Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Daniel Terrón Santos
Director of the Almirante Martín Granizo Chair, USAL-CESEDEN

Email: datersa@usal.es

Artificial intelligence and biometric systems for military use: redefining artificial intelligence from an ethical and legal perspective

Abstract

This article addresses the need for prevention, without limiting or doing it just enough, so that artificial intelligence, as an almost plenipotentiary tool, may make a major contribution to security and defence applications. More specifically, the use of biometric systems opens up a whole world of opportunities in the security sector, but at the same time it clashes with inalienable rights and guarantees. This confrontation must be resolved on the basis of ethics and law, without in any case setting an absolute limit to the use of a decisive tool, with basic and essential military applications.

Keywords

Technology, Military applications, Biometrics, Ethics, Control.

Cite this article:

Terrón Santos, D. (2024). Artificial intelligence and biometric systems for military use: redefining artificial intelligence from an ethical and legal perspective. *Journal of the Spanish Institute for Strategic Studies*. 24, pp. 509-529.

1 Introducing predictive artificial intelligence

To predict means to be able to anticipate that which is undesirable in order to prevent it or, on the contrary, to take advantage of the opportunities that prior knowledge can bring, obtaining optimal results. Prediction, according to the definition provided by the Dictionary of the Royal Spanish Academy of Language, can be arrived at by revelation, founded knowledge, intuition or conjecture. This assumes, eliminating the option of intuition, where one starts from indications or observations, that prediction, in the end, is an analysis of data obtained in different ways. In a way, it all depends on the meaning, within those that are accepted, which people seek to give to the concept of intelligence. This concept coincides with that of prediction, in that both involve data analysis to obtain knowledge that, once applied, may be used for problem-solving, decision making, etc.

By now, almost everybody is familiar with the concept of artificial intelligence (hereinafter AI), therefore, all that has been said until now is perfectly transposable at this point. However, we must approach it in relation to predictive analytics. If the concept of artificial intelligence is approached, especially in relation to its nature which is alien to human behaviour, algorithms that are capable of predicting behaviour have to be used, especially when the variables do not allow, for reasons of volume, human decision-making, or make it ineffective due to the time required to make a prediction.

It is then when one will be able to speak of predictive artificial intelligence, when that, and no other, is the objective to be pursued: to predict. In general, artificial intelligence implies that it is the machine that thinks, that it can even learn to think, i.e. *machine learning*, but predictive artificial intelligence goes further. *Machine learning* implies that a machine can learn to classify, cluster and especially compute by developing algorithms based on a previously given set of data. But predictive analytics interprets and, above all, puts into practice all the results obtained —information— from the data provided, which is the precise moment when prediction becomes intelligence.

Predictive artificial intelligence (hereinafter, PAI) is a data analysis method that, unlike AI, allows prediction and anticipation, insofar as the full set of possible scenarios has been simulated, based on all current and past information collected within a given domain. This means that without this data, it would be impossible to model useful and effective predictions. In no case can it be reduced to a mere forecasting process, as the data incorporated into the forecasting equation that enables the generation of more accurate forecasts, also use real-time data. Here one can also distinguish between traditional AI, where data is processed with a previously written program —algorithm— in order to generate results, and machine learning processes, where the program is generated based on the data and its historical results, in an automated and continuous machine learning process. In this way, what is learned may be reused, predicting what will happen next and making it possible to propose specific and appropriate actions to optimise results or achieve objectives.

The volume and variety of data, as well as the automation of learning, boost accuracy, and create a robust system. One factor which has not been addressed so far, but which plays an undeniable role in this entire system, comes into play at this point: the data quality. It is certainly worth considering the existence of adjacent factors that distort the data, even intentionally, for example by resorting to counter-intelligence. While it is true that the more internal or external data used, the more accurate the PAI will be, the data quality may distort the results, even if specific scenarios have been taken into consideration and generated accordingly.

So far little progress has been made on the original question of this paper, or at least it may seem so. However, it is perhaps not as far away as it may appear. It is well known that nowadays almost every security application uses biometric systems to protect people and facilities. Armed forces around the world use biometrics to control access to facilities, equipment and IT systems, above all. Biometric technology used to identify adversaries on the battlefield or in operational terrain is of a more advanced nature. Even cutting-edge biometric technology goes beyond the more traditional realm of defence and plays a role in intelligence. It is clear then that biometrics goes far beyond what has been its main objective: to recognise a person's identity for the purpose of prohibiting or restricting access, based on whether they are authorised and their level of authorisation, and if not authorised, prohibiting access to physical spaces within the physical area or virtual environment they are confined to (Illanas, 2024).

These biometric systems are defined by the collection of data from individuals for the purpose of unequivocal recognition, automatically applying a series of techniques to the physical or behavioural traits of each person. But is legislation keeping pace with the technical progress of biometric systems? Clearly, the answer is no, as is generally the case when it comes to technology and personal data.

The current situation may be said to be one of complete legal uncertainty and the reasons for this are none other than the uniqueness of the subject matter, the variety of authorities and "voices" that issue their opinions and doctrine on this matter and the unstoppable advance of technology, which is increasingly sophisticated and intrusive in terms of people's privacy.

Science and technology have brought to the fore the question of what is possible and feasible from a scientific and technical perspective so that, in these times of metaverses and avatars[5], the definitive advent of robots is not surprising, and may even seem obsolete. But, beyond the automation implied by their use in physical or mechanical tasks[6], it is especially interesting when referring to the non-mechanised

5 According to the Royal Spanish Academy of Language or RAE, (RAE 4. M. Inform.), an avatar may be defined as the graphical representation of a user's virtual identity in digital environments. In turn, the Oxford English Dictionary or OED, 1.1992–Computing (originally Science Fiction), recognises "metaverse" as a colloquial term used to describe a representation of reality executed by means of virtual reality programmes, a meaning that has been validated by the DRAE, but not yet included in its Dictionary, accepting that it covers universes based on virtual environments.

6 Automation refers to means by which different processes of production, data management, instrumentation, compilation, etc. may be controlled externally. In short, it is the implementation of machines, computer systems, robots or intelligence

aspect of these tasks, which is their ability to take decisions instead of humans having to take decisions for them. Humans are also interested in intelligent robots.

After so much time among people, they have almost suddenly realised that the fact that a robot is capable of "thinking", even artificially, is due to the algorithm, and under no circumstances is this because of the machine, which is merely a medium, regardless of its configuration. Algorithms have been around for 3,000 years, which makes it clear that there is no absence of human intervention in its origin. Obviously, the moment in which a human being establishes a set of rules that, systematically applied to suitable data, can solve a specific problem, is when we have an algorithm. This is how it has evolved over the centuries until recently. Now, moreover, this algorithm is incorporated into a computerised tool capable of undertaking an amount of data management and processing that would be unmanageable for a human being.

