDPR[8] is that the data subject should be able to determine in advance what the scope and the consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data have been used. In particular, for complex, technical or unexpected data processing, WP29's position is that controllers should separately spell out in unambiguous language what the most important consequences of the processing will be; in other words, what kinds of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? [45]. In accordance with the principle of accountability and in line

[8] 'transparency' means that the controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. [Refer GDPR article 12(1)].

with Recital 39,[9] data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data [46]. Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights [47]. The concept of transparency in the GDPR is user-centric rather than legalistic and is realized by way of specific practical requirements on data controllers and processors in a number of articles.

Furthermore, technological transparency implies that AI systems be auditable, comprehensible and intelligible by human beings at varying levels of comprehension and expertise. Business model transparency means that human beings are knowingly informed of the intention of developers and technology implementers of AI systems. According to the Ethics Guidelines, explicability is a precondition for achieving informed consent from individuals interacting with AI systems. In order to ensure that the principle of explicability and non-maleficence are achieved, the requirement of informed consent should be sought. Explicability requires accountability measures be put in place. Thus, individuals and groups may request evidence of the baseline parameters and instructions given as inputs for AI decision making (the discovery or prediction sought by an AI system or the factors involved in the discovery or prediction made) by the organizations and developers of an AI system, the technology implementers, or another party in the supply chain. Computer scientists for instance have focused on the technological possibility of providing interpretable data for interpretable models of opaque AI systems [48] and propose model explanation, model inspection and outcome explanation.

III. ARTIFICIAL INTELLIGENCE AND ETHICS: THE GDPR APPROACH

Algorithmic systems and artificial intelligence rely on the use of data, either personal or not, being processed to produce a result. The quality, the quantity and the relevance of data provided to these systems, can be in each case the ‘‘guide’’ to answer whether the AI use is legal and ethical, according to the aforementioned principles. Wrong data or out-of-date ones, can lead from an erroneous advertisement targeting to a false medical diagnosis. Ensuring the quality of incoming data in algorithmic and artificial intelligence systems is an issue that will become increasingly important.

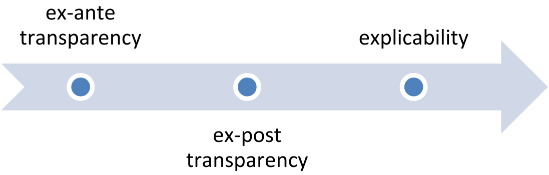


FIGURE 5. The principle of explicability.

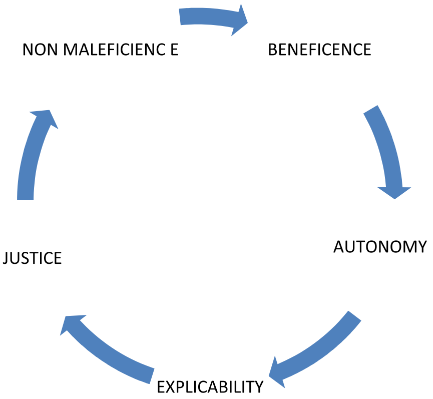


FIGURE 6. The cyclic flow of the AI ethical principles' application during the data processing.

The quantity of data available is similarly a detrimental factor to the quality of the results provided by algorithmic systems and artificial intelligence. While the technologies differ, both Big Data[10] and machine learning AI algorithms need a large amount of data to produce useful results. Thanks to AI, all kinds of personal data can be used to analyze, forecast and influence human behavior. In particular, AI enables automated decision-making even in domains that require complex choices, based on multiple factors and non-predefined criteria. The impact of the GDPR to the AI application in human interaction is decisive. Even if AI is not explicitly mentioned in the text of GDPR, many of its provisions are relevant to AI and some are indeed challenged by the new ways of processing personal data that are enabled by AI. Data subject's consent, data protection principles, data subject's rights and data's privacy by design and by default, according to the GDPR provisions may provide a 'preventive' approach to AI use. The question is whether the abovementioned legal and ethical framework fit AI technology.

[9] It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing [Refer GDPR recital 39].

[10] 'big data' refers to a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights [Refer GDPR recital 91].

