

Artificial Intelligence Governance in Latin America: amidst State Regulation, Privacy, and Digital Ethics

Daniel Castaño*

Abstract

The objective of this article is to analyze the different models of artificial intelligence governance in Latin America. In particular, the focus will be on the right to explanation about individual automated decisions (“right to explanation”) whenever this right is at a crossroad between rights to privacy and personal autonomy. To that effect, first the regulatory and theoretical grounds for the right to explanation in Europe will be analyzed. Based on that, the analysis will focus on whether that right exists in the Latin American scenario and how the digital ethics will play a decisive factor to define the regulatory environments and the practical implementation.

* Professor of Law at Universidad Externado de Colombia and lawyer at the same institution. LL.M and J.S.D from the University of California, Berkeley. Independent consultant in law, technology and digital ethics.



Introduction

In a recent conversation with Fei-Fei (<https://profiles.stanford.edu/fei-fei-li>) Li at Stanford University, Yuval Noah Harari (<https://www.ynharari.com/>) used this equation to explain how some traditional philosophical concepts are being questioned by disruptive technologies: **biological knowledge multiplied by computing power multiplied by data = ability to “hack” humans**¹. To prevent this, Harari proposes that all individuals should have a personal artificial intelligence system to serve us and our personal interests over corporate or government interests. Although this equation and Harari's proposals are not scientifically backed so far, his proposals bring up complex legal and ethical questions that must be solved in the short term to make sure that artificial intelligence will be there to help humans, and not the other way round.

Stephen Hawking posited that the creation of artificial intelligence could be the most important event in the history of humanity (Hawking, 2018). In this sense, according to the literature, artificial intelligence has the potential to radically alter social, cultural, economic, political and legal relationships (Domingos, 2015). In effect, the advancements on this field could optimize or increase human intelligence, both at an individual and a collective level, to foster creativity, to diversify thoughts and to make more efficient many tasks that take up our everyday personal and work lives (Goldberg and Kumar, 2018; Jordan, 2019). But as pointed out by Barrat (2013) and Bostrom (2014), artificial intelligence could also be our last invention if we do not learn how to prevent and control the risks derived from its fast development and implementation.

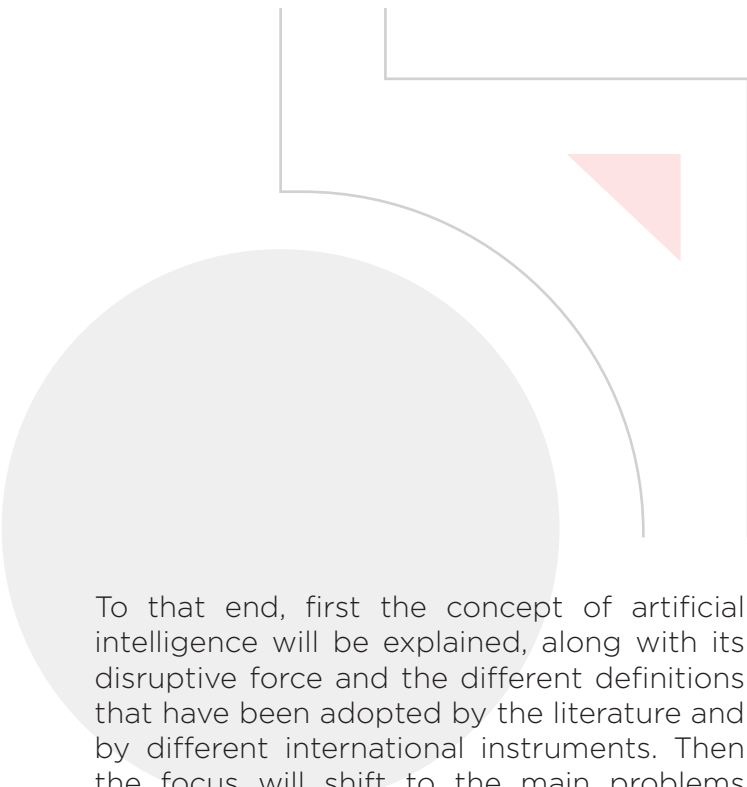
Therefore, this article does not tackle the concerns raised by the potential development of what Bostrom (2014) calls “superintelligence” (also known as general or strong AI). This is understood as a general artificial intelligence system that could exceed all human cognitive abilities in virtually any field. The idea here is to concentrate on legal and ethical issues generated by weak or limited artificial intelligence. In particular, the focus will be in matters related to human rights, democracy and the Rule of Law, and the effects that this artificial intelligence may have on the privacy, agency, autonomy and self-determination of individuals (Katyal, 2019 and Barlett, 2019).

¹ El evento académico se puede consultar en <https://www.youtube.com/watch?v=d4rBh6DBHyw>

It is not the first time that humankind faces the challenge of a complex issue in an uncertain scenario. This has happened with each industrial revolution, giving rise to regulatory transformations in different fields. This article seeks to explore the main legal and ethical challenges posed by artificial intelligence, to then suggest which the most suitable regulatory strategy might be to manage those challenges in Latin America, especially in issues related to the privacy and autonomy of individuals.

According to the doctrine, privacy, agency, autonomy and self-determination are rights sitting at a crossroad between ethical principles and legal regulations, seeking to play a role in the field of personal privacy and autonomy to achieve two goals: (i) protecting personal information in the manner, degree and extent to which the individual decides to share it with others, and (ii) protecting the free and autonomous manner in which individuals take their personal decisions based on that information without any unconsented, undue or illegal external interference.

Given the extension of the topic and the space limits, this article will make special emphasis on the right to explanation on individual automated decisions. The starting point is the principle that this right is at a crossroad between the right to privacy and personal autonomy, and its aim to make sure that individuals know how their personal data are automatically processed by AI systems. Based on that, they may take decisions to fit their life plan without any unconsented, undue or illegal external interference.



To that end, first the concept of artificial intelligence will be explained, along with its disruptive force and the different definitions that have been adopted by the literature and by different international instruments. Then the focus will shift to the main problems related to the governance of artificial intelligence in terms of transparency, accountability, control, and algorithm explainability.

Based on these considerations, the main legal and ethical problems will be described in relation to the automated processing of personal data through artificial intelligence. Then there will be a general review of the regulatory and theoretical bases of the right to explanation in Europe. Then it will analyze if said right exists in the Latin American context and the way in which the digital ethics will play a decisive role to define the regulatory environments and the practical implementation.

Lastly, the importance of implementing regulatory sandboxes in Latin America will be discussed to define the kind, extent, limits and practical application of the right to explanation through the technological experimentation and regulatory innovation through alternative regulatory instruments (see Castaño, 2019).

2

Artificial Intelligence and its disruptive force

As was indicated in the previous section, this study will focus on the ethical and legal challenges derived from the design, development and implementation of the weak or limited artificial intelligence, as opposed to the general or strong AI systems (see Russell, 2017). To do so, it is important to bear in mind the definitions of “artificial intelligence systems” adopted by the High-Level Expert Group (HLEG) of the European Union on Artificial Intelligence and by the OECD, which have been widely accepted worldwide. In the report published on April 8th 2019, this expert group defined artificial intelligence systems as follows:

“Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal.” (HLEG, 2019).