The evolution of computer science together with the variable that is the algorithm has finally led to the generation of AI. Once formulated, technological development means that, based on its initial configuration, this algorithm, which is becoming increasingly complex as a result of technical circumstances, is capable of creating other algorithms. If one stops at this initial stage of the question, it is clear that people are not dealing with a behaviour alien to human beings and, it is therefore, subject to rules determined by them. Even the possibility of progress implies that the human factor has foreseen this possibility, has agreed to it, so that its willingness to "transfer" the decision to the machine is clear. What we will explore below will determine even the possibility of attributing responsibility to the creator of the original algorithm, insofar as they could have, but did not avoid contingencies, deliberately leaving it up to the algorithm to make decisions that were their responsibility.

2 Approaching biometrics from the perspective of AI

It would not be far-fetched to say that AI exists because machines are able to perceive their environment and, consequently, carry out actions that maximise their chances of success in certain goals or tasks. Without going into a comprehensive analysis from the perspective of language, the term "artificial intelligence" is used to refer to a machine that mimics the cognitive functions of human beings, who in turn associate them with other human minds, such as the ability to perceive or reason, but, above all, with the capacity to learn and to solve problems. A more elaborate concept would see it as the recognised ability of a system to correctly interpret external data, learn from that data and use this acquired knowledge to perform tasks and achieve specific goals through flexible adaptation, the latter being the characteristic feature of AI (Kaplan and Haenlein, 2018).

That machines are becoming increasingly capable means that technology once thought to require intelligence will fall outside the definition, just as there are different kinds of

programmes in the different production fields mentioned above.

perceptions and actions, which may be elicited and produced respectively by physical sensors and mechanical sensors in machines; electrical or optical pulses in computers; as well as by inputs and outputs of *bits* and *software* environments, which, having become part of our routine, might seem far from the consideration of AI, but are nevertheless perfect examples of it. Systems control, automated planning, the ability to respond to diagnostics and consumer queries, optical character recognition, speech recognition, and pattern recognition are integrated into everyday reality. Fields such as economics, medicine, engineering, transport, communications and defence, among others, cannot be understood without the presence of AI, and it is even present in leisure by means of different software applications present in strategy games or even in chess itself[7] .

There is no denying the intelligence of AI, but one should not mistake it for human intelligence, simply because the two are substantially different, at least for the time being. For example, AI has no fixed values and is not one-dimensional, which means that it cannot be compared[8]. However, within the context of AI, they cannot be compared with each other, because they are different AI systems, just as substantially different objects cannot be compared from single perspectives or key points. Similarly, it makes no sense to ask which algorithm is smarter, nor does it make sense to ask whether one object is better than another when the two are different. The advocated narrow character of AI undermines this line of discussion[9] .

7 It is necessary to consider that the move towards non-human pattern-based learning models moves AI away from human-like behaviour. This is undoubtedly an advantage, but not without ethical problems, as it may generate results that are unacceptable to individuals even if they are optimal for the machine. A well-known case is that of the AlphaGo Zero robot in 2016, which was trained by a method known as *Reinforcement learning,* where it does not need to learn from human behaviour but is able to generate knowledge from scratch. These learning patterns allow machines to accumulate the equivalent of thousands of years of learning in a matter of hours, which meant that AlphaGo Zero was able to beat the Go world champion by 100 games to zero. If one refers to other major AI challenges such as self-driving, avoiding taking the human factor into consideration will mean that AI decisions may become incompatible with human thinking, thus being rejected by humans. It should not be forgotten that neither ethics nor morality are at the core of AI but are incorporated through training based on human behaviour.

8 It is interesting that even though we are talking about intelligence, it is not possible to apply the Intelligence Quotient (IQ) to AI. IQ compares a subject's ability to learn, to understand, to form concepts, analyse information, apply logic and reasoning, in relation to others. It is informative in nature and therefore reflects the influence of uncommon characteristics that may only be determined in society. Thus, from the perspective of relationships, the presence of isolation, rejection or distancing, even pondering them, can be detected, while at the same time it is possible to appreciate the facilities and/or difficulties encountered in intellectual activities. This would lead us to understand that some achievements by individuals require less cognitive effort than others, or that the same achievements do not require the same level of effort for all subjects. It is absolutely correct to state that IQ is basically a formula for estimating intelligence, which mostly does not respond to a single factor; in fact different standardised tests are used to determine it. Therefore, the measurement of intelligence is in itself questionable, although in any case it should be recognised as having a predictive value when applied to certain functions or behaviours.

9 In understandable terms, one cannot compare a car with a house. They can be evaluated separately and always in comparison with similar objects, but not with each other. Individually (without any comparison) one could only say whether they like the object or not, whether they are satisfied with their use, and so on. It is not that people seek to avoid the eternal question "car or house", it is simply that intelligence cannot compare both objects because of the differences between them. Obviously, depending on the information about a given situation, it would be able to determine whether it is more interesting to buy a car or to buy a house in a specific case, and it could even determine the ideal purchasing system and, from that perspective alone, determine which is not better, but ideal. This is even more accentuated in the case of AI, as its narrow character is derived from the AI's own ability to solve a problem. This leads humans to affirm that the fact that a given AI is capable of finding the solution to a problem does not mean that it has the capacity to solve a different problem. Only by submitting the new problem to its consideration, can one ascertain this capacity, without the result, positive or negative, in terms of recognising the capacity, in turn allowing humans to predicate the same with regard to a new problem.

The use of the term AI by laypersons lacks rigour. Its general use is not possible, precisely because there is no single AI, therefore it would only be correct to express the certain presence of AI, but in a partial manner, rather than to confirm that AI has done this or that.

In this sense, the use of AI in the military domain enables the creation of tools that can collect, process and store biometric indicators, fingerprints, eye scans and facial parameters in order to establish, with the help of databases and AI, indicators of matches when identifying a potentially hostile individual. However, the system should be subject to supervision and rely heavily on the human factor (the latter will decide the criteria to be followed by the system in order to identify subjects, the aspects on which to focus its search, and will also be able to control and deactivate the system in case of error).