TABLE 1. Legal bases for lawful processing.

consent for lawful data processing		***Article 7 GDPR***
PURPOSES	for one purpose	
	for more purposes	*in case of written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters*
CARACTERISTICS	freely given	
	informed	
	using clear and plain language	
RIGHT TO WITHDRAW	yes, at any time in the future	
other legal bases for lawful data processing		***Article 6 GDPR***
PURPOSES	the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	
	for compliance with a legal obligation to which the controller is subject	
	in order to protect the vital interests of the data subject or of another natural person	
	for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	
	for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child	
RIGHT TO WITHDRAW	no	

A. DATA SUBJECT'S CONSENT

According to the GDPR article 6, a valid legal basis for the processing of personal data in the context of AI application is needed. Data subject's consent plays a key role in the traditional understanding of data protection, based on the 'notice and consent' model, according to which data protection is aimed at protecting a right to 'informational self-determination.' This right is exercised by consenting or refusing to the processing of one's data, after having been given adequate notice. However this notice may be meaningless while the data subject has any knowledge at all or no choice concerning the processing (present or future) of his/her data. According to the Article 29 Working Party Guidelines on consent under Regulation 2016/679 [49], consent has to meet three criteria; The criterion of specificity of consent according to which further processing is permitted when it is covered by a legal basis and it is not incompatible with the purpose for which the data were collected, the criterion of granularity of consent, that means that consent to profiling must be separate from access to the service and the criterion of freedom of consent that means that consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller. In the case of data analytics and profiling when processing is AI-based, all the above prerequisites have to be followed.

B. DATA PROTECTION PRINCIPLES

Automated decision-making, profiling and related machine learning techniques pose new opportunities for discriminatory, biased or invasive decision-making processing. GDPR states specific data protection principles to prevent data from their illegal processing, affecting also AI systems [50]. The GDPR Article 5(1)(a) requires that personal data should be processed 'lawfully, fairly and in a transparent manner' in relation to the data subject. In the context of machine learning, transparency has two different concepts; the 'information fairness', which requires that data subjects are not deceived or misled concerning the processing of their data and raises specific issues in connection with AI and big data, because of the complexity of the processing involved in AI applications, the uncertainty of its outcome and the multiplicity of its purposes and the 'substantive fairness', which concerns the fairness of the content of an automated inference or decision, under a combination of criteria, which may be summarized by referring to the aforementioned standards of acceptability, relevance and reliability.

The GDPR article 5(1)(b)sets forth the principle of purpose limitation and the GDPR article 6, establishes a link between the purpose of processing operations and their legal basis. The reuse of the same data is permitted in case of compatibility with the purpose of the original collection, however, when the processing is AI based, the problem becomes complicated, while the data subject has any knowledge at all or has not given a priori his/her consent for future automated processing. The reuse of data should be considered as creation of new personal data, which should be subject to all applicable rules.

In the article 5(1)(c), GDPR states the principle of data minimisation, according to which personal data should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.' In the case of big data and data analytics by using AI and statistical methods, the problem that arises is whether a group of data subjects is affected or not. In fact, while using anonymisation and pseudonimisation techniques, statistical processing may not affect directly or at all an individual data subject however these methods can affect the collective interests of the data subjects who share the factors that are correlated to certain inferences.

The principle of accuracy which is stated in GDPR article 5(1)(d) requires data to be 'accurate and, where necessary kept up to date'. Inaccurate data may expose data subjects to harm, whenever they are considered and treated in ways that do not fit their identity.

The principle of storage limitation stated in GDPR article 5(1)(e), prohibits personal data's storing when they are no longer needed for the purposes of the processing. Within the AI context big data can be stored under appropriate security measures for archiving, research, or statistical purposes.

The principle of security stated in GDPR article 5(1)(f), ensures that data remain integral and confidential while they are processed in a manner that protects them from the unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. In the opposite case, AI surveillance methods used for rating, scoring, selecting or excluding people, may engage data subjects in experimentation, observing every behavior and linking them automatically with penalties or rewards. In such circumstances democracy is under discussion.

It is noteworthy that GDPR states a new data protection principle, also applied in AI, strengthening the controllers' obligations on the one hand and data-subjects' rights on the other hand. According to the principle of accountability (article 5(2)), the controller shall be responsible for, and be able to demonstrate compliance to all the above-mentioned data protection rules. The case of Cambridge Analytica used the data about test-takers as a training set for building a model to profile their friends and other people, correlating the information in people's Facebook pages to predictions about psychology and political preferences, proved that stakeholders, policy makers, tech giants and governments have to give answers to citizens who want to know how and why a certain algorithmic response has been given or a decision made.

