EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Robots, unwearable profiling and protection of vulnerable users

PAOLA GRIMALDI
Ph.D. at University Federico II of Naples
Lawyer

Abstract

The massive spread of the Internet, the growing use of social networks and the creation of apps have increased and simplified the activity of unaware profiling of users. The phenomenon becomes much more serious when it affects vulnerable users. The GDPR 679/2016 deals very precisely with the issue of profiling personal data by offering adequate protection in several articles by providing adequate security measures to protect users of new technologies and paying particular attention to vulnerable users.

Keywords: Robot - Unwareble profiling - Privacy - Vulnerable users.

Introduction.

Technological evolution has come to create machines equipped with cognitive abilities and able to interact with humans and the enviroment, showing an ability to adapt independently to surrounding simuli and to assume consequent behaviors; a faculty therefore, similar to the will expressed through a behavioral response (so-called feedback)[1]. The debate of the intelligence of machines started from that strong position[2] of those who imagened that machines would come to think like humans and to be independent; to then fall back on a light position[3] by virtue of which the machines, while showing to be, to some extent, psychologically similar to humans because they can assume psychological states similar to human ones, will not be able to emulate skills and characteristics such as creativity, imagination, intuition, emotion and, above all, awareness of oneself and one's actions[4].

In other words some specific tasks performed by the mind are not algorithmic in nature and, at least for now, cannot be developed by software.

---

[1] P Moro, 'Libertà del robot? Sull'etica delle macchine intelligenti', in R Brighi, S Zullo (ed.) *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica,* (Aracne, 2015), 525-544.

[2] LA Del Monte, *The Artificial Intelligence Revolution, Will Artificial Intelligence Serve Us Or Replace Us* (Louis A Del Monte, 2014) 87; according to which there is no regulatory limitation on the amount of intelligence that can be inserted in a technological apparatus, by 2040 there will be what the author defines "the incredible overtaking" for which the dominant "living" species will no longer be the human one but that of the machines that will acquire self-awareness and progressively conquer the ability to protect themselves.

[3] Position known as the "weak approach to artificial intelligence": to create a new intelligence which, while being characterized from a cognitive point of view, will nevertheless be different from the human one.

[4] For an overview on the topic: E De Santis, 'Computational intelligence and computational thinking: le macchine intelligenti si stanno avvicinando a noi?' <https://www.academia.edu/16172952/Computational_Intelligence_e_Computational_Thinking_le_macchine_intelligenti_si_stanno_avvicinando_a_noi> accessed 28 september 2015.

The light approach to artificial intelligence, supported by authoritative scholars, therefore, does not deny that machines can perform operations that would require an intellectual commitment to humans, but affirms that the intelligence of machines still has a different nature from that of humans.

This last aspect has been explained with reference to the capacity for self-awareness: the intelligence of machines is expressed in conditions of unconsciousness, in the sense that they act "not thinking of themselves".

And in this regard, it is stated that in order to attribute consciousness (or, at least, intentionality) to machines it is not enough to verify that the behaviours and results achieved by a machine do not differ from human ones, but it is necessary to prove that the machine has account of his behavior and really wanted those results[5]; in other words, that there was some willingness to activate the behavior.

The vision of a light intelligence does not exclude a cognitive and behavioral autonomy of the machines, albeit of a technological nature.

In this respect, autonomy rests on data processing and learning processes; in interacting with the environment, machine learn and emancipate themselves, making decisions and behaviors without the intermediation of a closed procedure.

In the machine learning perspective[6], behaviors are not predetermined by the instructions of a software, but are learned from the processing of the experience according to a criterion for improving performance; which implies how said behaviors, although attributable to a learning model, are to some extent non-deterministic and therefore not predictable in their specific unfolding.

In this regard, one can realistically imagine that a robot can assume an initial behavior defined by a software, but also has the ability to modify it after processing a set of data detected, through its sensors, in the surrounding environment.

In this condition, it appears somewhat complex to know in advance which data will be collected and what the new behavior of the machine will be.