Although AI systems have converted devices such as drones and unmanned vehicles into autonomous units (especially in the military), the United Nations and the European Union recommend that they should always be subject to human factors, without total autonomy in their actions[10]. Moreover, current biometric identification systems include AI systems in conjunction with satellites hosting defence systems or are ready to collect and store such biometric data, thanks to the use of *Big Data*; all activities in which the human factor must be involved, both in the programming and in the subsequent control of their execution[11].

The Helsinki Final Act of 1975 already states "the need to contribute to reducing the dangers of armed conflict and of misunderstanding or miscalculation of military activities which could give rise to apprehension, particularly in a situation where the participating States lack clear and timely information about the nature of such activities". Without expressly mentioning a reality that did not exist at the time, this reflection by the Organization for Security and Co-operation in Europe (hereinafter OSCE) may be extrapolated to the current situation if the goal is to reduce the risks inherent to conflicts, including improving transparency in the area of military planning and activities[12]. This is obviously not an explicit reference to the use of AI in the field

10 At EU level, see document 2018/2752(RSP) Resolution on Autonomous Weapon Systems. Similarly, the opinion of the European Economic and Social Committee of 31 May 2017 advocates an approach to artificial intelligence based on human control and a ban on lethal autonomous weapons systems. This ideology may be summed up in recent statements by the UN Secretary-General who has said that "what's most serious is that artificial intelligence is eroding the fundamental principle of human control over the use of force," citing the selection of targets via algorithms to make life-and-death decisions. See: https://news.un.org/es/story/2024/12/1535261

11 The Spanish Data Protection Agency has recently imposed a fine (not yet final) of 200,000 euros on GSMA LIMITED, the organiser of the Mobile World Congress in Barcelona (the world's leading technology conference), for not clearly informing a citizen who attended the event as a speaker about its use of the biometric data obtained from her at the congress itself. The resolution is available at: https://www.aepd.es/es/documento/ps-00553-2021.pdf

12 A key element of the OSCE is the Vienna Document on Confidence- and Security-Building Measures, which promotes confidence and predictability through verification and transparency measures covering armed forces and major equipment systems. The Framework for Arms Control, agreed in 1996, recognised that arms control, including disarmament and confidence- and security-building, is integral to the OSCE's comprehensive and co-operative concept of security The Vienna Document, the Treaty on Conventional Forces in Europe (CFE) and the Open Skies Treaty constitute a web of interlocking and mutually reinforcing arms control obligations and commitments. Together they enhance predictability, transparency and military stability and reduce the risk of a major conflict in Europe.

of armaments, but the continuous reference to the existence of controls, the need for trust and predictability, distances itself from the idea of an autonomous decision making option by weapons systems without ultimate human control.

This leads to the debate around Lethal Autonomous Weapons Systems (LAWS), Autonomous Weapons Systems (AWS), robotic weapons or even killer robots. Again, the question is whether it is necessary, desirable, or essential to set limits and controls on the autonomy of these systems, given the collateral effects of such technological devices, even when they are controlled by operators or controllers, even in compliance with the rules of international humanitarian law (Queirolo Pellerano, 2019).

It is appropriate at this point to make a brief reference to the difference between strong and weak AI. The latter is designed to perform specific and easily predictable tasks, while strong AI has the ability to learn and adapt to new situations. Expressed in other terms, one may consider strong AI as that which is capable of reasoning and making decisions on its own —self-learning— while weak AI simply follows instructions, so that the human factor is decisive in the latter case, both in terms of carrying out instructions and, above all, because of the perpetual capacity for control. A weapons system with a weak AI would be acceptable, as both decision making and control originate in and are implemented by a human being. However, the same will not be true for a weapon system that employs strong AI.

2.1 Intelligent machines

Strictly speaking, an algorithm, regardless of whether it is a formula, a method, even a procedure, in itself does not necessarily have to be AI. As long as the result of its application is the exclusive product of that user-specified formula, it would not be a manifestation of AI. When John McCarthy defined it in 1956, he defined it as the "science and engineering of making intelligent machines", that is, a combination of algorithms designed to create machines with the same capabilities as human beings. If this combination is not completed and the algorithm is limited to the formula that provides results according to its programming, one will be dealing with automation, but not with AI[13].

Ultimately, the defining characteristic of AI is that it makes it possible for machines to learn from their own experience, while adjusting to new contributions and, like human beings, to carry out tasks. This requires three processes: learning (the acquisition

13 One cannot fail to refer to the man considered the father of artificial intelligence. In 1947, Alan Turing's (1912) answer to the question "Can a machine think?" laid the foundations of AI. The publication of this response in 1950 is the first bibliographical manifestation of AI. While the answer is not irrefutable nor absolute, it outlines the general lines along which an answer that combines a certain precision with ease of use should be developed. These lines, the Turing Test, lead to the conclusion that a machine is deemed capable of thought if a human being communicating with the machine and with other human beings is not able to distinguish between their interaction with the machine and with another human being.

of information and the application of rules for the use of information)[14], reasoning (the use of rules to arrive at approximate or definitive conclusions) and self-correction.

These processes occur in all types of artificial intelligence, as every time one seeks to categorise something, it must always be executed taking into account the classifying criterion, if not the lens through which it is observed or, in other words, the subjectivisation of the expert. Without any conceit, but simply for the sake of clarification, it may be said, with relatively little chance of being mistaken, that the manifestations of AI may be divided into two groups. Firstly, there are those that only use logic, as opposed to those that use intuition in addition to logic.

The first, which are the most recurrent, apply algorithms (rational principles of human thought). The second group, which includes intuition, is called "artificial neural networks", whose precursor is Hinton. Similar to the first group, they work with algorithms, but these are designed much like human neurons, so that the machine may learn by itself. This group is possibly better known by its colloquial name "*deep learning*"[15]. In short, in the first case, the algorithm operates on an individual basis, and the result it produces is a direct consequence of said individual operation. Conversely, deep learning contemplates multiple algorithms, such that one algorithm is designed to in turn create other algorithms, thus contributing to learning processes based on the results obtained by one and the others, in what is an entire training process[16].

Within a legal limbo as regards the complete regulatory framework applicable to the use of biometric systems in terms of privacy, the use of AI applications for biometric identification is becoming increasingly common. The regulatory issue of the "custody" of biometric data and the various processing operations to which they may be subjected have only been addressed in a variety of ways from the perspective of data. From applications to detect body language that may indicate the commissioning of a legally inadmissible behaviour (criminal or at least illicit behaviour), to voice analysis to replace the traditional polygraph in job interviews, especially in senior management positions or positions that require specific qualifications, and where it is necessary to reduce the risks inherent to the candidate seeking to occupy the post.