TABLE 2. **Conditions for lawful processing (GDPR principles).**

GDPR Principles	
Article 5(1)(a)	transparency
Article 5(1)(b)	purpose limitation
Article 5(1)(c)	data minimisation
Article 5(1)(d)	accuracy
Article 5(1)(e)	storage limitation
Article 5(1)(f)	security
Article 5(2)	accountability

C. DATA SUBJECT'S RIGHTS

GDPR ensures data subject's protection, with a list of rights. In the context of AI based process the rights' content interpretation is often complicated. The right to access information about the processing of a person's data (article 15) contains the information of the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. However, according to the STOA,[11] it is not specified whether the obligation to provide information on the 'logic involved' only concerns providing general information on the methods adopted in the system or rather specific information on how these methods where applied to the data subject. The right to erasure stated in the GDPR article 17 that permits the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay may affect seriously the credibility of an algorithmic model. Similarly, the right to portability stated in the GDPR article 20 permitting the data subject to receive the personal data concerning him or her, which he or she has provided to a controller in a structured, commonly used and machine-readable format and to transfer the data to other controller, may affect the correctness as well as the confidentiality of an algorithmic model, while the portability of the applicant subject's data may affect the rest data set. The right to object stated in the GDPR article 21, enables data subjects to request and obtain that the processing of their data is terminated. This right guarantees the data minimization and protects importantly data subject from his/her data infringement. The GDPR article 22 specifies the right of objection and is most relevant to AI. The prohibition of automated decisions of the article 22 allows data subject not to be subject to a decision based solely on automated processing, including profiling, which produces 'legal effects' concerning him or her or similarly significantly affects him or her. However, data's protection may be misinterpreted as AI decisions use mainly but not necessarily automated methods. Moreover, the legal effects concerning the data subject or similarly significantly affects him or her, like performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements (GDPR recital 71), is a wide notion, not necessarily clear to the data subject. Probably for this reason, paragraph 2 of article 22 excepts the abovementioned prohibition on automated decision-making when the processing: a) is necessary for entering into, or performance of, a contract between the data subject and a data controller, b) is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or c) is based on the data subject's explicit consent.

[11] Scientific Foresight Unit [37]

TABLE 3. Data subject's rights.

Data subject's rights according to GDPR						
Right to access	Right to rectification	Right to erasure ('right to be forgotten')	Right to restriction of processing	Right to data portability	Right to object	Right not to be subject to an automated individual decision-making, including profiling
GDPR						
Article 15	Article 16	Article 17	Article 18	Article 20	Article 21	Article 22

The article 22(4) introduces a prohibition, limited by an exception, to ground automated decisions on special categories of personal data. According to the study concerning the impact of the GDPR on AI, the importance of AI based processing is that the so called "sensitive" data can be inferred from "non-sensitive" data. For instance, sex orientation ("sensitive" data) can be inferred from a data subject's linear activity, likes or even facial features ("non-sensitive" data). In this case, the inference of sensitive data should count as a processing of sensitive data and therefore would have to be considered unlawful unless the conditions under Article 9 are met. Similarly, "non-sensitive" data can work as proxies for "sensitive" data correlated to them, even though the latter are not inferred by the system. For instance, the place of residence can act as a proxy for ethnicity. In this case, an unlawful discrimination may take place.

D. AI AND PRIVACY BY DESIGN

Both in the data protection law and in the AI ethics, the focus is on the preventing of harm to individuals. Privacy by design and privacy by default mission is to empower data's confidentiality and strengthen systems' functionality in a secure lifecycle management of information. Security measures help to avoid privacy invasive events before they happen. According to Cavoukian [51], privacy must be embedded into technologies, operations, and information architectures in an holistic, integrative and creative way by re-inventing existing choices in case that the alternatives are unacceptable. Privacy by design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible and far more desirable, to have both. Privacy by design in practice is a real challenge for AI developers as they are asked to explain the logic of an AI solution which has to be compatible to fundamental rights and principles. However explicability is very relevant and depends often on the system's outcome, while different machine learning approaches vary in their ability to provide explanations, depending on the importance of the interests that are affected (e.g. health data, financial status, recruitment, etc).

TABLE 4. Top 10 rankings for government AI readiness 2020.

Rank	Country	Score
1	United States of America	85.479
2	United Kingdom	81.124
3	Finland	79.238
4	Germany	78.974
5	Sweden	78.772
6	Singapore	78.704
7	Republic of Korea	77.695
8	Denmark	75.618
9	Netherlands	75.297
10	Norway	74.430

Source: Oxford Insights, 2020

The ability of AI systems to make automated and self-learned decisions enlightens the need for transparency in the way that such systems reach decisions [52]. Machine learning algorithms have changed the way patterns are extracted from datasets and how predictions and decisions are made [53]. Automated decision making-systems affect individuals and society at large and provoke fundamental questions regarding the relation between humans and machines, the responsibility -for example- in case of an accident, a false diagnosis, a wrongful conviction, a denial of a loan demand, as well as the human dignity and the human autonomy.

