PROFILING IN THE DIGITAL AGE: IMPLICATIONS OF ARTIFICIAL INTELLIGENCE AND CHALLENGES TO DATA PROTECTION

KALLIOPI TERZIDOU*

I. UNDERSTANDING ARTIFICIAL INTELLIGENCE

Artificial intelligence was officially conceived at the 1956 Dartmouth Artificial Intelligence Conference, organized by former Assistant Professor of Mathematics at the same institute, John Mc Carthhy. The purpose of this summer conference was to "*... proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it*", as described in the relevant proposal[1]. The outcome of two - month workshops was the conceptualization of AI, which refers to the ability of a machine to present and develop human cognitive functions by use of algorithms.

Artificial intelligence technology can be deployed for the facilitation of everyday life. "AI for Good" is a notion relating to the beneficial application of AI that contributes to the promotion of sustainability and the evolution of humanity. With a view to the 2030 UN Sustainable Development Agenda[2], AI leads to the prognosis of weather and climate change through simulations of climate models or to the treatment of diseases through analysis of radiological images[3]. On the other hand, there are voices warning about the threats deriving from the development of AI. The campaign "Stop Killer Robots", initiated by Human Rights Watch and other

* *LLB, Legal Intern at CIEEL*

1. J. MCCARTHY ... [et al.], A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955.
2. UN Resolution A/RES/70/1, Transforming our world: the 2030 Agenda for Sustainable Development, 25.09.2015, 4th plenary meeting.
3. The Royal Society, You and AI– AI Applications event, 2018.

similar NGOs, focuses on the ban of unmanned armed vehicles in warfare[4], while various tasks attributed to certain professions, such as the preparation of a legal document or the driving of a taxi, are to be performed by AI assistants[5].

At the same time, AI raises a certain amount of legal questions. Privacy is in the center of current talks, with this new technology interfering to private and family life by the processing of personal data or the creation and perpetuation of bias while automatically making decisions. Responsibility is another great debate, with experts leaning between liability of human agents and liability of robots[6]. Finally, the lack of foreseeability due to the advanced nature of these technologies is a drawback for transparency and sets the regulation of their use even more difficult[7].

II. PROFILING AND DATA PROTECTION

A. Definition of profiling and automated profiling

Profiling as treated in the General Data Protection Regulation (GDPR) is defined in Article 4(4) as "*...any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements*". In the words of Valeria Ferraris "*profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that can subsequently be applied as a basis for decision-making*"[8].

Profiling in the digital context is happening through automated decision-making which constitutes an application of AI technology. In specific, automated decision-making involves the forming of a decision without the human factor through the collection of mostly personal data that are made available with or without the individual's consent. Hildebrandt makes a distinction between automated and autonomic profiling. Automated profiling is defined as being based on "*automated functions that collect and aggregate data*" and develop into "*automation technologies that can move beyond advice on decision-making, taking a load of low-level and even high-level decisions out of human hands*". Autonomic profiling, on the other

4. See https://www.stopkillerrobots.org/.
5. J. MCKENDRICK, Artificial Intelligence Will Replace Tasks, Not Jobs, Forbes, 2018.
6. U. PAGALLO, Three Roads to Complexity, AI and the Law of Robots: On Crimes, Contracts, and Torts, AI Approaches to the Complexity of Legal Systems. Models and Ethical Challenges for Legal Systems, Legal Language and Legal Ontologies, Argumentation and Software Agents, Springer, 2011, p. 48.
7. B. BOUTIN, Technologies for International Law & International Law for Technologies, Groningen Journal for International Law, 22.10.2018.
8. V. FERRARIS ... [et al.], Working Paper Defining Profiling, UNICRI, 2013, p. 32.

hand, is described as "*the process whereby the human role is minimized and the decision-making process is entirely driven by the machine*"[9]. The main difference between the two cases is that in autonomic profiling the entire process of decision – making is driven by the machine without any human intervention and as such it is much more limited in use than automated profiling[10]. The Regulation is addressing the first case of automated profiling.

B. Purposes of automated profiling

Profiling can be used for a range of scopes. First of all, profiling provides a tool to predict someone's personal status and behavior. A common example would be inferring through posts on social media, such as tweets, the individual's location and ultimately his socioeconomic background.

It might, also, be used to decide or update a decision concerning a person. For example, in cases when companies want to determine during a hiring period if the applicant fits the criteria of the vacant position. In these lines, the company may deploy an algorithm that will help it sort out all the applicants that do not fit the predefined standards.