14 Here, in the learning process, is where the question of the use of data becomes important and where all data protection regulations are manifested, insofar as the data are of a personal nature, being a maximum manifestation of the links between AI and the law.

15 Also known as connectionist systems, it is characterised by the fact that neurons, forming a neural network, are connected to other neurons through links that determine the effects on adjacent neurons. Thus, these systems learn and train themselves, rather than being explicitly programmed, and excel in areas where solution or feature detection is difficult to express with conventional programming (Hinton, 1912).

16 One of the best known examples is that of trial-and-error algorithms. These include the Newton-Rapshon method. It is a type of recursive "backwards and forwards" search algorithm, which is based on reapplying the result of previous applications, which can be done an infinite number of times. For example, it is used for training computers in games such as chess. Thus, a (recursive trial-and-error) system is set up where the tests performed by the computer build up a series of search paths for solutions. These search paths will generate a subtask tree, where some paths do not reach the solution while others do. In short, it is a system of repetitive tasks that seeks to gradually improve the result by means of "deep layers" . This how neural networks operate through deeper and deeper layers of information to make predictions, solve problems or detect features in objects or situations.

The truth is that humans are facing a situation of reduced legality due to the only certain feasibility of being able to apply data protection regulations (at the European level, unlike other nations such as the PRC, USA, Japan, etc.).

This situation, which is certainly close to alegality, keeps supervisory authorities all over Europe on edge and, far from maintaining common criteria, they occasionally overwhelm the citizen with discretionary resolutions with the catchphrases "in case of doubt, the most favourable interpretation", and must overcome the judgements of "suitability, necessity and proportionality in the strict sense", "a regulation with the status of law is not sufficient", "the need for the processing is not justified", "necessity cannot be confused with convenience", "the current regulation is insufficient" or the use of this technology must be considered "the last resort"[17].

But if data protection has not yet solved the legal problems posed by globalisation and technology, Europe is not going to fare any better with biometric systems and AI.

The *White Paper on Artificial Intelligence - A European approach to excellence and trust* (2020)[18] explains that the collection and use of biometric data for remote identification carries specific risks to fundamental rights, and concludes that in order to address possible societal concerns regarding the use of AI and in order to avoid fragmentation within the internal market, the Commission will launch a European debate on the specific circumstances, if any, which may justify such use, as well as on common safeguards.

2.2 Legal response

As stated above, the law cannot be content to follow reality, reflecting the context, but must be able to respond adequately to the challenges posed by the new scenarios. The law must understand its implications, functioning and uses. However, given the nature of the new reality, one has to anticipate and suggest future applications derived from the computation, calculation and use of AI, in everything that entails an aid to decision-making, especially if it is decided to delegate decision-making to AI itself, as it evolves and approaches human *ratio decidendi* (Hoffmann, 2018).

Following the above discussion, the mere execution of systematic tasks, reproducing mechanisms, where decision-making capacity is circumscribed by specific limits that govern their functioning is what we know as automation, not AI. Certainly, examples such as the Automated Complaints Centre of the Directorate General of Traffic (ESTRADA), which automatically and immediately handles the offences captured by radars or cameras installed on Spanish roads by selecting the images captured by the radars and discarding those that "in its judgement" do not meet the requirements

17 See, among others, COM(2021) 205 final, COM(2024) 28 final.

18 COM (2020) 65 final.

to initiate penalty proceedings with guarantees[19], are highly simple manifestations of AI. The most interesting part, from the perspective of this work, is that it raises the possibility of a robot making its own decisions or even going a step further, developing its own ideas, to the extent that the ownership of these ideas may be enquired, whether one may understand them as a direct consequence of the initial programming, which depends on people or, conversely, at least in part, is the result of the system's own learning via data processing.

Following on from the above example, AI systems, when used for active defence in the military domain, may coordinate and carry out certain pre-emptive attacks virtually autonomously and recognise devices, military elements and individuals.

It would be necessary to determine to what extent technological advances and the growing autonomy of these systems to the detriment of the human factor (in data collection, processing and decision-making), now affect the control of weapons by states. The ability to monitor and process data through AI systems facilitates the monitoring and verification of limits set by international law or agreements between states, while increasing and improving the quality of stored data.

The human factor would be reduced to monitoring and decision-making at the lower levels of the system, as well as controlling the flow of information derived from the implemented systems.

3 Ethics in AI. What is and what ought to be

It is irrefutable that artificial intelligence is one of the most advanced but, at the same time, most compromising technologies of recent times. The numerous applications that help to improve social, economic, traffic, health and educational systems, among many others, should not obscure their many risks, as machines have an automatic character, especially when it comes to applying privacy and data protection rights, which have been protected by other regulations in recent years[20].

19 According to the Directorate General of Traffic itself, as reported on its website, (https://www.dgt.es/menusecundario/dgt-en-cifras/dgt-en-cifras-resultados/dgt-en-cifras-detalle/Evolucion-de-Denuncias-e-Ingresos.-Denuncias-en-funcion-de-la-provincia-y-el-precepto/), the National Centre for the Processing of Automated Complaints handles approximately 1.5 million complaints for traffic violations every year, of which around 40% are usually discarded because the image captured may raise doubts or does not meet the requirements. The system works on the basis of the images taken by the radar or camera, detecting speeding or other traffic offences such as not wearing a seat belt or not respecting traffic signs such as "not stopping at traffic lights", stop signs, etc. The information is then sent via satellite to the processing centre, where the offender is identified by consulting the general vehicle register; the system itself generates the report notification and also automatically notifies the owner of the vehicle.

20 The European Commission itself, in conjunction with the Member States, executed a plan for proper regulation of this particular issue which resulted in the publication of the non-binding "Ethics Guidelines for Trustworthy AI" (European Commission, Directorate-General for Communication Networks, Content and Technologies), *Ethics Guidelines for Trustworthy AI*, (Publications Office, 2019, see: https://data.europa.eu/doi/10.2759/14078). In turn, the Parliament has also approved certain resolutions within the scope of Artificial Intelligence, such as the most recent European Parliament Resolution of 3 May 2022, on artificial intelligence in a digital age (2020/2266(INI)). But the proposal for a regulation that would establish both ethical principles and legal obligations for the development as well the implementation and use of

The existence of unknown, "*opaque, unregulated and irrefutable* algorithms" (O'Neil, 2016) is causing a major setback for citizens' freedoms and real equality.