Moreover, while designing an AI system a basic priority is to teach morality to machines. But are developers moral? Humans can't objectively convey morality in measurable metrics that make it easy for a computer to process. A machine cannot be taught what is fair unless the engineers designing the AI system have a precise conception of what fairness is. Ethical values and data collection on explicit ethical measures need to be formulated as quantifiable parameters in an AI system. It is truly difficult to define clearly ethical norms and even more difficult to train appropriately algorithms while there is no common rule for what makes a moral human, so it is complicated to design 'moral robots'. The lack of the value of forgiveness when children are exposed to AI mediated risk profiling practices used by Dutch government authorities is a very characteristic example of how morally designed a system could be. Children who are victims, witnesses or falsely accused, cannot be held responsible for their correlations to crime; they can feel unjustifiably punished, 'unforgiven' and hampered in their choices, develop low self-worth and negative judgmental attitudes towards others. Due to a lack of a special legal framework, a child can be unjustifiably stigmatized for the future. Incorporating the value of forgiveness into the personal data legal context by amending the right to erasure and set this ethical parameter in an AI system would not only benefit individual children but would also foster public safety as a result [54].

Automated decision making-systems have to be designed in respect to a transparent morality,that is in respect to the human dignity and the human autonomy. Otherwise, we may be placing ourselves in the dangerous situation of allowing algorithms to decide for us [55].

IV. CONCLUSION

AI ethics raise the problematic of broad surveillance, manipulation, lack of autonomy and lack of democracy. Whether machine learning leads to algorithmic determinism or self-determination is not a simple question to answer. A human centric AI may give explanations about decisions or estimations. It is clear that there are various approaches to ethics.[12] Robust ethical principles are essential in the future of the rapidly developing AI technology, but not all countries understand ethics in the same way [56]. The current frameworks address the major ethical concerns and make recommendations for governments to manage them, but notable gaps exist. A unifying legal framework for AI development, according to the European Commission's plan for 'ethics guidelines with a global perspective', could promote coordinated approach to maximize the benefits and address the challenges brought about by AI [57].

In the AI world, the real challenge is to reconcile the innovation with individual rights and social values, ensuring the adoption of data protection rules and principles that GDPR states and preventing from the undermining of autonomous rational choice. Governance is needed to align digitalization with democracy [58]. A fair and moral algorithmic treatment may promote the values of democracy, social equality, welfare and solidarity on condition that the data controller is able to give the explanations of the AI logic to the data subject. To achieve fairness and transparency in personal data processing and machine learning, data protection authorities have to discuss in depth both with the controllers and with the society, by interpreting very specifically AI legal demands in case of GDPR legal or technical insufficiency.

However morality and data protection principles alone cannot guarantee ethical AI [59]; an holistic approach to a responsible, transparent and trustworthy AI is needed, defining each time the scope to be achieved, estimating the impact on individuals and communities that may be affected and evaluating the reasonable risk assessment posed to individual wellbeing and public welfare, in order to formulate proportional procedures and protocols [60].

ACKNOWLEDGMENT

The research work was not funded. All websites were accessed on 1st March 2021.

REFERENCES

[1] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, and E. Vayena, "AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations," *Minds Mach.*, vol. 28, no. 4, pp. 689–707, Nov. 2018, doi: 10.1007/s11023-018-9482-5.

[2] European Commission. (Apr. 8, 2019). *A Definition of AI: Main Capabilities and Scientific Disciplines High-Level Expert Group on Artificial Intelligence*. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[3] European Commission, Brussels. (Feb. 2, 2020). *White Paper on Artificial Intelligence—A European Approach to Excellence and Trust*. [Online]. Available: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[4] M. Milossi, "The Internet of Things (IoT) in digital health: Data treatment and legal challenges," in *Proc. Int. Conf. Med., Law Internet*, Thessaloniki, Greece, May 2018, pp. 244–247.

[5] European Commission. (Dec. 2018). *European Commission for the Efficiency of Justice (CEPEJ) European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. [Online]. Available: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

[6] T. Talaviya, D. Shah, N. Patel, H. Yagnik, and M. Shah, "Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides," *Artif. Intell. Agricult.*, vol. 4, pp. 58–73, Apr. 2020, doi: 10.1016/j.aiia.2020.04.002

[7] R. Mark, "Ethics of using AI and big data in agriculture: The case of a large agriculture multinational," *ORBIT J.*, vol. 2, no. 2, pp. 1–27, 2019, doi: 10.29297/orbit.v2i2.109.

[8] H. Shin and J. Lee, "Temporal impulse of traffic accidents in South Korea," *IEEE Access*, vol. 8, pp. 38380–38390, 2020, doi: 10.1109/ACCESS.2020.2975529.

[9] N. Kallioinen, M. Pershina1, J. Zeiser, F. Nosrat Nezami, G. Pipa1, A. Stephan, and P. König, "Moral judgements on the actions of self-driving cars and human drivers in dilemma situations from different perspectives," *Frontiers Psychol.*, vol. 10, p. 2415, Nov. 2019, doi: 10.3389/fpsyg.2019.02415.