The unpredictability of machine behaviors: whoever produces or programs an intelligent machine is able to predict its behavior once it has started to learn from experience? Are these simply objects or do these intelligent machines have to be given some level of subjectivity? Has technology created a new legal entity? Are those non-human subjects able to manifest their own action?[7]

Starting from these questions, there is now a strong need expressed by many to increasingly develop robot law[8], to regulate the behavior of robots and their coexistence with humans[9].

---

[5] GT Elmi, 'I diritti dell'«intelligenza artificiale» tra soggettività e valore: fantadiritto o ius condendum?', in L Lombardi Vallauri (ed.), *Il meritevole di tutela,* (Giuffrè, 1990), 685-711.

[6] When we talk about *machine learning*, we are talking about a particular branch of computer science involved in the study and development of artificial intelligence and we refer to the different mechanisms that allow an intelligent machine to improve its capacity and performance over time. The machine, therefore, will be able to learn to perform certain tasks by improving, through experience, its skills, responses and functions. At the base of machine learning there are a series of different algorithms which, starting from primitive notions, will be able to make a specific decision rather than another or carry out actions learned over time.

[7] On this point see B Bisol, F Lucivero, 'Diritti umani, valori e nuove tecnologie. Il caso dell'etica della robotica in Europa' (2014) 2 Metodo.ISPP, 235, 252; E. Datteri, 'The epistemic roles of automata from cybernetics to contemporary robotics' (2019) 6 RS 245, 256.

[8] In this sense, see P Stanzione, 'Biodiritto, postumano e diritti fondamentali' [2010] CDC 1,15; and also, L Marini, I Aprea, 'Le guidelines on regulating robotics: una sfida per il diritto dell'Unione' 5 (2015) OIDU 1295, 1302.

[9] For an overview of the point: Pontificia Accademia per la Vita, *Roboetica. Persone, macchine e salute*, Workshop 25-26 February 2019.

As part of the debate on the ethical-legal implications of the behavior of robots, there is, among others, the issue of the processing of personal data that they can carry out within the activities for which they were designed, and their compliance with the framework European legislation; the reference, of course, is to the GDPR 679/2016[10].

In this regard, he points out that the processing of data (personal and otherwise) is an essential function of robots in the light of cognitive characteristics by virtue of which they interact with the environment, learn and exhibit autonomous behaviors. In this respect, it should not be excluded that cognitive robots may collect data regarding the users who use them and then transfer them to other people and/or organizations with which the same robots interact.

1. The unwareble profiling.

In general, profiling means any form of automated processing of personal data consisting in the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of that natural person.

There are three ways of using profiling: general profiling, decision-making based on profiling, decision-making based solely on automated processing.

The legislator pays particular attention to the fully automated decision-making process which also includes profiling, which is capable of producing legal effects or significantly affecting the personal sphere of the data subject; as specified in the guidelines of the European Guarantors[11], it is, concretely, that process in which human intervention is not present or is not significant for the purposes of the decision.

User profiling specifically means the set of data collection and processing activities relating to users of services (public or private) to divide users into behavior groups.

In the commercial field, user profiling is a so-called profiled marketing tool[12], which makes extensive use of this and other techniques to obtain accurate analysis of potential customers, often operating at the limit of the legally permitted, if not beyond[13].

A similar scenario, indeed, re-proposes a question well known in digital news which, from the most recent cases related to the introduction on the market of the so-called apps, date back to the experience of the nineties of the software called *Real Player*[14].

These applications allow access to information and entertainment content, only to discover that the same have been designed to contain instructions for the transmission to other parts of information on the behavior and preferences of users, on their geographical location, often without them are aware.

The massive diffusion of the Internet and the growing use of social networks have

---

[10] G Crea, 'Macchine intelligenti e protezione dei dati in una prospettiva di ethics by design' <https://www.altalex.com/documents/news/2018/02/20/macchine-intelligenti-e-protezione-dei-dati-in-una-prospettiva-di-ethics-by-design> accessed 20 February 2018.

[11] Guidelines on the automated decision-making process relating to natural persons and on profiling for the purposes of the regulation 2016/679, adopted on 3 October 2017 in ec.europa.eu, page Justice and Consumers.