Iti s not clear how they operate, occasionally people are even unaware of their existence, but the most striking thing is that they are also unaware of their capabilities: the maximisation of the result sought from them may surprise us. By discovering connections and patterns that human beings do not pick up by detecting coincidences and regularities that humans would overlook in the vast amount of data they are trained on, such discoveries are now elevated to results that accurately predict that those coincidences will occur in the future. They serve, then, not only to explain, but also to "predict" and guide human decision-making, even if they do not make such decisions on their own. But they do so based on correlations and the rules of human behaviour that have been called Law and which are based on causality and responsibility.

On the other hand, the data used to train such systems are conveying real information, which also communicates current social biases. If people let AI systems interpret such data as the only data to be considered, will they not reinforce existing inequalities, biases leading to injustice that are offered by the current data?[21]

Technology has been busy providing good and efficient solutions through massive data analysis, computation and algorithms, but have people ensured its suitability to their values of dignity of the person, liberty and duty, equality and solidarity, which should be the principles of all *ius algoritmia*? And, furthermore, have people taken care that such solutions respond to *human rules*? Because, in the end, this is what it is all about: technical solutions, which produce excellent results, are based on a non-causal (*non-responsible*) consideration of human behaviour. The law, the rules of the law of today were built on the assumption of responsibility and causality. Is society heading towards an algorithmic right of simple *correlation*?

At the very least it will be possible to generalise some general legal principles of *ius algoritmia*. Human beings have a right to know about the existence of AI systems that influence their legal position. It does not matter now, whether or not they function by establishing "profiles" in a strictly normative sense. Any decision based primarily or exclusively on the use of AI systems must have, as a prerequisite for its legal admissibility, the possibility that the human logic on which it is based may be challenged. It is therefore a prerequisite that its existence be made public. Even the

artificial intelligence, robotics or other technologies of a similar nature is undoubtedly noteworthy: *Proposal for a Regulation of the European Parliament and of the Council of 21 April 2021 laying down harmonised rules in the field of artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union (COM(2021)0206).* Undoubtedly, there is a clear intention to regulate high-risk technologies, those that are considered to have a significant risk of causing some kind of harm to people or society, especially by breaching fundamental rights or EU standards, which undoubtedly includes AI.

21 The philosopher Daniel Innerarity (2022) has not hesitated to point out that "algorithms are conservative, and our freedom depends on them letting us be unpredictable". It is not a question of denying the outcome of what is ultimately humans' own work, people simply have to adapt to new realities, while also doing the same with procedures and institutions. All of this without renouncing the human essence, such that technology will make tasks easier, rather than the determination of their purpose.

awareness of its existence would not be sufficient; as long as it is not positive, it will not be subject to examination[22].

After transparency, the precautionary principle (prior assessment) is fully consolidated by Community law, which has declared it to be a general principle of Community law (Judgement of the Court of First Instance of 26/11/2002, *Artegodan and Others v Commission)*[23]. Accordingly, not every algorithm will be admissible in law because, for example, its use may end up leading to anti-competitive practices. Thus, this principle would operate in a very simple way, which could be graphically summarised with a basic algorithm: scientific uncertainty + suspicion of harm = precautionary action. The issue is not unknown to Cotino Hueso (2019) and Fernando Pablo and Terrón Santos (2019), who consider ethics as a definitive tool to address the risks of AI with a similar argument.

The application of this principle requires taking into account the unique aspects of this reality, where technology without Law will encounter serious problems in its implementation due to the inherent risk of its use, of which there is a growing awareness. The progressive awareness of the problems linked to AI lead people to rethink, not its undisputed usefulness, but the need, which will end up being unavoidable, to understand how this reality works, in order to control algorithms as far as possible and, when this is not possible, to limit their use (Bostron, 2014). If humans do not

22 With regard to transparency and in relation to the right of access to software used to appoint the members of the committees responsible for assessing the public university entrance exams, Resolution 200/2017, of 21 June, of the Commission for the Guarantee of the Right of Access to Public Information of Catalonia, recognised the claimant's right to access the source code of the software used by the Inter-University Council to appoint the members of the selection boards responsible for assessing the public university entrance exams, for reasons similar to those that led this Commission's Resolution of 21 September 2016 to uphold Complaint 124/2016 and declare the right to know the mathematical algorithm implemented by the said software.It states that:

> " […] the source code of a computer program used by the Administration to appoint members of evaluation tribunals constitutes public information for the purposes of Article 2.b of Act 19/2014, of 29 December, on transparency, access to public information and good governance (LTAIPBG). According to this provision, public information is understood to be 'the information produced by the administration and that which it has in its possession as a consequence of its activity or the exercise of its functions, including that which is supplied to it by other entities subject thereto, pursuant to the provisions of this act'. This definition includes all information produced or held by the Administration in the exercise of its functions, regardless of the language or form in which it is expressed. Public information thus includes not only that which is expressed in natural language (in words, which is the most common), but also that which is expressed through photographs, videos, maps, signs, etc. or through other languages, such as mathematical or, in this case, computer language. Article 19.1 LTAIPBG confirms this broad notion of public information when it provides that 'the right of access to public information includes any form or medium in which this information has been prepared or in which it is kept'. The same follows from Article 13 of the Basic State Law 19/2013, of 9 December, on transparency, access to public information and good governance, when it states that 'public information is understood to be the contents or documents, whatever their format or medium, which are in the possession of any of the subjects included in the scope of application of this title and which have been drawn up or acquired in the exercise of their functions'".

23 Judgement of the Court of First Instance of 26 November 2002 Artegodan and Others v Commission, Joined cases T-74/00, T-76/00, T-83/00 to T-85/00, T-132/00, T-137/00 and T-141/00. The dispute arose over the withdrawal of marketing authorisation for a medicinal product for human use with an anorexic effect. Paragraph 184 of the judgement states:

"It follows that the precautionary principle can be defined as a general principle of Community law requiring the competent authorities to take appropriate measures to prevent specific potential risks to public health, safety and the environment, by giving precedence to the requirements related to the protection of those interests over economic interests. Since the Community institutions are responsible, in all their spheres of activity, for the protection of public health, safety and the environment, the precautionary principle can be regarded as an autonomous principle stemming from the above-mentioned Treaty provisions".

understand the workings of the technological mechanisms on which algorithms are based, it is difficult to justify their results. This leads people to observe that it is equally important to identify the objectives sought to be achieved by their use, as only then will people understand what role regulation should play. Otherwise, any attempt to limit the use of AI through regulations will be a failure by any standard[24].