[10] B. Dattner, T. Chamorro-Premuzic, R. Buchband, and L. Schettler, "The legal and ethical implications of using AI in hiring," *Harvard Bus. Rev.*, Apr. 2019. [Online]. Available: https://hbr.org/2019/04/the-legal-and-ethical-implications-of-using-ai-in-hiring

[11] "Regulation (EU) 2016/679 of the European parliament and of the council of 27April 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)," *J. Eur. Union*, vol. 119, no. 1, pp. 1–88, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[12] *Charter of Fundamental Rights of the European Union, OJ C 326*, Standard 26.10.2012, European Union, 2012, pp. 391–407.

[13] *Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine*, Standard no. 164, Oviedo, 4.IV.1997, Convention on Human Rights and Biomedicine, European Treaty Series, 1997. [Online] Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/164

[14] E. Alexandropoulou-Egyptiadou, "Personal data," Nomiki Bibliothiki, Athens, Greece, Tech. Rep., 2016, pp. 69–72.

[15] C. McCrudden, "Human dignity and judicial interpretation of human rights," *European J. Int. Law*, vol. 19, no. 4, pp. 1–70, 2008. [Online]. Available: http://www.ejil.org/article.php?article=1658&issue=86

[16] J. Whittlestone, R. Nyrup, A. Alexandrova, and S. Cave, "The role and limits of principles in AI ethics: Towards a focus on tensions, Leverhulme centre for the future of intelligence," Assoc. Advancement Artif. Intell., Univ. Cambridge, 2019. [Online]. Available: https://www.aaai.org, doi: 10.1145/3306618.3314289.

[12] See the European Parliament detailed study concerning "the ethics of artificial intelligence: issues and initiatives" that deals with the ethical implications and moral questions that arise from the development and implementation of artificial intelligence (AI) technologies and reviews the guidelines and frameworks which countries and regions around the world have created to address them. It presents a comparison between the current main frameworks and the main ethical issues and highlights gaps [56]

[17] Future of Life Institute. *Asilomar AI Principles*. [Online]. Available: https://futureofife.org/ai-principles

[18] I. García-Magariño, R. Muttukrishnan, and J. Lloret, "Human-centric AI for trustworthy IoT systems with explainable multilayer perceptrons," *IEEE Access*, vol. 7, pp. 125562–125574, 2019, doi: 10.1109/ACCESS.2019.2937521.

[19] T. Abate. (Sep. 2016). *Stanford-Hosted Study Examines How AI Might Affect Urban Life in 2030*. [Online] Available: https://news.stanford.edu/2016/09/01/ai-might-affect-urban-life-2030/

[20] S. F. Weng, L. Vaz, N. Qureshi, and J. Kai, "Prediction of premature all-cause mortality: A prospective general population cohort study comparing machine-learning and standard epidemiological approaches," *PLoS ONE*, vol. 14, no. 3, 2019, Art. no. e0214365, doi: 10.1371/journal.pone.0214365.

[21] D. Wall, R. Dally, R. Luyster, J.-Y. Jung, and T. F. Deluca, "Use of artificial intelligence to shorten the behavioral diagnosis of autism," *PLoS ONE*, vol. 7, Aug. 2012, Art. no. e43855, doi: 10.1371/journal.pone.0043855.

[22] L. Mertz, "AI-driven COVID-19 tools to interpret, quantify lung images," *IEEE Pulse*, vol. 11, no. 4, pp. 2–7, Jul. 2020, doi: 10.1109/MPULS.2020.3008354.

[23] C.-M. Mörch, A. Gupta, and B. L. Mishara, "Canada protocol: An ethical checklist for the use of artificial intelligence in suicide prevention and mental health," *Artif. Intell. Med.*, vol. 108, Aug. 2020, Art. no. 101934, doi: 10.1016/j.artmed.2020.101934.

[24] Europen Commission. (May 2020). *Shaping Europe's Digital Future. Using AI to Fastnd Effectively Diagnose COVID-19 in Hospitals*. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/using-ai-fast-and-effectively-diagnose-covid-19-hospitals

[25] C. Stergiou, A. P. Plageras, K. E. Psannis, T. Xifilidis, G. Kokkonis, S. Kontogiannis, K. Tsarava, and A. Sapountzi, "Proposed high level architecture of a smart interconnected interactive classroom," in *Proc. South-Eastern Eur. Design Autom., Comput. Eng., Comput. Netw. Soc. Media Conf. (SEEDA_CECNSM)*, Kastoria, Greece, Sep. 2018, pp. 1–6, doi: 10.23919/SEEDA-CECNSM.2018.8544922.