In item I from the Recommendations on Artificial Intelligence from May 22nd 2019 the OECD defines artificial intelligence systems as follows:

“An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.” (OECD, 2019a).

In this context, the disruptive force of artificial intelligence is conditioned by three essential variables: the exponential increase in computing power, the sophistication and emergence of open code algorithms, and last but not least, the daily generation of billions of gigabytes. Not surprisingly, data have been described as the raw material of the Fourth Industrial Revolution, to such an extent that its current value is higher than that of oil (Stephens-Davidowitz, 2017). In this sense, the OECD has pointed out that the collection and processing of countless data has generated and strengthened an ecosystem known as data intelligence, macrodata or Big Data (OECD, 2015).

Data can be personal, as for instance the data associated with someone identified or that can be identified through their habits, behaviors or movements. On the other hand, such information can be institutional, as it is the case of public health, property and taxes (Mittelstadt and Floridi, 2015). According to the OECD, users of different digital platforms and services provide data intelligence to companies for processing, enabling them to automatize processes, to experiment and create new products and business models (OECD, 2015). In this regard, HM Treasury Department in the UK has pointed out that data allow for the development of new digital business models that monetize user reactions (user engagement) and for the transformation of services provided by the State (HM Treasury, 2018).

That is why both public (OECD, 2019b) and private actors (McKinsey Global Institute, 2017 and Shaw, 2019) maintain that artificial intelligence and data intelligence are driving not only a transformation in various productive sectors but also a digital disruption in several industries and in the digital economy, which generates billions in profits. Besides, artificial intelligence could also have a high value and social impact because it could help to fight inequality, corruption, crime and climate change, foster social justice and improve the quality of life of the population (Floridi et al., 2018 and OECD, 2019b). In other words, data have an important social and economic value and their processing through artificial intelligence systems has the potential to radically boost the digital economy, to create new business models and to transform the State along with the services it provides.





Artificial Intelligence Governance: Amidst State Regulation, Privacy and Digital Ethics

The processing of personal and institutional data by artificial intelligence systems to diagnose, describe, predict or prescribe information creates legal and ethical problems at three different levels, although closely linked to the challenges posed by the governance of artificial intelligence systems: (i) transparency and algorithmic accountability, (ii) control of AI systems, and (iii) explainability and algorithmic intelligibility,

Based on the abundant literature on the subject, it is possible to affirm that the main legal and ethical challenges of artificial

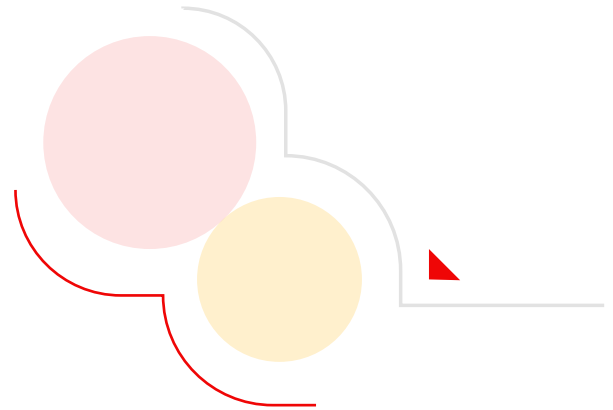
intelligence systems derive, in essence, from situations related to the three types of problems mentioned above, and that these could eventually compromise certain ethical principles governing artificial intelligence systems and violate human rights, democratic values and the rule of law (Keats-Citron and Pasquale, 2014; Keats-Citron, 2008 and Kroll et al., 2017). This does not mean that there are no other problems associated with the massive collection of data and its automated processing by intelligence systems. However, for reasons of format and length, these will be only partially addressed here.

Algorithm Transparency and Accountability

As a human creation, artificial intelligence can reproduce our greatest virtues and also our worst defects. The literature points out that decision-making algorithm models or processes may seem at first to be objective, rational, unbiased and free from all the prejudices typical of human reasoning (Katyal, 2019). However, the truth is that the data and the algorithm models that are processed by in an automated fashion could be full of the same irrational prejudices present in their human creators or programmers, either because they do not realize it or because they take into account information about systemic prejudices or structural discrimination, or simply because they make a mistake in the model design or implementation (Katyal, 2019).

This results in algorithm transparency and accountability, the diagnosis of which is the most complex due to the proprietary nature of those algorithm models and the difficulty to analyze or scrutinize them publicly as a consequence of restrictions related to intellectual property (Katyal, 2019 and Levine 2007).

Control of artificial intelligence systems



It has been pointed out in the literature that the problems related to the control of artificial intelligence systems derive mainly from the complexity of the algorithms and their architecture (Russell, 2019 and Information Society Project, 2017). However, the problem of control should not be confused with the explainability or intelligibility of the decisions made by such systems, a topic that will be further discussed below.

For Russell (2017), the problem of control of artificial intelligence is, in essence, "(...) how to ensure that systems with a highly arbitrary level of intelligence remain strictly under human control". In this author's opinion, the problem of control implies that there could be systems of super artificial intelligence whose actions are by definition unpredictable by simple humans. Such systems may operate under imperfectly and incompletely established objectives that conflict with those of individuals and whose motivation to preserve their own existence in order to achieve those objectives is insurmountable (Russell, 2017).

Similarly, the control problems of AI systems relate to the degree, nature and extent of human intervention in the automated decision-making process. The second edition of the AI governance framework model proposed by Singapore (Singapore Digital, InfoComm Media Development Authority and Personal Data Protection Commission, 2020) is illustrative on this point. This governance framework is structured on a methodology that identifies the risks associated with the operation of AI systems and proposes a strategy to identify the different degrees of human intervention.