Finally, profiling helps to personalize the experience of the user based on the information provided by him/her or inferred by his/her past online activity. This tactic can be found in social media platforms or e-commerce websites when recommending contacts or products, respectively[11].

C. Effects of automated profiling

The effects of this practice are experienced on an everyday basis in the digital field. Initially, profiling poses a threat to someone's privacy, otherwise puts an interference to the right to respect for private and family life, as stated in the text of human rights treaties[12]. This happens on a two-fold basis: firstly, the high-degree intrusiveness of advanced technological means that are used to perform profiling. In specific, identification of an individual user can be achieved through cookies, small pieces of data sent from a website and stored in the user's computer in order for sites to remember stateful information or record the user's browsing activity. Another means is cross-device tracking used to track owners of smart-devices through

9. M. HILDEBRANDT, Defining profiling: new type of knowledge?, in M. Hildebrandt / S. Gutwirth (eds), Profiling the European Citizens, Cross-Disciplinary Perspectives, Springer, 2008, pp. 17-47.
10. M. HILDERBRANDT, Profiling: from Data to Knowledge. The challenges of a crucial technology, DuD Datenschutz und Datensicherheit, 2006, pp. 548-552.
11. Privacy International, Data Is Power: Profiling and Automated-Decision Making, GDPR, 2017, pp. 4-6.
12. Article 12 of the Universal Declaration of Human Rights, Article 8 of the European Convention of Human Rights and Article 7 of the Charter of Fundamental Rights of the EU.

ultrasounds emitted from the microphone of the device and recognized through the microphone of another one. Device fingerprint is an additional measure that collects information from a remote device for purposes, such as identity theft[13].

Secondly, profiling threatens people because of the artificial intelligence's advanced nature. The problem sums up to one word: superintelligence. Superintelligence can be defined as "*any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interest*". Artificial intelligence can, through ongoing developments, reach this level of intelligence so as to perform cognitive tasks at a higher speed, greater quality and greater range of specialized domains so as to outperform the human input. Scientists discuss the possibility of a seed AI that is different from the artificial general intelligence, which is dependent on the human factor. Seed AI will be capable of developing on its own the intelligence amplification superpower, that is the human designed system that enables the AI to develop independently its cognitive powers. Therefore, issues of transparency through information of the public about this technology and control of advanced cognitive capabilities of AI need to be addressed[14].

Moreover, profiling can create bias since the inferred data can lead to identification of people to whom are attributed, accurately or not, characteristics that refer to their racial, socioeconomic or sexual orientation background and can lead to discriminatory decisions for the data subject. Questions of ethics can be raised as well, like the limitation of the variety of information in the net, due to the directing of the users' preferences every time AI personalizes the online experience through recommendations, or the restriction of their online behavior for fear of surveillance[15].

III. PROFILING AND THE GDPR

The General Data Protection Regulation includes a set of provisions, both general and specific ones, in order to respond effectively to the issue of profiling. Profiling is a form of processing of personal data and as such will be governed by principles, lawful bases and rights that restrict the unlawful execution of this practice according to Articles 5-18 of the Regulation. But the main provision for profiling in the GDPR is Article 22, which prescribes that the individual can object to being subject to a decision that is made solely on the basis of automated processing, otherwise said with the aid of AI technology.

A. Right not to be subject to automated decision-making practices

The practice of profiling is specifically targeted in Article 22. The first paragraph states: "*The data subject shall have the right not to be subject to a decision based*

13. Privacy International, o.p., p. 8.
14. N. BOSTROM, Superintelligence: Paths, Dangers, Strategies, OUP, 2014, pp. 63-74.
15. Privacy International, o.p., pp. 8-9.

solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her". The scope of the article is to give the benefit of choice to the data subject to allow or deny a machine to make a decision regarding his online activity. Paragraph 1 already reflects the notion of automated decision-making, distinguishing the involvement of a human being assessing the content of the said decision from a machine implementing itself the same task[16]. The mention of profiling is indicative, as deduced by the word "including", meaning that other practices using AI technology can also fit under the predictions of this provision.