For example, what would happen if a robot —a deep learning algorithm— were designed for a certain task but, as a result of this task, invented something? Would the result of their work be the property of the purchaser of the robot or of the initial programmer? It is clear that the *software* allows for two rights holders, the initial manufacturer or programmer, and the user who obtains this intelligence that can conduct further programming. From a legal perspective the answer comes to light almost immediately: it will depend on what is agreed in the contract of sale or transfer of use. Thus, situations may arise in which the user only obtains a licence of use and not the ownership of the algorithm itself, or the opposite. But it would also be problematic if people were to consider the robot as having a legal capacity of its own. In such a case, who would have ownership of the invention? The answer can only be approached from the different question of whether the AI has the ownership of the legal person, in which case the dispute will be between the manufacturer, the user or between the robot itself (Eidenmüller, 2017). Until legislation clearly clarifies this issue, it is not possible to say with certainty who the true owner of the discovery is.

4 Limits to artificial intelligence

This issue has already come up before, as shown by the fact that in the middle of the first decade of the 21st century, i.e. more than 15 years ago, the need to control AI from a legal perspective was already being considered[25]. Developments in this area have moved away from those initial pronouncements that liability derives from ironclad

24 Opinion shared by Boix Palop (2007: 145), who advocates for the correct, as well as consensual, identification of what should be the final objectives of the regulation, without forgetting the values which it should serve. This reasoning implies that only if they are aware of the implications, will people be able to draft regulations that program AIs to achieve certain objectives or others. Therefore, in the face of this new third technological and productive revolution, the role of the law must be fully consistent with this need to establish objectives and goals and from there, to try to reorient the functioning of these instruments.

25 Various media outlets at the time reported that the issue had been the subject of more detailed analysis in countries such as Japan and South Korea, to the point that first in Japan and then in South Korea documents were drawn up which, taking up Asimov's basic principles, argued for the clear intention that machines should always be under human control, without the possibility of attributing legal or any other kind of ownership to robots Among others, see the article by Delclos, (2007).

Asimov (1942) laid down the three laws that should govern the existence of robots: «A robot may not injure a human being or, through inaction, allow a human being to come to harm; a robot must obey the orders given it by human beings except where such orders would conflict with the First Law; a robot must protect its own existence as long as such protection does not conflict with the First or Second Law». In conclusion, a robot will do what it is told, but not what is wanted or needed.

The European Parliament's Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) acknowledges the existence of precedents for the adoption of regulatory measures in the field of robotics and artificial intelligence, even with certain positive results, to the extent that certain Member States had tentatively approached the drafting or amendment of legal standards in order to include new technological applications.

human control. But the circumstances are in charge and nowadays it is difficult to claim "algorithmic responsibility" for the developers of certain programmes, especially those that use machine learning (see: https://www.abogacia.es/2018/05/14/ese-algoritmo-el-discriminador/ - _ftn2). The absence of this intended control means that preventive methodologies must be sought to avoid biases in automatic decision-making that could affect fundamental rights[26] and to avoid the existence of pre-programmed and self-executed discrimination[27]. In short, to avoid "unwanted" liability.

Certainly, machine learning machines pose more perplexing challenges to the values embedded in administrative law than the first wave of expert systems. Transparency, responsibility, predictability, equality before the law, even coherence, are fulfilled as long as certain rules prevail, and the specific technology implemented in accordance with them is valid. But the rapid evolution of AI means —note that it is in the present tense— that algorithms are increasingly embedded in opaque decision-making processes, without human intervention, which will make it extremely difficult to challenge them, with the obvious loss of guarantees that this entails. This leads to the fact that the decision regarding the degree of sophistication of the automation to be implemented must be carefully considered among the elements designing a specific rule to confer decision-making power[28].

AI systems, whether used by public authorities for citizens' security or by the military to guarantee the effectiveness of their actions, have been the object of international regulation and of demands to limit their capacity to act. In 2017, the United Nations Security Council issued Resolution 2396/2017, which is mandatory for all States Parties and obliges them to implement biometric data collection systems in order to improve security measures to prevent terrorist attacks. These systems involve better identification of citizens (facial scanners, fingerprints), as well as the use of cross-data systems between government and security agencies and organisations, at national and supranational levels.

Also at European level, in 2021 the European Union (EU) declared itself in favour of strict regulation of the collection of biometric data in public spaces as a threat to security[29].

26 Creating systems that learn automatically, that is to say, identifying complex patterns in millions of data items, means that the algorithm reviews this data and is capable of predicting future behaviour, transforming them from reactive to proactive. In this context, it also automatically implies that these systems improve autonomously over time, without human intervention.

27 A good parameter for legislators would be to try to review the presentations and subjects addressed at Neural Information Processing Systems, one of the major international meetings on algorithms and information processing. Setting limits on the requests made by the system, something similar to what Amazon ML does (see: https://amzn.to/2TDQQPF) may also be considered.

28 For further information, see Pasquale, 2015: 147. The 2004 Report of the Australian Administrative Review Council, particularly highlights that already long before 2000, administrative bodies used to resort to automated processes in relevant decision-making, often without even mentioning it in the decision itself.

29 C(2021) 32 Commission Implementing Decision (EU) 2021/27 of 7 January 2021, on the request for registration of the European citizens' initiative entitled "Civil society initiative for a ban on biometric mass surveillance practices".

In Europe, biometric techniques are assessed by the 1950 European Convention on Human Rights and Fundamental Freedoms (hereinafter ECHR). This type of technology presents certain vulnerabilities, such as the reasonable doubt that arises in relation to its possible failures, whether provoked or fortuitous. Moreover, the ethical concerns inherent to the use of a fully autonomous system and the implications of misidentification of persons (at civilian or military level) are shown: for example, AI failures to identify certain racial or sexual patterns are common, or the relative ease with which the AI can be "fooled" when identifying the biometric data obtained[30].

4.1 Responsibility

Beginning from the premise that law and society are not rivals —on the contrary, they are symbiotic and inseparable elements—, it must be noted that law is necessary for social development and evolution. Therefore, it cannot limit itself to providing answers but must also remove obstacles and facilitate scientific and technological progress, which is only possible through regulatory anticipation. Achieving this is a matter of flexibility rather than adaptation[31].

Flexible rules, based on logic and up-to-date general principles, will offer this safeguard to society so that it does not lose the legal guarantees it requires for its normal development.

Among these legal guarantees is obviously being subject to the principle of legality, which is as much the basis for the prominence of the law as fairness, transparency, rationality and responsibility.