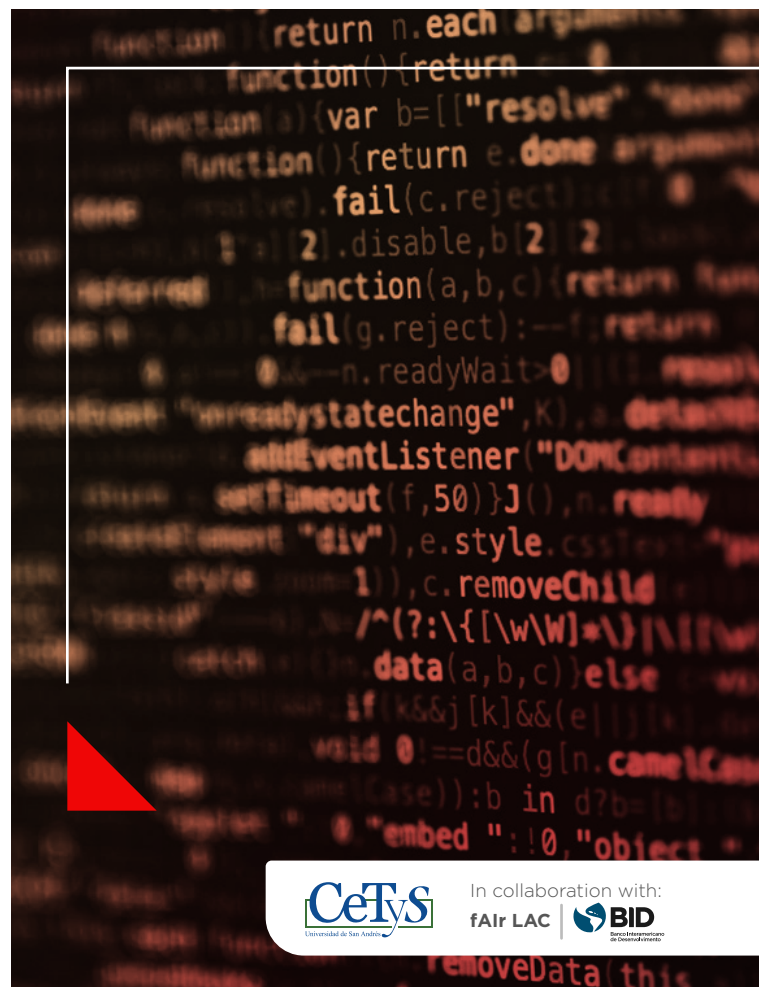
This framework includes, in the first place, the model in which the human actively intervenes and exercises absolute control over the automated decision-making process (Human-in-the-loop), while the IA system is limited to generating recommendations or inputs. An example of this would be an AI system designed to support the physician in the process of diagnosing this or that pathology, even though he/she is the one who has the last word in terms of diagnosis. Second, the framework adopted in Singapore describes the model in which the human does not intervene in any way and has no control over the AI system or its outputs or outcomes (Human-out-of-the-loop). An example of this would be automated profiling for advertising purposes. Thirdly, the document in question identifies the model in which the human actively supervises or monitors the AI system, so that it can assume control in those cases in which it must deal with unexpected or undesirable events (Human-over-the-loop or Human-on-the-loop). An example of this would be an AI system that calculates the best route to move from point A to point B, in which case the human has the control to adjust the necessary parameters to complete the path according to the unexpected circumstances that may arise (Singapore Digital, InfoComm Media Development Authority and Personal Data Protection Commission, 2020).

Algorithm Explainability and Intelligibility

Literature states that one of the main challenges faced by the governance of artificial intelligence lies in the technical difficulty to understand, ex ante or ex post, the way in which an algorithm causes a certain result (The Information Society Project at Yale Law School & Immuta). It explains that one of the main features of machine learning is its capacity to analyze great amounts of data and identify behavior patterns that can even be unknown by the human mind. Then, based on this learning, it applies these identified behavior patterns to different situations that they have not been explicitly programmed for. This implies that programmers will not need to manually incorporate explicit rules for any and all situations that the machine pretends to analyze –which is not only a complex human task but also technically tedious and very expensive.

In this context, Floridi and Cowls (2019) point out that algorithm explainability is supported on two key pillars. On the one hand, it gets the “epistemological meaning of ‘intelligibility’ (to answer the question ‘how does it work?’)”, while from the other part it encompasses “(...) the ethical meaning of accountability (as an answer to the question ‘who is accountable for the way in which it works?’)” (Floridi and Cowls, 2019). Other authors (Lehr and Ohm, 2017; Selbst and Barocas, 1918) posit that explainability problems of machine learning algorithms are due to inscrutable and non-intuitive rules that govern decision-making processes, into which this algorithm architecture is incorporated.

The literature explains that the inscrutable nature of machine learning refers to “(.) a situation in which the rules that govern a decision-making process are so complex, so many and dependent on each other that they challenge any practical inspection and resist any attempt to understand them” (Selbst and Barocas, 1918). Further, it is indicated that the non-intuitive aspect of machine learning lies in “(.) the incapacity to structure a sensible story that can account for the statistical relations of the [algorithm] model”. This means that, although it is possible to spot the statistical relations the algorithm is based on, “(.) these relations may question the intuitive expectations related to the relevance of some criteria that are at the basis of the decision [made by the machine]” (Selbst and Barocas, 1918).



4

Main Ethical and Legal Challenges of Artificial Intelligence

All the situations described before about the governance of artificial intelligence suggest that due to its disruptive force, it gives rise to a high degree of uncertainty when it comes to its ethical and legal consequences. For instance, from an ethical perspective, Floridi and Cowls (2019) explain that algorithm accountability, transparency and explainability are closely related to safeguarding the ethical principles of benevolence, no harm and autonomy that should govern artificial intelligence systems. These authors state that the only way to check if these systems will be benevolent and will keep the autonomy instead of undermining it is precisely by fully understanding the way in which this system operates and identifying who will be responsible for its undue functioning (Floridi and Cowls, 2019).

From a legal point view, the doctrine has identified that transparency, accountability and explainability issues could have legal consequences in different fields such as the labor market, competition, intellectual property, privacy, civil and criminal liability, human rights and the Rule of Law, among others (see O'Neil, 2016; Rubinstein, Lee and Schwartz, 2008; Zarczy, 2011; OECD, 2019a). For instance, there are several different legal viewpoints and opinions about the legal nature of data, its processing, property, and control and about the nature, degree and extent to which those data can be shared or transferred. For these reasons, the academy and different international bodies maintain that general personal data protection regulations are not enough to safeguard the right to privacy from the challenges posed by the automated data processing through artificial intelligence systems (see Tene and Polonetsky, 2012; Tene and Polonetsky, 2013; Crawford and Schultz, 2014; Katyal, 2019; Solove, 2001; Russell, Dewey and Tegmark, 2015; HM Treasury, 2018).

Further, the literature has pointed out that another legal effect is the automated perpetuation of systemic prejudices and structural discrimination (Katyal, 2019), problems to comply with explainability requirements demanded by the Fair Credit Reporting Act and the Equal Credit Opportunity Act in the United States and those demanded by the GDPR in the European Union (Selbst and Barocas, 2018), discrimination to access credit and the financial system due to the implementation of artificial intelligence in FinTechn products or services (Bartlett et al., 2019), the violation of the right to due process by scoring systems executed by artificial intelligence that may compromise the access to the financial, labor or housing system (Keats-Citron and Pasquale, 2014), and the

discrimination derived from the application of data mining technology and artificial intelligence to create profiles that may optimize the fight against terrorism (Rubinstein, Lee and Schwartz, 2008), among others (O’Neil, 2016).

Artificial intelligence, data intelligence and privacy

The regulatory framework in force in Latin America will be reviewed, in order to determine whether there are any regulations governing the design, development and implementation of artificial intelligence systems, the processing of data through such systems, and their possible consequences on human rights, democracy and the rule of law. However, it should be clarified that this will not be a general and/or exhaustive review, but limited to the subject matter of this brief. A normative inventory will then be made to ascertain whether or not there are legal norms of a constitutional, legal and regulatory nature regulating aspects of the governance of artificial intelligence such as accountability, transparency, control and algorithmic explainability, and their relationship with the human rights to privacy and autonomy. On this basis, it will be determined whether there are currently any legal norms on the governance of artificial intelligence systems and the automated processing of personal and institutional data carried out by them, and on decision-making based on descriptions, predictions and prescriptions made by machines.