[12] Profiled marketing is a form of advertising that allows you to send personalized advertising messages according to the interests and preferences of users acquired through profiling tools that allow you to collect information suitable for defining the user's profile or personality or analyze his habits or consumption choices.

[13] R Rapicavoli, *Privacy e diritto nel web. Manuale per operare in rete e fare marketing online senza violare la legge,* (Hoepli, 2017) 132.

[14] Regarding the software most downloaded by all users at the time, security researcher Richard Smith discovered in 1999 that there were serious privacy concerns as RealPlayer assigned a unique ID to each user and then subsequently transmitted a list to RealNetworks of all stored media files.

increased and simplified the activity of user profiling. Concrete cases are represented by the "like"button of Facebook or of the surveys that the social network itself carries out through special app[15]; in this last regard, the sensational case is that of Cambridge Alalytica which collected user data through survey applications on Facebook, organized the data with the so-called profiling activity and sold them to Trump and other interested parties, without his know ledge of Facebook users who the Nametest survey app convinced that the results were used for research purposes and, on the other hand, subsequently found their profiles, with all their data, used to target targeted advetising campaigns.

What is even more serious in the story just described is that Cambridge Analytica has also collected data relating to friends of users who had used the app.

This is all due to the fact that Facebook's policies and default privacy settings allow apps to collect huge amounts of data from profiles. It should be noted, however, that Facebook does not work alone in this collection of personal data, but rather finds itself in good company with other giants of the web, such as Google, Netflix, Amazon, Spotify, Youtube and Apple.

In short, the serious risk of finding oneself really in that era defined as *Surveillance Capitalism*[16] with a power in the hands of a few who possess various personal data analyzed in the light of special algorithms, which allow to profile the users of the service, refining their identities digital.

The effect of this activity as described is that an individual will be associated, in a completely unconscious way and without his consent, targeted predictions that outline a digital identity that may even be completely misleading with respect to reality. Sensitive data of an individual, such as personal, genetic, health, behavioral data, could be subject to digital profiling, caging the identity of the same. It is evident that such solutions circumvent the phase of giving consent by the interested parties and, by exploiting their unawareness, they do not even favor ex post interventions to oppose the treatment.

2. Unaware profiling by smart speakers and protection of vulnerable subjects.

The phenomenon described above becomes even more serious when it affects the so-called subjects. vulnerable. And in this regard, there is a wealth of cases that we now have available worldwide, also through the widespread use of the so-called in homes. digital assistants that certainly make our homes more and more smart home, but with the serious risk of compromising our privacy in the place that should represent for us the safest place away from prying eyes and ears.

Smart speakers equipped with a voice assistant are able to collect much more data than a simple Internet search engine and then make them available to companies that already have a huge amount of information on our behalf; think of Google and Amazon[17].

Just to give a few examples, in the United States an important multinational such as Mattel was forced to withdraw the launch of an innovative product such as Aristotle, the first smart speaker designed for children, due to protests and accusations of risk of invasion of the privacy of the same and of an unaware profiling of minors and their families; in Germany the authorities of the German Federal Agency for telecommunications networks have asked their dealers to withdraw the American Cayla doll from the shelves, considered a potential spying tool because, connected via Bluetooth and connected to the Internet, easily hackable, able to listen, record and respond, violating the local national law on telecommunications as it hid a camera and a microphone capable of sending signals and forwarding data unnoticed,

[15]To name a few, survey apps widely used by social networks are Nametest, Toluna and Polly.
[16]S Zuboff, P Bassetti, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, (Luiss Press, 2019).
[17] https://www.gpdp.it/web/guest/temi/assistenti-digitali.

thus damaging the private sphere of people and specifically children, vulnerable subjects from protect and protect even more.