[26] V. A. Memos, G. Minopoulos, C. Stergiou, K. E. Psannis, and Y. Ishibashi, "A revolutionary interactive smart classroom (RISC) with the use of emerging technologies," in *Proc. 2nd Int. Conf. Comput. Commun. Internet (ICCCI)*, Nagoya, Japan, Jun. 2020, pp. 174–178, doi: 10.1109/ICCCI49374.2020.9145987.

[27] (Nov. 2019). *European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Plenary meeting*. [Online]. Available: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

[28] Y. Zhang, S. Balochian, P. Agarwal, V. Bhatnagar, and O. Jaber Housheya, "Artificial intelligence and its applications," *Math. Problems Eng.*, vol. 2014, Apr. 2014, Art. no. 840491, doi: 10.1155/2014/840491.

[29] Reuters. (2018). *J.Dastin: Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*. [Online] Available: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[30] C. C. Perez, *Invisible Women: Data Bias in a World Designed for Men*. New York, NY, USA: Abrams Press, 2019, pp. 1–419.

[31] O. Keyes. (2019). *Counting the Countless*. [Online]. Available: https://ironholds.org/counting-writeup/

[32] S. M. West, M. Whittaker, and K. Crawford, "Discriminating systems: Gender, race and power in AI," AI Now Inst., New York, NY, USA, 2019. [Online]. Available: https://ainowinstitute.org/discriminatingsystems.pdf

[33] R. Susskind, "AI, work and 'outcome-thinking', artificial intelligence and the future of work," *Brit. Acad. Rev.*, no. 34, pp. 30–33, 2018. [Online]. Available: https://www.thebritishacademy.ac.uk/documents/970/BritishAcademyReview34-Autumn2018.pdf

[34] (2014). *Canadian Bar Association: Futures: Transforming the Delivery of Legal Services in Canada*. [Online]. Available: https://www.cba.org/CBAMediaLibrary/cba_na/PDFs/CBA%20Legal%20Futures%20PDFS/Futures-Final-eng.pdf

[35] T. Panch, H. Mattie, and L. A. Celi, "The 'inconvenient truth' about AI in healthcare," *NPJ Digit. Med.*, vol. 2, no. 1, pp. 1–3, Dec. 2019, doi: 10.1038/s41746-019-0155-4.

[36] M. Milossi, "The 'smart glasses' in the era of augmented reality: Protecting the personal data as 'the pupil of the eye,'" in *Proc. Int. Conf., New Technol. Health, Med., Legal Ethical Issues*, Thessaloniki, Greece, Nov. 2019, pp. 255–264.

[37] X. Zhang, L. Liu, L. Xiao, and J. Ji, "Comparison of machine learning algorithms for predicting crime hotspots," *IEEE Access*, vol. 8, pp. 181302–181310, 2020, doi: 10.1109/ACCESS.2020.3028420.

[38] CNIL. (2018). *SynthèSe Du DéBat Public Animé Par La Cnil Dans Le Cadre De La Mission De RéFlexion éThique Confiée Par La Loi Pour Une République NuméRiquecomment Permettre À L'Homme De Garder La Main Les Enjeux ÉThiques Des Algorithmes Et De L'Intelligence Artificielle*. [Online]. Available: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

[39] European Group on Ethics in Science and New Technologies (EGE). (2018). *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*. [Online] Available: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

[40] European Parliamentary Research Service, Scientific Foresight Unit (STOA). (Jun. 2020). *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

[41] M. P. E. Hardt and N. Srebro, "Equality of opportunity in supervised learning," in *Proc. 30th Int. Conf. Neural Inf. Process. Syst.*, Dec. 2016, pp. 3323–3331. [Online]. Available: https://dl.acm.org/doi/pdf/10.5555/3157382.3157469

[42] (Apr. 2018). *Article 29 Data Protection Working Party, Guidelines on Transparency Under Regulation 2016/679* [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[43] S. Feuerriegel, M. Dolata, and G. Schwabe, "Fair AI," *Bus. Inf. Syst. Eng.*, vol. 62, pp. 379–384, May 2020, doi: 10.1007/s12599-020-00650-3.

[44] Ad hoc Committee on Data Protection (CAHDATA), Strasbourg. (2018). *Explanatory Report of the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. [Online]. Available: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

[45] *Opinion of Advocate General Cruz Villalon, 9 July 2015 in the Bara case (Case C-201/14), Paragraph 74: The Requirement to Inform the Data Subjects About the Processing of Their Personal Data, Which Guarantees Transparency of All Processing, is all the More Important Since it Affects the Exercise by the Data Subjects of Their Right of Access to the Data Being Processed, Referred to in Article 12 of Directive 95/46, and Their Right to Object to the Processing of Those Data, Set Out in Article 14 of That Directive*. [Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CC0201&from=EN

[46] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, "A survey of methods for explaining black box models," *ACM Comput. Surv.*, vol. 51, no. 5, p. 93, 2018, doi: 10.1145/3236009.