However, although some specific examples of domestic regulations will be cited here to

illustrate the arguments made, it is not intended to conduct a comparative law analysis of the regulation of artificial intelligence systems in various countries. Hence, the presentation does not focus on any particular nation, but rather, given the normative nature of the regulations, it is assumed that they are compatible with any rule of law structured under a constitutional order committed to democratic values, the principle of legality, the separation of powers, and the protection of human rights.

The first thing that should be pointed out is that in Latin America the design, development, and implementation of artificial intelligence systems does not operate within a legal vacuum. As in the case of any scientific, industrial, or commercial activity, artificial intelligence systems are subject to a variety of regulations of different kinds, including those pertaining to the democratic principles of the rule of law; human rights; the regime for exchanging data messages; technological neutrality; intellectual property; consumer protection; competition; protection and processing of personal or institutional data; and tax law, criminal law, and civil liability, among others.

As has already been indicated in this document, the automated personal and institutional data processing through artificial intelligence systems to describe, predict or prescribe information gives rise to many doubts related to the legal system applicable to said data to protect privacy.

/ Under this premise, the most recent reforms introduced to the general data protection system in Europe will be described. Then, based on these regulations, the focus will be to analyze the way in which some Latin American countries have recently incorporated or are about to incorporate similar regulations into their internal legal systems.

The Right to Explanation on Individual Automated Decisions in Europe

The European General Data Protection Regulation (RGPD (<https://gdpr.eu/>)) is an essential reference in terms of data protection because it contains specific rules on the automated processing of personal data. In particular, Section 4 from Article 4 sets forth the following provisions concerning “Automated individual decision-making, including profiling:

- 1.** *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*
- 2.** *Paragraph 1 shall not apply if the decision:*
 - a.** *is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
 - b.** *is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
 - c.** *is based on the data subject's explicit consent.*
- 3.** *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*
- 4.** *Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*



There have been many debates on whether there is a right to explanation on individual automated decision-making on the GDPR, applicable on the cases in which personal data are automatically processed by an artificial intelligence system without any human intervention. At first, Goodman and Flaxman (2017) posited that the GDPR created a “right to explanation” when a decision is made in an automated manner based on the processing of personal data. However, these authors did not go into further detail on the grounds, nature and structure of such right.

On the other hand, Wachter, Mittelstadt and Floridi (2017) denied the existence of the right to explanation on the GDPR, given how ambiguous the text of this regulatory document is. Instead, based on an interpretation of articles 13, 14, 15 and 22 of the GDPR, these authors conclude that there is a “right to be informed” about how an artificial intelligence system works which automatically processes personal data to produce a decision without human intervention. The conclusions reached by Wachter, Mittelstadt and Floridi (2017) must be analyzed in context, which may be made easier by the classification of different explanations that an individual may demand about how an artificial intelligence system works.

Said explanations can be of two types: (i) about how the system works and (ii) about specific decisions. On the one hand, these authors believe that the way the system works encompasses the “(...) logic, meaning, foreseen consequences, general functioning of an automated decision-making system such as its technical specifications, decision trees, predefined models, criteria [and] classification structures (.).” On the other hand, the explanations about the specific decisions may fall on “(.) the reasoning, drivers and individual circumstances of a specific decision adopted in an automated manner, such as weight factors, the rules of the decision generated for a specific case by a machine, [the] reference information or [the] profile groups.”

Wachter, Mittelstadt and Floridi (2017) also propose an additional classification of the moment in which the explanations and the automated decision-making process are realized. For these authors, the explanations are ex ante when they are presented before that moment, so they can only refer to the functionality of the system and not to the specific decision. In turn, explanations are ex post when they are presented after the individual automated decision-making, and in this sense they could refer both to the functionality of the system and to the specific decision.

In order to understand the extent to which this debate on the existence of a right to explanation exists in the GDPR, it is worth presenting the position adopted by Selbst and Powles (2017). These authors indicate that there is no provision in the GDPR that clearly establishes a right to explanation on individual automated decisions. However, they do posit that there is a right to obtain “significant information on the logic applied” in the individual automated decision-making pursuant to the provisions set forth in article 13 (2)(f), which arises from a functional and flexible interpretation of articles 13, 14 and 15 of the GPDR.

Although the positions exposed so far about the existence of a right to explanation on automated decisions are reasonable, all seems to point at the fact that the controversy on interpretation was settled based on the guidelines on individual automated decisions and profiling issued by the Working Party of Article 29 dated February 6th 2018². Considering these guidelines and also a vast interpretation of articles 13, 14, 15 and 22 of the GPDR and its whereas clauses, Margot Kaminski (2019) maintains that there is no doubt that there is a right to explanation about an individual automated decision taken as a measure of algorithm accountability.

It is worth considering some clarifications about the exercise of this right. Pursuant to article 22 of the GPDR, the literature and the Working Party of Article 29 have pointed out that the right to explanation on individual automated decisions can only be exercised when the decision is “only based on the automated treatment, including profiling” which causes “legal effects” or “affects it significantly in a similar way.”

Considering the first requirement mentioned, the Working Party of article 29 pointed out that the right provided by article 22 of the GPDR can only be exercised when the decision causes “seriously significant” effects, and it provided some criteria that help to determine what that means. For instance, the Working Party mentions that among those decisions there are some which affect financial situations, the access to health or to education, which deny access to a job or which may put an individual in a “seriously disadvantaged position.”³

As regards the second requirement on human intervention, the Working Party indicated that for the decision to be subject to article 22 the human intervention needs to be significant, meaning that it must be “made by someone with authority and skills to change the decision.” To do so it will be necessary to have access to information that goes beyond the products or results generated by the algorithm⁴.

² See Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making And Profiling For The Purposes Of Regulation 2016/679, 17/EN, WP 251rev.01 (Feb. 6, 2018)*.

³ See Article 29, *op cit*.

⁴ *Ibid*.

The right to explanation on individual automated decisions in Latin America

Whether the right to explanation on individual automated decisions is in place all across Latin America is the focus of this section. To do so it will study the Lei Geral de Proteção de Dados Pessoais [General Personal Data Protection Law] from Brazil (LGPD) dated 2018, the Argentine Bill on Personal Data Protection [Proyecto de Reforma del Régimen de Protección de Datos Personales] and the Bill on Data Protection [Proyecto de Reforma de Ley de Protección de Datos] from Chile.

In Brazil, the Lei Geral de Proteção de Dados Pessoais (LGPD) dated 2018 (<https://lgpd.com.br/home-eng>) is structured pursuant to the GDPR and the California Consumer Privacy Act dated 2018. In particular, its article 20 refers to the automated processing of personal data:

“Data subjects are entitled to request a review, by a natural person, of decisions made only based on the automated processing of personal data that affects their interests, including of decisions designed to define their personal, consumption and credit profile or the aspects of their personality.”

By reading this law, it is possible to infer the existence of a right to explanation on individual automated decisions. In fact, paragraphs 1st and 2nd of that article indicate that the person in charge, upon request of the data subjects, must inform them about the criteria and procedures used to make an automated decision. If the person in charge evokes the protection of industrial secrets to refuse to provide information, it is still possible to request an audit by the national authority.