This article has already focused on the issue of ethics, accompanied by transparency and rationality from an ethical perspective. Next, the question of responsibility as applied to AI will be discussed. It is worth remembering that algorithms serve not only to explain, but also to "predict" and guide human decisions, if not to make them themselves. But they do so on the basis of correlations and the rules of human conduct which, having been called law, are based on causality and responsibility.

30 A simple test is enough to confirm this. If one searches for an image of a successful man or a beautiful woman on any search engine, the results are much more likely to show images of Caucasians, thus excluding racial diversity. Though a simple example, it is a significant one, as it demonstrates how algorithms display biases towards certain racial groups and discriminate against or undervalue others.

31 "The law must develop in greater proportion to technical progress, increasing its role and its responsibility. The law-technology dilemma can bring factors that threaten the already existing divergence between technical-economic and legal development. Showing this has been one of the aims of this work, which I conclude with the awareness that it is only a warning and not a solution". With these words, Villar Palasí (1975) refers to the need for the law to resort to logic to avoid being disconnected from development, taking for granted that development will happen, even with a legal framework that is not ideal for it, although it may be slowed down, with the obvious social harm that this would entail. Therefore, contrary to the opinion of those who only see law as the persecutor, the science of law must be the promoter of scientific and technical development, and by extension, economic development, for the benefit of society.

Technology has traditionally been concerned with providing solutions that are generally valid and positive, through the analysis of massive data, computation and algorithms. It so happens that, in doing so, the appropriateness of these solutions for our values of personal dignity, freedom and equality, solidarity and, of course, responsibility have been set aside, which should be the principles of all *ius algoritmia* (Terrón, 2022). Going further, it can be said with little room for error that humans have neglected to ensure that such solutions respond to human rules, which should have been the main argument to make. Because, in the end, this is what it boils down to when technical solutions producing excellent results are based on a non-causal (non-accountable) consideration of human behaviour. The law, the rules of today, were built on the assumption of responsibility and causality, but society has moved (without realising it?) towards an algorithmic law of simple correlation.

Although the discussed topic is AI, sight must be not lost of the fact that this is not behaviour that is alien to human beings, as has already been made clear. This means that it is humans who set the rules —they develop the source code— and therefore the AI engine's algorithm is subject to human determinations from the outset. There is certainly the possibility of "transferring" the decision to the machine, but it will always depend on the willingness to do so. This is directly related to the possibility of attributing responsibility to the material authors of the original algorithm since they will be responsible for the contingency that they did not prevent with their decision when they could have done so. Deliberation implies the attribution of responsibility, which may even be understood as a manifestation of bad faith by attempting to waive the known responsibility by attributing the decision to a third party, the algorithm in this case. It would not be a case of neglect of duties, nor would it be strictly speaking a delegation of powers; rather, it is particularly aimed at preventing the decision-makers from being liable even though they should be.

If this were about dealing with mere manifestations of automation, the question would undoubtedly be much simpler, since in this case the entity's responsibility for its acts, including automated acts, is determined to be continuous, and these must be based on a specific and known procedure. But since it is not possible, nor is it wise, to equate automation with discretion, since the technological resource of automation is restricted to clearly regulated and very limited scenarios with regard to possible variations, AI poses a challenge from the perspective of responsibility.

It is not time at this point to analyse all possible manifestations of responsibility as far as AI is concerned. But it is possible to state that, for the sake of technological neutrality, the question should be cleared up, even in broad terms, as the impact of AI on society is clear. In this regard, it is a priority to strengthen mechanisms of responsibility and accountability, while guaranteeing the protection of the rights and freedoms of citizens, whether natural or legal persons in their different

manifestations[32]. This can be achieved in only one way and that is by setting constraints on the configuration of the algorithms. Formulas such as algorithm auditing, raising awareness among technological developers —digital humanism— and public evaluation when developing algorithms can serve as mechanisms for achieving the explicability of the algorithm, without the need to go to the extreme of liberalising the algorithm in order to take a break from its intellectual property.

The understanding of the algorithm is crucial in order to attribute responsibility, since only when it is clear that there has been no neglect of duty, in that there was no will to transfer responsibility for the decision generating the circumstance, can liability for the circumstance be avoided, and the algorithm itself be held liable, which may be equated to a cause of *force majeure*. In other words, the determination of the end is something that must be inherent and exclusive to the human essence. The goal may be more or less ambitious and, if it involves "using" the algorithm by not determining the goals, which should have been determined by the programmer, the responsibility will continue to be the latter's, and it will not be useful to blame the algorithm (Innerarity, 2022).

5 Conclusions

What is presented here is not the result of chance or inventiveness. Many international organisations (United Nations, OSCE, etc.) have expressed their concerns regarding the use of biometric systems and their military application, without ignoring attempts, so far in vain, to regulate this resource. As the issues arising from autonomous AI systems come closer, the main concern is derived from the collection of biometric indicators, such as facial recognition. Lethal Autonomous Weapons Systems or LAWS are the focus of civil society and binding political organisations, such as the EU, are exploring legislation to regulate the use of LAWS and other types of autonomous weaponry based on multilevel coordination through AI. In all of them, the use of biometric data as a means of target identification is an indispensable, but not uncontroversial, element.

Europe and the EU undoubtedly represent a space in the global arena, but are not major players in the global geopolitical scenario. As risky as it may be for the author to make this assertion, the truth is that as long as the United States, China, Russia, even North Korea, Iran or Israel, do not show any interest (indeed they all seem far from doing so, beyond the odd token gesture) in drafting actual legislation regarding LAWS or autonomous drones, the problem is not going to go away[33].

32 For this purpose, see the "Algorithm Audit Guide" produced by Eticas Research and Consulting S.L., available at: https://bit.ly/3hBvtX9.

33 The paper *Principles and Good Practices on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, signed by Australia, Canada, Japan, Korea, the United Kingdom and the United States, was presented at the headquarters of the Convention on Certain Conventional Weapons and the Group of Governmental Experts (CCW and GGE) on Lethal Autonomous Weapons Systems, without advocating a total ban on LAWS, limiting their use to those stated in international humanitarian law.

It is also not legitimate to deny that there are initiatives in the US Congress aimed at assessing the risks involved in the development of this type of autonomous systems, but they do not go beyond a risk analysis and are far from being a standard for the application and regulation of the use of these systems[34].

In Europe, biometric techniques are covered by the generic umbrella of the ECHR, although with limited effectiveness due to the scope of its coverage and relative application, given that the convention does not cover, much less regulate, the use of weapons that involve biometrics for autonomous decision-making, but it is the text that would cover, to date, their use. The members of the Council of Europe, including the 27 EU states, the UK and Türkiye, are party to the ECHR, so the level of protection might seem higher, especially because of Russia's presence until September 2022, but in reality, it is not and has not been the case.