There are two prerequisites for the data subject to be able to block the automated processing of his/her personal data. The decision based solely on automated processing of the individual's data must produce "*legal effects concerning him or her or similarly significantly affects him or her*". "Legal" means that the decision is affecting the legal status and the rights of a person. Therefore, the denial of child benefits granted by law is affecting the right of the individual to access social security. "Similarly significant effects" relate to effects that are reaching the threshold of significance afforded by the legal ones. The examples provided by Recital 71 of the Regulation are the automatic refusal of an online credit application and the e-recruiting practices without any human intervention. More specifically, in order for the decisions to be significant enough they must: significantly affect the circumstances, behavior or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals[17].

The second paragraph introduces three circumstances that, if applied, will render inactive the right to object to automated processing. Therefore, paragraph 1 will not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorized 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.

The first case of a performance of a contract is common in transactions. An exemplary case would be the automatization of the recruiting process by the companies. The norm in the latest years is that the employer will use a professional program that runs with AI, which sorts out the candidates based on predefined criteria and eventually distinguishes the most competent applicant. The second exception occurs when the Union or a member state allows by law the use of these means. Such

16. P. VOIGT, The EU General Data Protection Regulation: A Practical Guide, 2017, pp. 180-184.
17. Article 29 data protection working party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2017 (Rev. 2018).

policies aim at the implementation of Union goals or national interests respectively, such as the freedom to provide services to the extent of the EU or the combating of fraud and tax evasion at a national and transnational level. The final exception constitutes a general reason of exemption of the unlawful character of an action, being the consent of the data subject. Such would be the case with the agreement to a set of "Terms and Conditions" when accessing a web page. The consent needs to be "explicit", it does not suffice to simply infer it. Furthermore, the consent needs to be "valid" as prescribed in Article 4(11), which states that the consent is "... *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*". It is really important, thus, that any individual is informed about the conditions under which his/her personal data will be processed and the relevant consequences[18].

The third paragraph is complementary to the second and refers to the requirement of regulated safeguards in the national and Union spectrum in relation to the exceptions of the performance of a contract and the provision of a consent. The minimum safeguards stated are the right to obtain human intervention on the part of the controller, the right to express their own view and the right to contest the decision made by automated means. Recital 71 elaborates further, adding the right to be informed in a specific manner of the data processing. Even if all the possible measures in relation to the data subject are followed, the procedure of the profiling must still fulfill certain criteria. Therefore, the controller should use "appropriate mathematical or statistical procedures" and implement "technical and organizational measures" to make sure that no inaccuracies and errors of personal data exist. This approach addresses the problem of bias that is presented when utilizing artificial intelligence, with the responsibility falling upon the creator of the algorithm that diffuses discriminating views when constructing it[19]. The algorithm cannot be totally unbiased, but the risk for discrimination can be limited by designated procedures to prevent at the designing stage and limit during the deployment of the algorithm such effects[20].

The last paragraph of Article 22 excludes "special categories" of personal data from the authorized cases of automated decision-making under the second paragraph. Those categories are described in Article 9(1) as: "... *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and ... genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation ...*". This kind of data cannot be processed whether they fall into the performance of a contract, the Union or member state

18. Article 29 data protection working party, o.p., pp. 6-19.
19. P. MILLICAN ... [et al.], Are all algorithms biased?, University of Oxford Podcasts, 2018.
20. Article 29 data protection working party, o.p., pp. 27-28.

law or the provision of the consent of the data subject, unless cases a-g of Article 9(2) are in place. These cases concern a set of legitimate aims, including public interest, social protection, facilitation of legal justice and protection of freedom of association, on the condition that these aims are accompanied by the appropriate safeguards. The explicit consent is also referred as a case that allows the processing of special data by automated means, with the terms described above[21].

B. Overview of legal protection from profiling afforded by the Regulation

Profiling under Article 22, with the particularity of being realized through automated means, constitutes, after all, a series of processing and, as such, it is subject to the general provisions of the Regulation on processing of personal data.

1. Article 5

The first provision deals with the processing of personal data is Article 5 which refers to six main principles. It starts with the requirement that the personal data will be processed lawfully, fairly and transparently. "Lawful" means that it needs to have a basis in the domestic law. "Fair" will be the processing that does not provide grounds for discrimination. Profiling can be unfair when it creates bias, as it is the case when a financial institute that needs to determine loan eligibility will use AI that categorizes the clients according to their race as to infer their financial credibility. "Transparency", as explained in Recital 39, essentially requires that the data subject is informed in principle of the identity of the controller, the purposes of processing and the right to obtain relevant information in an accessible and clear manner[22].