⁵ El Proyecto de Ley se puede consultar en: https://www.argentina.gob.ar/sites/default/files/mensaje_nde_147-2018_datos_personales.pdf

In Argentina, the Bill on Personal Data Protection also referred to the automated treatment of said data for the production of individual decisions⁵. Article 28 of said bill defined the rights of the data subject on automated decisions in the context of the information content:

ff *Information Content. The information shall be provided clearly, free from coding, and in that case, it shall contain an explanation of the terms used, in a clear language accessible for the average population, and it must refer to:*

[...] (h) The existence of automated decisions, including the creation of profiles mentioned in section 32 and, at least in those cases, significant information about the logic applied, which shall not affect the intellectual rights of the Data controller.”

Section 32 of this Bill sets forth the following provisions:

ff *“SECTION 32.- Personal automated valuations. The data subject has the right to oppose to being object to a decision based only in the automated treatment of data, including profiling, which may cause harmful legal effects or may affect him or her significantly in a negative way.*

The data subject shall not exercise this right if the decision:

(a) Is necessary to enter into or execute a contract between the data subject and the data controller in charge of the treatment;

(b) Is authorized by law;

(c) Is based on their express consent.

In the cases mentioned by subsections (a) and (c), the data controller must adopt suitable measures to safeguard the rights of the data subject.”

It is worth mentioning that the wording of the above-mentioned sections 28 and 32 of the Bill is closely related to articles 13, 14, 15 and 22 of the GDPR. In effect, the wording of section 28 is similar to that of article 22 of the GDPR, so it can be inferred that it contains the structural pillar of the right to explanation on individual automated decisions.

In Chile the Bill on Data Protection⁶ contains several provisions which make it possible to establish the existence of the right to explanation on individual automated decisions. Article 8 of this bill sets forth the following:

ff "ARTICLE 8.- Right to opposition. The data subject has the right to oppose before the data controller to a specific or certain treatment of personal data he or she may be concerned with, in the following cases:
(...)
(c) When an automated treatment of their personal data is made and decisions are adopted which imply a valuation, evaluation or prediction of their behavior made only based on this kind of treatment, except for the provisions set forth in article 15 ter herein."

In this sense, article 15 ter of this bill points out the following:

ff "Article 15 ter. – Automated treatment of large volumes of data. The data controller may establish automated procedures to treat and transfer large volumes of data, provided these safeguard the rights of the data subject and the treatment is related to the purposes of the participating individuals or entities.

The data controller has the right to request the data controller that no decision that may **significantly affect him or her** (highlighted in the original) shall be adopted exclusively based on the automated treatment of their data, unless it is necessary to enter into or execute a contract between the data subject and the data controller, there is a prior and express consent by the data subject of if provided for by the law."

⁶ E The Bill is available at: <http://www.informatica-juridica.com/proyecto-de-ley/proyecto-ley-proteccion-datos-chile-abril-2017/>

It must be pointed out that the wording of the article in the Chilean bill is different from that of articles 13, 14, 15 and 22 of the European GDPR. In effect, article 15 ter. seems to contain a right to opposition to the production of individual automated decisions that cause a significant impact, rather than a right to explanation on said automated decision. Unlike the GDPR, as well as the new data protection law in Brazil and the

reform project in Argentina, the data protection reform project in Chile apparently does not contain the right to know the logic applied in the automated data processing for the production of an individual decision. However, it will be necessary to wait for the final drafting of the bill to be approved by the Chilean Legislature.

In any case, the projects that are in the legislative process in Argentina and Chile still have a long way to go. Once the final texts are approved, it will be necessary to study the way in which the Brazilian, Argentinean and Chilean data protection agencies (DPAs) will interpret these provisions in order to determine whether they will closely follow the interpretation of Article 22 of the RGPD made by the Article 29 Working Group, or whether a different interpretation will be made there that restricts or extends the algorithmic liability derived from the automated processing of data by artificial intelligence systems.

The development, design and implementation of digital services and/or business models that incorporate the automated processing of personal data through AI systems must fully comply with the Constitution and laws currently enforced. Under this perspective, the design and implementation of said systems must be subject to the legality in its widest dimension, i.e., a set of conventional, constitutional, legal and regulatory rules.

Likewise, digital ethics is performing a decisive role to interpret and update the current regulation, while it allows the public and private sectors to take a step beyond legality to protect the right of all individuals to take their own decisions in an autonomous, informed manner without undue, unconsented or illegal interferences.

As was indicated at the beginning of this document, the High Level Expert Group on Artificial Intelligence of the European Union (HL-Expert Group \ or HLEG) has recently published some ethical guidelines (<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>) to foster a trustworthy design, development and implementation of artificial intelligence systems. These EU guidelines are supported on the premise that trustworthy artificial intelligence systems must be: (i) legal, (ii) ethical and (iii) technically robust.

This report clearly states from the very beginning that artificial intelligence systems must fully comply with any and all laws and regulations in force. However, the report does not mention the minimum regulatory standards to which the design, development and implementation of AI systems are subject. Neither does it suggest any kind of strategy or method for those systems to duly comply with applicable regulations. Once this has been clarified, the report emphatically points out that it will only revolve around the guidelines on the ethical and technical aspects concerning any trustworthy AI system.

The HLEG maintains that trustworthy AI cannot be achieved by only complying with the law but that it is necessary to make sure that these systems are subject to ethical principles and values. According to HLEG, this is so because laws may lag behind other challenges posed by the hectic development of new technologies, they may not be suitable to solve some issues or they may follow a different pace from that followed by ethical rules⁷.

The HLEG also indicates that trustworthy AI systems must be technically and socially robust to make individuals and society certain that these systems will not cause undesired harm. To do so, the expert group suggests that AI systems should operate safely, reliably and under certain safeguards to prevent any adverse impact on individuals and society.

The HLEG maintains that an ethical artificial intelligence must “(...) help people to make a better, more informed choice depending on their goals. It must be an enabler for a thriving, egalitarian society, supporting human intervention and essential rights without decreasing, limiting or deviating human autonomy” (HLEG, 2019). In order to make sure these ideals are met the EU HLEG points out that a trustworthy artificial intelligence must be supported on four ethical principles: (i) respect for human autonomy, (ii) harm prevention, (iii) justice and (iv) explainability (HLEG, 2019).