[47] F. H. Cate, P. Cullen, and V. Mayer-Schönberger, "Data protection principles for the 21st century: Revising the 1980 OECD guidelines," Oxford Internet Inst., 2014, pp. 7–9. [Online]. Available: https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf

[48] L. Edwards and M. Veale, "Slave to the algorithm: Why a 'right to an explanation' is probably not the remedy you are looking for," *Duke Law Technol. Rev.*, vol. 16, p. 18, May 2017. [Online]. Available: https://ssrn.com/abstract=2972855, doi: 10.2139/ssrn.2972855.

[49] The Working Party on the Protection Of Individuals With Regard to the Processing of Personal Data. (2018). *Guidelines on Consent Under Regulation 2016/679, WP259 rev.01*. [Online] Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[50] *ARTICLE 29 DATA PROTECTION WORKING PARTY, Article 29 Working Party Guidelines on consent under Regulation 2016/679 17/EN WP259 Rev.01*. [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[51] A. Cavoukian, "Privacy by design the 7 foundational principles implementation and mapping of fair information practices," Inf. Privacy Commissioner Ontario, Toronto, ON, Canada, Jan. 2011. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

[52] H. Felzmann, E. Fosch-Villaronga, A. Tamò-Larrieux, and C. Lutz, "Towards transparency by design for artificial intelligence," *Sci. Eng. Ethics*, vol. 26, pp. 3333–3361, Nov. 2020, doi: 10.1007/s11948-020-00276-4.

[53] M. V. Otterlo, "A machine learning view on profiling," in *Privacy, Due Process and the Computational Turn: Philosophers of Law Meet Philosophers of Technology*, M. Hildebrandt and K. D. Vries, Eds. London, U.K.: Routledge, May 2013, pp. 41–64, doi: 10.4324/9780203427644.

[54] D. K. L. Fors, ''Legal remedies for a forgiving society: Children's rights, data protection rights and the value of forgiveness in AI-mediated risk profiling of children by Dutch authorities,'' *Comput. Law Secur. Rev.*, vol. 38, Sep. 2020, Art. no. 105430, doi: 10.1016/j.clsr.2020.105430.

[55] S. Polonski. (Dec. 2017). *Can We Teach Morality to Machines? Three Perspectives on Ethics for Artificial Intelligence*. [Online]. Available: https://medium.com/@drpolonski/can-we-teach-morality-to-machines-three-perspectives-on-ethics-for-artificial-intelligence-64fe479e25d3

[56] International Development Research Centre (IDRC). *Government AI Readiness Index 2020, Oxford Insights*. [Online]. Available: https://www.oxfordinsights.com/government-ai-readiness-index-2020

[57] EPRS. (Mar. 2020). *European Parliamentary Research Service Scientific Foresight Unit (STOA), The Ethics of Artificial Intelligence: Issues and Initiatives, Study Panel for the Future of Science and Technology, PE 634.452*. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

[58] D. Messner, ''Redefining and renewing humanism in the digital age [opinion],'' *IEEE Technol. Soc. Mag.*, vol. 39, no. 2, pp. 35–40, Jun. 2020, doi: 10.1109/MTS.2020.2991498.

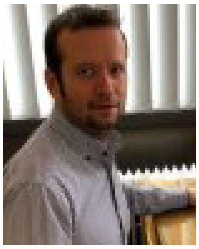
[59] B. Mittelstadt, ''Principles alone cannot guarantee ethical AI,'' *Nature Mach. Intell.*, vol. 1, pp. 501–507, Nov. 2019, doi: 10.1038/s42256-019-0114-4.

[60] D. Leslie, ''A guide for the responsible design and implementation of AI systems in the public sector,'' Alan Turing Inst., London, U.K., 2019, doi: 10.5281/zenodo.3240529.

MARIA MILOSSI was born in Thessaloniki, Greece. She received the degree from the Faculty of Law, School of Law, Economics and Political Sciences, Aristotle University of Thessaloniki, Greece, in 2003, the DESS/M2 degree in internet law from the Faculty of Law, School of Law, University of Paris 1–Panthéon, Sorbonne, France, in 2004, and the Ph.D. degree from the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece, in 2014. She is currently an independent Attorney at law with more than 16 years of court and deep legal experience. She is also an Adjunct Professor with the University of Macedonia, where she teaches Internet law and AI ethics to undergraduate and postgraduate students. She is also a member of the Bar of Thessaloniki (Supreme Court) and an Associate of the IT Law Team Research Group. Since 2010, she has been participating in legal conferences and seminars as a main or guest Speaker to talk as an Expert in IT law, constantly interested in the new challenges that the digital era brings to people's everyday life. Since November 2020, she has been a member of the Committee for Research Ethics of the University of Macedonia.