Another case is that of Amazon's *Alexa*, which is also now a famous and widespread smart home device;

for some time, Amazon has been increasingly looking for methods and strategies to use technology as a resource to improve the lives of the elderly and in particular is developing new skills, skills aimed at facilitating the daily life of this growing demographic group which, often, despite the health problems and advancing age, he insists on wanting to live independently for as long as possible. But even for *Alexa* there is no lack of perplexity regarding the real and effective privacy policy of its users put in place by the manufacturer; all considering the "personal data" cases that occurred in Germany and the United States, which concerned the device in question which, after having listened to and recorded a conversation at home, sent the conversation itself, by mistake in interpreting a word heard to some contacts of its users; all this without the knowledge of the latter. It is clear that in this case it was not a human error, but an error of the artificial intelligence system; which leads us to think that, if on the one hand the advantages of technological evolution cannot be denied, on the other, however, it is necessary to approach it with awareness of the potential, but also of the risks, especially when it is the weakest groups who benefit from it. and defenseless of the digital population (children, elderly, disabled, etc. ..).

It is clear that the technology in question must also comply with the rules and principles provided for by the GDPR 679/2016, but to meet the general need to provide strong and targeted protection to those who use such devices, on the European regulatory side there has been the " issuance of the "Cybersecurity Act"[18], a European Regulation which aims to create a uniform and well-defined framework on the certification of IT security of ICT products and digital services; and this, of course, is also of great importance for the smart speaker sector, as the manufacturers of the same must also comply with these new rules in the near future[19].

3. GDPR and legal protection of vulnerable subjects in automated profiling.

The profiling activity has never been the subject of organic and unitary legislation because the regulatory framework has always been very fragmented. Directive 95/46, for example, deals with profiling only with reference to automated decision-making #. In 2002, as a lex specialis with respect to the aforementioned European source, the so-called E-privacy directive (2002/58 / EC) which introduced more specific rules on online tracking technologies (such as cookies), as well as the user's informed consent for their use for profiling purposes. The Privacy Code (Legislative Decree 196/2003), on the other hand, includes the profiling activity among the so-called treatments at risk to be notified, therefore, to the Privacy Guarantor. Finally, the advent of increasingly complex, innovative

[18]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, the European Union Agency for Cybersecurity, and on the certification of cybersecurity for information and communication technologies, and which repeals regulation (EU) no. 526/2013 («cybersecurity regulation»).

[19]The Regulation in question represents an important step for the European Union because it constitutes a clear strategy of strengthening against cyber attacks and the consequent violation of privacy. Furthermore, the legislator's intention was also to strengthen the role of the European Union Agency for Network and Information Security (ENISA) which, therefore, will no longer act as a simple supervisor and assistant to member states in the development of cybersecurity strategies, but will play a concrete operational role because it is used to prepare new European certification schemes compliant with the Cybersecurity Act. These schemes will subsequently be adopted by the EU Commission and will become executive and available to European companies. Clearly these schemes will replace national regulations; it should be noted, however, that, for products certified at national level, their validity will remain unchanged until their expiry.