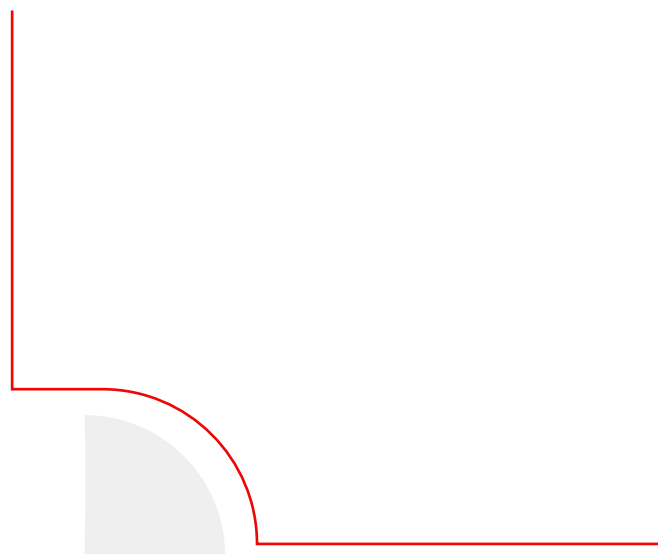
Likewise, the OECD Council Recommendation on Artificial Intelligence (OECD, 2019a) points out that the development and implementation in affiliated countries must abide by the Rule of Law, human rights and democratic values. To do so, the development and implementation of artificial intelligence systems must respect freedom, human dignity, privacy and data protection, as well as equality. It should also prevent discrimination and foster diversity, social justice and labor rights.

⁷ See p. 7 of the EU's ethical guidelines report



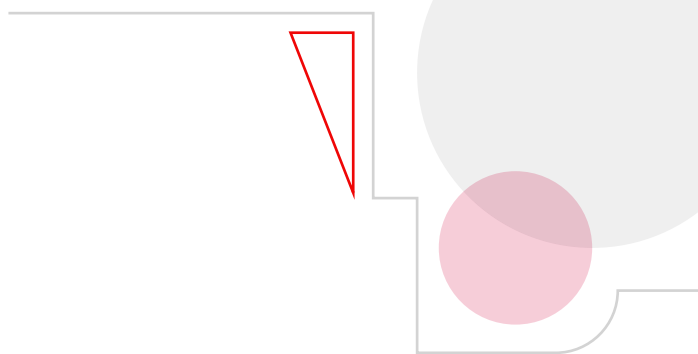
In this context, the OECD (OECD, 2019a) recommends a development and implementation process of artificial intelligence systems that pursue ends that benefit people and the planet, expands human capacities and drives the inclusion of marginalized populations, reduces economic, social and gender inequalities and protects the environment.

In this order of ideas, the European Union and the OECD have maintained that the process of artificial intelligence system design, development and implementation must comply with four ethical principles: (i) transparency, (ii) accountability, (iii) control and (iv) explainability. Based on these recommendations, it is suggested that contracting entities should conduct any necessary studies and analyses to make sure that the digital goods or services acquired to manage or provide an activity or service to be delivered by an administrative authority must comply with those legal and ethical principles. Of course, this is an additional requirement to the one that establishes a strict compliance with the democratic principles of the Rule of Law.



However, this is not only achieved by designing written procedures, rules and protocols. Any State under the Rule of Law, as well as the democratic principles on which it is supported, requires the design and implementation of **X-by-design (X= legality, privacy or digital ethics) and by default** tools and methods to incorporate legality, privacy and digital ethics into the technologies, operations and architecture of digital goods or services and/or business models that apply the automated processing of personal data through AI systems⁸.

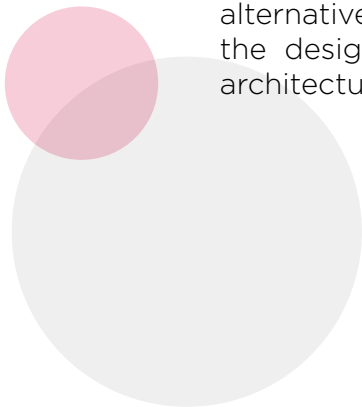
In fact, the literature explains that the X-by-design and by default tools or methods mentioned above are not an add-on to the design, development or implementation of the digital good or service (Cavoukian, S.f.). The main consequence of this is that the legality, privacy and digital ethics become an essential default element of the functional feature of the digital product or service provided by a public or private agent. As a result, this element should be an inherent part of the digital good or service, but it should not compromise its functionality or aptitude to comply with the aim they pursue (Cavoukian, S.f.).



⁸ This section collects a large part of the ideas that the author has presented in other scenarios (Castaño, 2019b). Based on this legal study conducted by the author, the Bogota City Hall issued the District Guideline No. 10 on December 17th 2019, which is only binding to the Capital District authorities.

Therefore, the legality, privacy and digital ethics should be fully integrated into the technologies, operations and architectures of the digital goods and services in a holistic, integrative and creative way. Considering the research studies and proposals by Cavoukian (S.f.), the x-by-design tools or methods should be as follows:

- ▶ **Holistic:** The design, development and implementation of x-by-design tools and architectures must consider all the visions, contexts and circumstances derived from the different disciplines.
- ▶ **Integrative:** The technology is a space where all visions and interests present in a pluralistic democratic community must coexist. It is recommended for all the interested parties to be consulted in terms of the design, development and implementation of those tools or methods in order to achieve a balance between all the different stakes at play in the automated processing of personal data through AI systems.
- ▶ **Creative:** The design, development and implementation of X-by-design tools or architectures must be creative because for a full integration of values by design (legality, privacy or digital ethics) it may be necessary to revamp the existing technical options. On occasions the current alternatives are unacceptable or not enough to meet the goal. That is why the design, development and implementation of X-by-design tools or architectures should always be at the avant-garde.



6 **Regulatory and Ethical Sandbox Initiatives**

In this order of ideas, the structuring and start-up of regulatory sandboxes could be decisive to the interpretation, implementation and update of currently enforced regulations on personal data protection, because it would allow the DPAs and other stakeholders to discover, through regulatory innovation and experimentation, the best way to regulate the right to explanation on individual automated decisions without compromising innovation.

These initiatives are the best scenario for the design, development and implementation of digital X-by-design tools and architectures, since they make it easy to experiment beyond the compliance with the spirit of the law. They allow public and private actors to introduce innovations to protect essential rights to privacy, due process and personal autonomy. This can be achieved not only through the authorizations to try technologies and business models that incorporate the automated processing of personal data through AI systems without being subject to currently enforced regulations, but also by creating and trying out experimental regulatory sandboxes to measure their real impact on said services and model businesses.

It is worth remembering that these sandbox initiatives are to be considered an area for the testing of regulatory proposal that is equipped with an open participation structure, where the public sector, companies and citizens define the best regulatory framework for a certain technology. The idea is to encourage a safe environment to experiment, gather experiences and try new technologies or business models that entail a systemic risk without being hindered by any existing legal rigidity.

Under this scheme, private parties are not subject to fines and/or sanctions, nor are they held accountable in the traditional sense as the scenarios for regulatory proposals are being defined. Thus, it is possible to create new rules and to facilitate the access to consumers in a controlled environment, which makes it possible to loosen or later define the public policy in the real world (Jiménez and Hagan, 2019).

The notion of sandbox initiatives⁹ attempts to redefine the way in which the State participates in the creation of public policy. The idea is not to talk about governability anymore but about governance, since the decision-making process entails open participation and experimentation processes that foster feedback in several society sectors.

So the implementation of this scheme must be done in stages and taking into account that this is an experimentation area where a regulation prototype is made. The aspects that must be considered to begin this initiative are: (i) objectives, sector and purpose of the sandbox zone; (ii) guidelines to determine who participate in this initiative and which ones are the enabling requirements to do so; (iii) access restrictions to the sandbox; (iv) nature of the legal action that can be used as a regulatory exemption and as a relevant authority and its limits; (v) evaluation of the sandbox results and possibilities to vary the parameters already established; (vi) informed consent of the participating agents and users.