EUGENIA ALEXANDROPOULOU-EGYPTIADOU is currently the Vice Rector and the former Deputy Rector of the University of Macedonia, Thessaloniki, Greece. She is also a Professor of information technology law with the Department of Applied Informatics, the Founder of the IT Law Scientific Group, and the Director of the Postgraduate Program (Master) in ''Law and Informatics.'' As a former Attorney at law at the Greek Supreme Court, she headed the Legal Department of Egnatia Bank in Northern Greece. She was also a member of the editorial board of the Law Review ''Harmenopoulos,'' edited by the Bar of Thessaloniki. She has written and/or edited numerous scientific articles and books in the area of Civil, European, Banking, Labour, International, and IT Law.

Her research interests include personal data protection and legal environment of the information society. She has acted as an Organizer, the Chair Person, and a Speaker in several International and Pan-Hellenic Conferences on IT Law and Ethics, reviewed numerous articles and dissertations and participates in many Scientific Associations and Projects.



KONSTANTINOS E. PSANNIS (Member, IEEE) was born in Thessaloniki, Greece. He received the degree in physics from the Faculty of Sciences, Aristotle University of Thessaloniki, Greece, and the Ph.D. degree from the Department of Electronic and Computer Engineering, School of Engineering and Design, Brunel University, London, U.K. He is currently an Associate Professor of communications systems and networking with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece, the Director of the Mobility2net Research and Development and Consulting JP-EU Laboratory, and a member of the EU-JAPAN Centre for Industrial Cooperation. He has more than 60 publications in international scientific journals and more than 70 publications in international conferences. His published works has more than 3000 citations (H-index 25, i10-index 52). He supervises two postdoctoral students and eight Ph.D. students. His research interests include digital media communications, media coding/synchronization, and transport over a variety of networks, from the theoretical as well as the practical points of view. His recent work has been directed toward the demanding digital signals and systems problems arising from the various areas of ubiquitous big data/media and communications. This work was supported by research grants and contracts from various government organizations. He has participated in joint research works funded by Grant-in-Aid for Scientific Research, the Japan Society for the Promotion of Science (JSPS), the KAKENHI Grant, The Telecommunications Advancement Foundation, the International Information Science Foundation, as a Principal Investigator and a Visiting Consultant Professor with the Nagoya Institute of Technology, Japan. From 2001 to 2002, he was awarded the British Chevening Scholarship. The Chevening Scholarships are the U.K. Government's Global Scholarship Programme, funded by the Foreign and Commonwealth Office (FCO) and partner organizations. The programme makes awards to outstanding scholars with leadership potential from around the world to study at universities in U.K. He was invited to speak on the EU-Japan Co-ordinated Call Preparatory Meeting, Green and Content Centric Networking (CCN), organized by European Commission (EC) and the National Institute of Information and Communications Technology (NICT)/Ministry of Internal Affairs and Communications (MIC), Japan (in the context of the upcoming ICT Work Programme 2013), and International Telecommunication Union (ITU-founded in 1865), SG13 meeting on DAN/CCN, Berlin, in July 2012, amongst other invited speakers. He received the Joint-Research Award from the Institute of Electronics, Information and Communication Engineers, Japan, the Technical Committee on Communication Quality, in July 2009, and the Joint-Research Encouraging Prize from the IEICE Technical Committee on Communication Systems (CS), in July 2011. He has been included in the list of Top 2% Scientists in the world (prepared by Stanford University, USA, in October 2020). He is also the TPC Co-Chair of the International Conference on Computer Communications and the Internet (ICCCI 2020), the Nagoya Institute of Technology, Japan, ICCCI June 2020, at Nagoya, Japan, and will be held on June 2021, at Nagoya, and the Conference Chair at the World Symposium on Communications Engineering held at the University of Macedonia, in October 2020, and to be held at the University of Macedonia, in August 2019 and 2021, Thessaloniki (WSCE 2021). He has been serving as an Associate Editor for IEEE Access and IEEE Communications Letters. He is a Lead Associate Editor of the Special Issue on Roadmap to 5G: Rising to the Challenge of IEEE Access in 2019. He is a Guest Editor of the Special Issue on Compressive Sensing-Based IoT Applications of *Sensors* in 2020 and the Special Issue on Advances in Baseband Signal Processing, Circuit Designs, and Communications of *Information* in 2020. He is a Lead Guest Editor of the Special Issue on Artificial Intelligence for Cloud Based Big Data Analytics of *Big Data Research* in 2020.