If it were infallible, the problem would be lesser or non-existent, but the truth is that biometric technology is not without its vulnerabilities. At the very least, a reasonable doubt as to the systems' integrity will have to be addressed. The possibility of failure is inherent to any piece of technology. Regardless of the origin, the results may be the same whether the systems failure is caused by malfunctioning or malicious manipulation. Then, if something goes wrong, it had better be the human decision-maker. Even when it may be controlled by setting up technological mechanisms such as double-checking systems, confirmation requirements, etc., which at least keep unintentional failure at bay. Ethical behaviour can be demanded of human beings; of AI, only that it may inherit it from the data it is trained on. Consequently, there must be ethical concerns inherent to the use of a fully autonomous system. Moreover, that would meaning entering into another issue such as responsibility arising from the autonomous error of the AI. Who is responsible, the algorithm, its developer, who would go bankrupt in the case of deep learning, or the system user? There are many possibilities for an answer that may seem simple, but has very delicate implications when humans resort to tools where it is known that ethics does not prevail, expecting moral impunity.

Moreover, AI failures are not exceptions to the general rule. Sexual, racial, ethnic, and other patterns are not foreign to automatic biometric systems, which may be deceived both in the capture of biometric indicators and in the identification of these indicators. Would society accept a system of whose ability to discriminate between military and civilians it were not absolutely certain?

All these questions are beyond the ethical dilemma, or perhaps not. Continuous technological advances cannot be left to develop at will, relying on a system that uses data, especially when these data must be controlled to ensure the feasibility of the outcome precisely because of the quality of the information that has been

34 Congressional Research Service Report R44466, Lethal Autonomous Weapon Systems: Issues for Congress.

provided. Those who advocate intervention, regulation, ethics, etc., are hardly going to come closer to those laxer, distracted moral subjects who do not see, or do not want to see, the risk in the form of arms control.

In an already present future, it is a reality that emerging technology will determine the relationship between states, necessitating arms control mechanisms and agreements. New weapons, higher risk. The greater the risk, the greater the need for prevention and anticipation in order to achieve early warning of attacks, which are increasingly capable of destabilising a state. One solution would be to limit, where possible, the use of such weapons or other non-conventional systems to ineligible users. It is evident it does not work like that. Technology sooner or later becomes accessible, maybe not the latest, but possibly the one immediately preceding it. Even biometric data itself will be subject to transformation. The collection of biometric data will refine its accuracy, thus increasing the reliability of the AI itself, provided that transparency, which is ultimately what guarantees security, is not lost.

Bibliography

Asimov, I. (1942). *Runaround*. USA, Astounding Science-Fiction.

Boyd, A. (2020). Intel Agencies Seek to perfect biometric recognition from drones. *Netxgov*.

Bostron, N. (2014). *Superintelligence. Paths, Dangers, Strategies*. Oxford, Oxford University Press.

Boix Palop, A. (2007). De McDonald's a Google: la ley ante la tercera revolución productiva. *Teoría y Derecho: revista de pensamiento jurídico*. 1, pp. 124-147.

Cotino Hueso, L. (2019a). Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y *big data* confiables y su utilidad desde el Derecho. *Revista catalana de dret públic*. 58.

—. (2019b). Riesgos e impactos del *Big data*, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho. *Revista general de Derecho administrativo*. 50.

Delclos, T. (2007). Japón y Corea del Sur preparan leyes para regular la conducta de los robots [online]. *El País*. [Accessed: 4 May 2022]. Available at: https://elpais.com/diario/2007/04/19/ciberpais/1176950126_850215.html

Eidenmüller, H. (2017). *The Rise of Robots and the Law of Humans* [online]. Oxford, University of Oxford. [Accessed: 2025]. Available at: https://www.law.ox.ac.uk/business-law-blog/blog/2017/04/rise-robots-and-law-humans

European Commission. (2019). *Directrices éticas para una IA fiable* [online]. Brussels, European Union. [Accessed: 2025]. Available at: https://data.europa.eu/doi/10.2759/14078

European Parliament. (2021a). *Report on artificial intelligence: questions of interpretation and application of international law in so far as the Eu is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice*.

—. (2021b). *Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206)*.

—. (2022). *Resolución de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI))*.

Fernando Pablo, M. M. and Terrón Santos, D. (2019). Sobre la gobernanza de la inteligencia artificial. In: Guayo Castiella del, I. and Fernández Carballal, A, (coords.). *Los desafíos del derecho público en el siglo XXI: libro conmemorativo del XXV aniversario del acceso a la Cátedra del Profesor Jaime Rodríguez-Arana Muñoz.* Insitituto Nacional de Administración Pública.

Gil, A. (2021). Bruselas quiere prohibir sistemas de identificación biométrica remota en espacios públicos` en su regulación de la inteligencia artificial. *El Diario*.

Hinton, C. H. (1912). *The fourth dimension* [online]. Kessinger Press. [Accessed: 2025]. Available at https://archive.org/details/fourthdimension00hintarch/page/n5/mode/2up

Hoffmann-Riem, W. (2018). *Big Data. Regulative Herausforderungen*. Nomos, Baden-Baden.

Illanas García, L. (2024). Fundamentos históricos de la biometría aplicada a la defensa y sus planteamientos éticos. *Historia Actual Online*. 63(1), pp. 199-212.

Innerarity, D. (2022). Igualdad algorítmica. *El País*.

Kaplan, A. and Haenlein, M. (2018). Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence. *Business Horizons*. Bloomington, Indiana University. 62(1), pp. 15-25.

Sayle, K. (2021). *Biometric technologies and global security*. Congressional Research Service.

O´Neil, C. (2016). *Weapons of Math Destruction, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* New York, Broadway Books.

Pasquale, F. (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge, Harvard University Press.

Queirolo Pellerano, F. (2019). Sistemas de armas autónomos letales (LAWS). Reflexiones para un debate [online]. *Revista Política y Estrategia*. 134, pp. 147-170. [Accessed: 2025]. Available at: https://doi.org/10.26797/rpye.v0i134.790

Terrón Santos, D. (2022). *Administración inteligente y automática. Una visión más allá del algoritmo*. A Coruña, Colex.

Turing, A. M. (2012). *¿Puede pensar una máquina?*. Oviedo, KRK.

United Nations Security Council. (2017). *Resolución 2396/2017*.

Article received: October 10, 2024.
Article accepted: January 14, 2025