The main regulatory sandbox proposals are used in the financial sector, probably after the World Bank recognized that “the development attempts based on a prominent State role have failed, and so will those to be attempted without it” (World Bank, 1997).

The first regulatory sandbox environment took place in the financial sector in the United Kingdom, where management and consumption companies, banks, insurance and blockchains companies took part. During the first year the objectives were achieved and now companies are more competitive in a wider market (Financial Conduct Authority, 2015). The report on the lessons learned shows that the project made it possible to achieve a significant innovation in the financial sector, a greater investment volume and an exponential technological growth (Financial Conduct Authority, 2016).

Further, Abu Dhabi has decided to open a Regulatory Laboratory (RegLab) for its global market so that FinTech participants can develop and try their proposal for a period of up to two years (Abu Dhabi Global Market, 2016).

The United States of America followed the trend with one of the first sandbox initiatives in the continent, the Arizona Regulatory Sandbox Program, through which they approached three FinTech categories: (i) electronic money transfers, (ii) consumer loans and (iii) Investment advice. Here the sandbox allows for mobility in these areas, so the regulations that fall outside its testing environment scope

⁹ Sandbox where children play, build and experiment. By extension, “experimentation environment”.

remain intact. It is valid for a period of two years and the business proposal in which the use of technology can bring about problems must be new or emerging (Watkins, Daniels and Slayton, 2018). The aim was to take advantage of the potential provided by this sandbox environment to mitigate the market distortions created by regulatory barriers.

Another example of success can be observed in Singapore, where any company that makes an innovative use of technology for financial services can access the Intelligent Financial Center. This is a controlled regulatory system where rules and regulations established by the Monetary Authority are less strict (Monetary Authority of Singapore, 2018). Based on this idea, the State becomes an enabler of rules for the participation of all stakeholders interested in developing new technologies, business models and regulatory instruments suitable to drive innovation in different sectors.





Conclusions and Recommendations

Based on the literature and the recently adopted international instruments, this document identified the concept of artificial intelligence, its potential disruptive force, and its main governance problems related to algorithm transparency, accountability, control and explainability.

Furthermore, it was proposed that privacy, agency, autonomy and self-determination are essential rights sitting at a crossroad between ethical principles and legal rules, with which it is intended to protect personal privacy and autonomy. This has two purposes: protecting our personal information, as well as the way, degree and extent to which we decide to share this information with others, and then safeguarding the way in which we take our personal decisions freely and autonomously based on that information, free from any unconsented, undue or illegal external interference.

In the international context, the right to explanation regarding a decision taken through an automated processing of personal data by AI systems is an important first step towards protecting the essential rights mentioned before. However, there is still a long way to go for the full articulation and implementation of this right in Latin America if one looks at the reform bills currently awaiting their approval in legislative bodies in Argentina and Chile. Once the final texts are approved, it is recommended to study the way in which the Brazilian, Argentine and Chilean DPAs interpret these provisions in order to determine if they closely follow the interpretation of article 22 of the GDPR by the Working Party of article 29, or if they make a different interpretation, restricting or broadening the algorithm accountability derived from the automated data processing made by artificial intelligence systems.

In addition, we explained the reasons why the right to obtain an explanation might eventually fall short of protecting our personal information, the manner, degree and extent to which we choose to share it with others, and the way in which we make our personal decisions freely and autonomously based on that information and without any non-consensual, improper or unlawful outside interference. For these reasons, it was argued that the digital ethic could play a critical role in interpreting, adjusting and updating existing regulations. To this end, the creation and implementation of regulatory experimentation initiatives is recommended, since these constitute the ideal scenario for the design, development and implementation of "X-by-Design" digital tools and architectures. Such exercises allow for experimentation beyond compliance with the letter and spirit of the law, since public and private actors can create new ways to protect the fundamental rights to privacy, due process, and personal autonomy.

It should be noted, however, that the eventual proliferation of this type of initiative in Latin American countries could result in the "technological balkanization" of the continent, that is, in a sort of regulatory fragmentation derived from the different legal and ethical regimes that the countries of the region may adopt in an uncoordinated manner, to the detriment of entrepreneurship and innovation.

In this sense, it would be reasonable to opt for the coordinated creation of experimental regulatory initiatives that promote innovation, entrepreneurship and uniform regulation of technology applicable to business models based on the automated processing of personal data by AI systems. Multilateral bodies can also contribute to this, considering the possibility of including contractual clauses or provisions that promote practices regarding methods or tools X-by design and by default (X=Legality, Privacy or Digital Ethics). Within the Latin American context, the IDB's fAIr Lac initiative is called upon to play a leading role by harmonizing and coordinating initiatives for regulatory experimentation or sandboxes, and also by documenting and sharing experiences and lessons learned from them.

In short, the regulatory and ethical experimental environments constitute the privileged space where all the interested actors should actively participate in order to forge in a coordinated way the regulation that governs the Fourth Industrial Revolution in all its aspects. But this will not happen only with the issuance of rules on paper, but these must be put into practice through alternative regulatory tools or methods that have a real impact on the protection of the individual's fundamental right to make informed decisions and without any kind of illegal, undue or non-consensual external interference.

Bibliographic references

Abu Dhabi Global Market. 2016. *ADMG Launches its Fintech Reglab*.
Consulted at:
<https://fintech.adgm.com/adgm-launches-its-fintech-reglab/>

Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation* 2016/679, 17/EN. WP 251rev.01, February 6th 2018.

World Bank. *World Development Report 1997: The State in a Changing World*. Washington: International Reconstruction and Promotion Bank [Banco Internacional de Reconstrucción y Fomento] / World Bank, August 1997. Consulted at:

<http://documentos.bancomundial.org/curated/es/701691468153541519/pdf/173000WDR0SPANISH0Box128708B00PUBLIC0.pdf>

Barrat, J. 2013. *Our Final Invention: Artificial Intelligence and the End of the Human Era*. Oxford, RU: Oxford University Press.

Bartlett, R., A. Morse, R. Stanton y N. Wallace. 2019. *Consumer-Lending Discrimination in the FinTech Era*. Consulted at:
<https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf>

Bostrom, N. 2014. *Superintelligence: Paths, Dangers and Strategies*. Oxford, RU: Oxford University Press.

Castaño, D. 2019a. Nudge + Código: una arquitectura digital para el precedente judicial. [Nudge + Code: a digital architecture for legal precedents]. In *XX Jornadas de Derecho Administrativo [Seminar on Administrative Law]*, Universidad Externado de Colombia, Bogotá.

-----2019b. *GovTech: Privacidad, legalidad y ética digital. [GovTech: Privacy, legality and digital ethics]*. Alcaldía Mayor de Bogotá.

Cavoukian, A. S.f. *Privacy by Design: The 7 Foundational Principles*. Consulted at:
https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20%207%20Foundational%20Principles.pdf

Crawford. J. y J. Schultz. 2014. *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 94.