The second principle calls for the processing for "specified, explicit and legitimate purposes" that will not be further altered in the future. An application, for instance, will require from its potential clients before the installment access to photographs or other forms of data for the purpose of optimization of their personal experience. These initial purposes can be supplemented only if the processing is dedicated for "*... archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ...*", along with the safeguards prescribed under Article 89.

The third principle introduces the reader to yet another manifestation of the concept of proportionality. In a general manner, proportionality demands that the said measure is adequate, relevant to the desired scope and necessary, being the least intrusive measure. The scope relates to the purposes of processing that must be clearly defined as required by the second principle. Massive and robust processing of personal data lacks proportionality and it is often executed while less intrusive means are in place, such as the anonymization of the obtained data.

---

21. P. VOIGT, o.p., pp. 110-116.
22. Article 29 data protection working party, o.p., pp. 9-12.

The fourth principle highlights the need for the "accuracy" of the personal data. Therefore, if they are not up to date, they need to be erased so as not to mislead the receiver about the profile of a person that has been falsely created. False information can have an impact to the civil and social rights of the data subject, limiting, for example, his ability to obtain insurance or a loan or participate in the public healthcare system, excluding him on the basis of miscalculated financial data.

The fifth principle concerns the "storage" of the personal data. The maintaining of data needs to be long enough to fulfill the legitimate and defined purposes of processing, with the exception of the purposes defined in Article 89(1). It is expected that the principle of proportionality is followed along with the accuracy requirement.

Finally, the sixth principle requires the existence of safeguards to ensure the respect of the rights of the data subject against unlawful processing and accidental loss, destruction or damage of the processed data, in accordance with technical and organizational measures in place as prescribed in Article 32, including pseudonymization, encryption and testing of the accessibility and confidentiality of the processing procedure. An additional safeguard is the accountability requirement as predicted in the second paragraph of Article 5. More specifically, the controller is accountable for the processing in accordance with the six principles of paragraph 1 and the ability to prove it. Regarding the appropriate processing, the controller must undertake all the necessary and relevant technical and organizational measures that exist so as to ensure the protection of the personality of the individual concerned. As for the demonstration of the rightful procedure, the controller is accountable under the supervisory authorities of Chapter 6 as appointed by the member states, namely independent public bodies responsible for monitoring compliance with the Regulation[23].

2. Article 6

Article 6 provides for six lawful bases of processing and leaves the elaboration of the conditions surrounding their application on the national legislators.

The first two bases concern the consent of the data subject and the purpose of the performance of a contract, as already analyzed. The third basis entails the necessity to comply with a "legal obligation", hence the requirement of national or Union legislation to assign certain positive or negative obligations for the controller to abide.

The fourth basis provides for the necessity to protect "vital interests" of the data subject or other natural persons. As explained in Recital 46, "vital" is an interest essential for life, meaning that the processing is allowed when the life of the person concerned is directly involved. This will happen in cases of medical emergencies,

23. P. VOIGT, o.p., pp. 31-32.

when the data subject will be unconscious and thus unable to give his/her consent for the processing of relevant personal data. The provision of the consent is generally a more preferable legal basis, while the protection of vital interests can be accepted as a last resort. In practice, the basis of vital interest will be rarely chosen since most processing actions can be justified by public interest. The vital interests of the natural persons are also taken into consideration, when, for instance, a parent needs to give his/her consent for the processing of his/her child's medical history for the purposes of a surgery.

The fifth basis is public interest or official authority. "Public interest" is a common justification ground when there is a need for the public authorities to derogate from the provisions of international legal texts. The risk for abuse by authorities is likely high, since the margin of appreciation in these cases will allow for discretionary powers that may not require specific and accessible reasoning. As a result, the principle of proportionality must apply for the measures to be mitigated in accordance with the subject's rights.

Lastly, processing has a legal basis if the controller or the third party pursues legitimate interest that does not override the fundamental rights of the data subject, especially if it is a child, always in accordance with the principle of proportionality. Recital 46 gives the example of the offering of services from the controller to the data subject, which in the case of profiling can apply to the installment of applications under the condition of providing access to personal data stored in the device[24].

3. Additional provisions on profiling

Some additional protection from unlawful profiling by automated decision-making includes Articles 9, 13-18 and 21.