technologies capable of unprecedented interconnection between users has been a harbinger of new and more appropriate protection strategies: above all for these reasons, during the design and drafting of the GDPR, the need to innovate the regulation of profiling. And precisely with respect to Artificial Intelligence and its multiple applications, the horizon of the topics of competence of the Privacy Guarantor is now boundless. The GDPR 679/2016 in a very precise way addresses the subject of profiling personal data by offering adequate protection in several articles. As specified above, the method of using profiling can also be completely automated and it is in this case that more critical issues are encountered and that the attention of companies, bodies and organizations should increase because in such cases the data collection mechanism for the automated taking of decisions could be based precisely on profiling. The GDPR deals with automated profiling in art. 22, affirming in particular the right of the interested party not to be subjected to a decision based solely on automated processing that produces legal effects concerning him or that significantly affects his person in a similar way. The European Data Protection Committee intervened on the subject and drafted specific Guidelines which, specifically, outline the activities that the data controller will be required to carry out in the event of automated profiling: he must provide, first of all, clear, complete and exhaustive information so that the interested party provides a consent that explicitly allows to pursue profiling purposes which, it should be remembered, according to art. 4 § 4 of the GDPR is represented by any manifestation of free, specific, informed and unequivocal will of the interested party. The possibility of using previously collected data for other purposes is therefore inhibited, unless there has been consent for the specific profiling purpose. Otherwise, it is up to the owner the obligation to implement adequate security measures to protect the data subject. And in this regard, art. 35 GDPR introduces the interesting and innovative institute of treatment impact assessment (DPIA Data Protection Impact Assessment). It applies when a type of data processing based on new technologies creates a high risk for the rights and freedoms of individuals. In this case, the data controller is required to assess the impact this may have on the protection of personal data. The risk inherent in the processing is to be understood as the negative impact on the freedoms and rights of the data subjects and represents the pivotal tool through which the owner carries out the analysis of the risks deriving from the treatments put in place. The owner, therefore, must develop a preventive assessment, before starting the processing, of the consequences of the data processing on the freedoms and rights of the data subjects. Unlike safety assessments, the impact assessment should be developed only for particular treatments, i.e. when the treatment involves the use of new technologies and can present a high risk for the rights and freedoms of individuals. Article 35 of the GDPR indicates the criteria on the basis of which the cases in which the DPIA is necessary are identified. Furthermore, paragraph 5 of art. 35 grants the supervisory authorities the possibility of drawing up a public list of types of processing for which the DPIA is required. In this perspective, our Privacy Guarantor, together with the high European authorities, has prepared a list that has been the subject of an opinion by the EDBP (European Data Protection Committee). In particular, the Italian Guarantor has identified twelve types of treatments subject to the DPIA obligation, listed in Annex 1 to the Provision of 11 October 2018. And the framework envisaged by this list would seem to go in the direction of an expansion of the scope of the obligation of DPIA. In particular, the hypotheses listed in point 6) include that relating to the non-occasional processing of data relating to vulnerable subjects (minors, disabled, elderly, mentally ill, patients, asylum seekers, etc.).

Conclusions.

From all the above, it is clear that personal data has an absolute value that must be

protected and safeguarded in the face of the rapid and relentless development of new technologies in the face of which man's approach should have a double attitude: of awareness with respect to potential of the technologies themselves and of prevention, with respect to the risks that inevitably derive from using them. Certainly, one cannot think of opposing technological development or of somehow curbing the creativity of information technology and, indeed, new technologies and their evolution must be viewed positively if one thinks, as already examined above, of the potential that they can have in covering roles of assistance and support to categories of vulnerable subjects; however, these potentials must be approached with awareness and intelligence, always remaining on guard against the concrete possibility that all this technology can "attack" the privacy of users. Therefore, an attitude of protection of personal data and the adoption of appropriate precautions is essential, even by the same large manufacturing companies that it is hoped that they will proceed increasingly planning according to the framework of ethics values (ethics by design) of which of course privacy is part of it[20].

And following the references made in several circumstances on this point by the Privacy Guarantor, the response of all the protagonists of this sector should be based on the ethics of responsibility to be implemented precisely in the design phase of the technological measures (software) that are able to minimize at the highest level the risks of harmful behavior of robots for the privacy of all, but in particular of the categories of the most vulnerable subjects in society; all this, spreading more and more the culture of the importance of the immense wealth of personal data available; the risks to which the data are subjected on a daily basis; creating awareness of the existing rules and means for the protection and safeguarding of one's privacy and, consequently, of the possibility of demanding the so-called privacy by design from companies that produce in the Internet of Things sector and therefore not adjusting to the passive use of robots, taking into account that companies themselves are responsible for assessing the privacy impact and subject to severe penalties if this is not done correctly. With specific reference to digital assistants, it is clear that they should be technically developed in compliance with the principles of confidentiality and data protection and, according to the GDPR legislation, ensure transparency and control of user information, allowing for concrete data governance.

Anyone who produces AI devices and places them on the EU market cannot disregard the GDPR, as already specified above is required to provide privacy by design in the design, to clearly define the perimeter of the processing of personal data. The principle of accountability returns, for which it would be essential for companies producing AI tools to provide basic technical product information in a transparent manner, which instead are almost never so easily available; and still companies or even consumers themselves should take action for a privacy impact assessment before purchasing and using such smart devices.

[20]A Nunn, 'Does Privacy By Default Mean Researchers Should Reconsiderer Reaserch Ethic Practice in relation to recording Informed Consent' (2018) 1 EJPLT.