Domingos, P. 2015. *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake our World*. Basic Books.

Financial Conduct Authority. 2015. *Regulatory Sandbox*. Financial Conduct Authority, Londres, noviembre. Pub ref. 005147. Consulted at:
<https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf>

Financial Conduct Authority. 2016. *Regulatory Sandbox Lessons Learned Report*. Financial Conduct Authority, Londres. Consulted at:
<https://www.fca.org.uk/publications/research/regulatory-sandbox-lessons-learned-report>

Floridi, L y J. Cows. 2019. *A Unified Framework of Five Principles for AI in Society*. 1 Harvard Data Science Review 1, 7.

Floridi, L., J. Cowls, M. Beltrametti et al. 2018. *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*. *Minds and Machines*, 28: 689 – 707.

Goldberg, K y V. Kumar. 2019. *Cognitive Diversity: AI & The Future of Work*. Tata Communications. Consulted at:
https://www.tatacommunications.com/wp-content/uploads/2018/09/Report_Cognitive-Diversity_AI-and-The-Future-of-Work.pdf

Goodman, B y S. Flaxman. 2017. *European Union Regulations on Algorithmic Decision-Making and ‘a Right to Explanation’*. 38 *AI MAG*. 50, 55-56.

Hawking, S. 2018. *Brief Answers to the Big Questions*. United Kingdom: John Murray Publishers. Consulted at:
<https://www.kobo.com/ww/en/ebook/brief-answers-to-the-big-questions>

High-Level Expert Group on Artificial Intelligence (HLEG) of the European Commission on Artificial Intelligence. 2019. *A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines*. Consulted at:
<https://www.aepd.es/sites/default/files/2019-09/ai-definition.pdf>

HM Treasury. 2018. *The Economic Value of Data: Discussion Paper*. Crown.

Information Society Project at Yale Law School & Immuta. 2017. *Governing Machine Learning: Exploring the Intersection Between Machine Learning, Law, and Regulation*. White Paper. Consulted at:
<https://www.immuta.com/governing-machine-learning-exploring-the-intersection-between-machine-learning-law-and-regulation/>

Jiménez, G. y M. Hagan. 2019. *A Regulatory Sandbox for the Industry of Law*. White Paper. Stanford Law School Legal Design Lab. Consulted at:
<https://law.stanford.edu/publications/a-regulatory-sandbox-for-the-industry-of-law/>

Jordan, M. I. 2019. *Artificial Intelligence: The Revolution that hasn't Happened Yet*. *Harvard Data Science Review*, 18. Consulted at:
<https://hdsr.mitpress.mit.edu/pub/wot7mkc1>

Kaminski, M. E. 2019. *The Right to Explanation, Explained*. 34 *Berkeley Tech. L. J.* 189.

Katyal, S. 2019. *Private Accountability in the Age of Artificial Intelligence*. 66 *UCLA L Rev* 54. Consulted at:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3309397##

Keats-Citron, D. 2008. *Technological Due Process*, 85 *Wash. L. Rev.* 1249.

Keats-Citron, D y F. Pasquale. 2014. *The Scored Society: Due Process for Automated Predictions*, 89 *Wash. L. Rev.* 1.

- Kroll, J., J. Huey, S. Barocas et al. 2017. *Accountable Algorithms*, 165 U. Pa. L. Rev. 633. Consulted at:
https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/
- Levine, D.S. *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 Fla. L Rev. 135, 139.
- McKinsey Global Institute. 2017. *Artificial Intelligence: The Next Digital Frontier?* Discussion Paper.
- Mittelstadt, B. D. y L. Floridi. 2016. *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*. Sci Eng Ethics, 303.
- Monetary Authority of Singapore. 2018. *Regulatory Sandbox*. Consulted at:
<https://www.mas.gov.sg/development/fintech/regulatory-sandbox>
- OECD (Organisation for Economic Cooperation and Development). 2019a. *Recommendations of the Council on Artificial Intelligence*, OECD/LEGAL/0449. Consulted at:
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- . 2019b. *Artificial Intelligence in Society*, OECD Publishing, Paris. Consulted at: <https://doi.org/10.1787/eedfee77-en>
- . 2015. *Data-driven Innovation: Big Data for Growth and Well-being*. OECD Publishing. Consulted at:
https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en#page1
- . 2014. 'Data-driven Innovation: Big Data for Growth and Well-being'. OECD Publishing, 10.
- O'Neil, C. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Journal of Information Privacy and Security, 13:3, 157-159,
- Rubinstein, R., D. Lee y P. M. Schwartz. 2008. *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*. 75 U. Chi. L. Rev. 261.
- Russell, S. 2019. *Human Compatible: Artificial Intelligence and the Problem of Control*. New York: Viking
- . 2017. *Provably Beneficial Artificial Intelligence, The Next Step: Exponential Life*. BBVA, OpenMind. Consulted at:
<https://www.bbvaopenmind.com/wp-content/uploads/2017/01/BBVA-OpenMind-Provably-Beneficial-Artificial-Intelligence-Stuart-Russell.pdf>
- Russell, S., D. Dewey y M. Tegmark. 2015. *Research Priorities for Robust and Beneficial Artificial Intelligence*. AI Magazine.
- Shaw, G. 2019. *The Future Computed: AI & Manufacturing*. Microsoft Corporation.

Singapore Digital, *InfoComm Media Development Authority y Personal Data Protection Commission*. 2020. Model: Artificial Intelligence Governance Framework, 2nd ed., enero 21. Consulted at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>

Solove, D. J. 2001. *Privacy and Power: Computer Databases and Metaphors for Information Privacy*. 53 Stan. L. Rev. 1393.

Selbst, A. D. y S. Barocas. 2018. *The Intuitive Appeal of Explainable Machines*. 87 Fordham. L. Rev. 1085.

Selbst, A. D. y J. Powles. 2017. *Meaningful Information and the Right to Explanation*, 7 Int'l Data Privacy L. 233, 235.

Stephens-Davidowitz, S. 2017. *Everybody Lies: Big Data, New Data, and What the Internet can Tell us about who We Really Are*. New York: HarperCollins Publishers.

Tene, O. y J. Polonetsky. 2013. *Big Data for All: Privacy and User Control in the Age of Analytics*. 11 Nw.J. Tech.& Intell.Prop.239.

-----, 2012. *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 Stan. L. Rev. Online 63, 65-66.

Wachter, S., B. Mittelstadt y L. Floridi. 2017. *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. 7 Int'l Data Privacy L.

Watkins, P., E. Daniels y S. Slayton. 2018. *First in the Nation: Arizona's Regulatory Sandbox*. *Stanford Law & Policy Review*, 29 (1): 1-17. Consulted at: <https://law.stanford.edu/publications/first-in-the-nation-arizonas-regulatory-sandbox/>

Zarsky, T. Z. 2011. *Government Data Mining and Its Alternatives*. 116 Penn. St. L. Rev, 285.

Disclaimer The opinions expressed in this publication are those of the authors. They do not purport to reflect the opinions or views of the CETyS or of any other organization involved in the project.