Article 9 grants legal protection to "special categories" of personal data, most often data that reveal racial origin, political or religious views and sexual orientation, in cases where algorithms create correlations based on data provided by the subject, so as to deduce such sensitive information. An example would be when, based on the online activity on social media, the controller can - sometimes with utmost accuracy - predict the ethnic origin of a person. Consequently, the controller must comply with the principles of Article 5 and ensure that the data subject is informed about such processing and has given his/her consent, while a lawful basis will be in place, as required by Article 6.

Articles 13-18 concern the rights of the data subject in relation to the processing of his/her personal data. In particular, Articles 13 and 14 provide protection to the data subject by giving him/her the right to be informed about the processing activity, whether the data is collected with or without his/her knowledge. There is a set of information that must be provided, mainly the identity of the controller, his/

24. Information Commissioner's Office (ICO), Guide to General Data Protection Regulation, Lawful basis for processing.

her contact details, the purposes of processing, the legitimate interests pursued, the recipients and, where applicable, the intention of transferring of the data to a third country or an international organization. Further information includes the period of processing, the existence of a complaint mechanism and the existence of automated decision-making, along with the explanation of the mechanism and its consequences.

Article 15 introduces the right of the data subject to have access to his/her personal data that is being processed by the controller. The right to access the data also includes general information around the profiling activity as prescribed in Article 13. There is the possibility of obtaining a copy of the personal data under processing in Article 15(3), if that does not abuse the freedoms of others.

The data subject can also be informed about his/her right to ask for the rectification, erasure and restriction of the profiling. "Rectification" under Article 16 will be requested when the data is inaccurate and needs to be either erased or supplemented with even more information to reach a valid point.

"Erasure" or the "right to be forgotten" under Article 17 calls for the deletion of the personal data meant for profiling, bound by a set of prerequisites, namely if the data is no longer necessary, there is no legal basis or legitimate interest, the profiling has been executed unlawfully, there is a legal obligation for erasure under Union or member states law or the collection was done for society services purposes under Article 8. The second paragraph of Article 17 provides for exceptions from the erasure procedure that concern the protection of fundamental rights or public interest.

Finally, "restriction" of profiling can take place under Article 18 when and if the data is inaccurate, the profiling unlawful or unnecessary and the individual concerned has objected in accordance with Article 21. The latter provision gives the individual the right to object to the processing of his/her data and is connected with Article 22 in a relation of general-to-specific. If the data subject objects, then the controller must cease the profiling immediately. There is room for continuing the profiling process, as long as there are legitimate grounds for justifying it. In that case, the controller must comply with the proportionality test[25].

IV. CONCLUDING REMARKS

It is evident that, while machine learning will only progress in efficiency and results, the response of the GDPR must be more adaptable to this ongoing progress. Therefore, the legislators, both at a national and at a Union level, should draft and pass certain amendments to ensure the effective protection of the data subjects from profiling that directly or indirectly affects their right to privacy.

As it concerns the main provision of the GDPR that tackles profiling by automated

25. Article 29 data protection working party, o.p., pp. 22-25.

decision-making, namely Article 22, there are two central issues that derive from the excessive technological advancements of artificial intelligence. The first one concerns the right to be informed of the processing of personal data about the scope of profiling as provided for in Article 5 of the Regulation. Such knowledge is a prerequisite for exercising the objection to have a decision taken through automated means and stems from the general principle of transparency. However, it is clear that there lies a complexity when it comes to explaining artificial intelligence and how it works to reach the ultimate goal of forming a profile and diffuse it for certain purposes. Therefore, the information provided must be in a simple language and given in an understandable manner, without further impeding the quality of the information[26].

With this comes the second issue relating to the rapid development of artificial intelligence and the creation of a superintelligence, which could become unable to tackle. Yet, there is room for exercise of control over these systems, at an extent which will prevent super intelligent AI from becoming harmful to the data subject by making decisions on its behalf that result in unlawful profiling. The key to this problem is strategic analysis and capacity-building. The former will be needed to envisage the possible paths that AI development will take, essentially forming the question before getting to the answer, while the latter will be important in order to arm scientists with the ethics to build mechanisms that will tackle the problems raised by superintelligence. Nevertheless, the focus will remain on the human manufacturers and controllers of AI systems that need, through best practices, to acquire a more risk-aware attitude towards future advancements that may cause harm to the rights of the people and will commit themselves in building and operating safer systems that will facilitate rather than restrict human activities[27].

26. P. VOIGT, o.p., pp. 87-92.
27. N. BOSTROM, o.p., pp. 314-320.