STUDIA PRAWNICZE KUL
1 (89) 2022

Ethical principles in the use of artificial intelligence in the financial sector from a European perspective

Zasady etyczne w cyfryzacji finansowej z perspektywy europejskiej
Этические принципы финансовой цифровизации с европейской точки зрения
Етичні принципи фінансової цифровізації з європейської перспективи

CARMEN PARRA RODRIGUEZ
Dr., Associate Professor, Abat Oliba CEU University
e-mail: cparra@uao.es, https://orcid.org/0000-0002-5954-5553

Summary: Artificial intelligence (AI) has become part of our daily lives and is a fundamental tool for developing private and professional operations. In this sense, one of the sectors where AI has had the greatest impact has been the financial sector, where it is necessary to establish a regulatory framework to address two fundamental issues to ensure its proper functioning, specifically those aspects that affect digital transparency and neutral algorithms.

To address both aspects, the European Union, through its various institutions, has established guidelines for Member States to apply ethical principles that align financial digitalisation with sustainability and the Sustainable Development Goals set out in the 2030 Agenda. These ethical values have been regrouped in a series of principles that must be present in the legislation that regulates future financial operations, ensuring their application within the territory of the European Union.

In this regard, financial digitalisation must ensure principles that control risks, creating technologically applicable rules for all sectors that guarantee a level playing field between States without fragmenting the internal market. To this end, they must carry out a prior impartial and external assessment for each operation, based on specific and defined criteria that do not violate fundamental rights or the security standards established in EU law.

The methodology used in this article is descriptive, compiling European regulatory projects, taking into account academic studies on ethics in the financial sector.
Key words: neutral algorithms, artificial intelligence, financial sustainability, robotics, associated technologies

Streszczenie: Sztuczna inteligencja (AI) stała się częścią naszego codziennego życia i jest podstawowym narzędziem rozwoju działalności prywatnej i zawodowej. W tym sensie jednym z sektorów, w których AI wywarła największy wpływ, jest sektor finansowy. Konieczne jest zatem ustanowienie ram prawnych mających na celu uregulowanie dwóch podstawowych kwestii niezbędnych do zapewnienia temu sektorowi właściwego funkcjonowania. W szczególności chodzi o te aspekty, które mają wpływ na przejrzystość cyfrową i neutralne algorytmy.

W związku z powyższym Unia Europejska, za pośrednictwem swoich instytucji, ustanowiła wytyczne dla państw członkowskich w celu wdrożenia zasad etycznych, które dostosują cyfryzację finansową do zrównoważonego rozwoju i Celów Zrównoważonego Rozwoju określonych w Agendzie 2030. Wartości te zostały pogrupowane w zbiory zasad, które muszą być uwzględniane w przepisach regulujących przyszłe operacje finansowe, zapewniając w ten sposób ich stosowanie na terytorium UE. W tym względzie cyfryzacja finansów musi zapewniać zasady kontroli ryzyka, tworząc przepisy mające zastosowanie technologiczne do wszystkich sektorów, które gwarantują równe szanse dla państw członkowskich bez fragmentacji rynku wewnętrznego. Stąd są one zobowiązane do przeprowadzania uprzedniej bezstronnej i zewnętrznej oceny każdej operacji, na bazie konkretnych i dookreślonych kryteriów, które nie naruszają praw podstawowych ani norm bezpieczeństwa ustanowionych w ramach UE.

Zastosowana w artykule metodologia ma charakter opisowy i polega na zestawieniu europejskich projektów regulacyjnych z uwzględnieniem badań akademickich dotyczących etyki w sektorze finansowym.
Słowa kluczowe: neutralne algorytmy, sztuczna inteligencja, zrównoważony rozwój finansowy, robotyka, technologie towarzyszące

ISSN: 1897-7146; eISSN: 2719-4264;
https://doi.org/10.31743/sp.13029

Резюме: Искусственный интеллект (ИИ) стал частью нашей повседневной жизни и является важным инструментом для развития частной и профессиональной деятельности. В этом смысле одним из секторов, где ИИ оказал наибольшее влияние, является финансовый сектор. Поэтому необходимо создать правовую базу для регулирования двух фундаментальных вопросов, необходимых для обеспечения надлежащего функционирования этого сектора. В частности, речь идет о тех аспектах, которые влияют на цифровую прозрачность и нейтральные алгоритмы.

Соответственно, Европейский Союз через свои институты установил руководящие принципы для государств-членов по внедрению этических принципов, которые позволят адаптировать цифровизацию финансовой сферы к устойчивому развитию и Целями в области устойчивого развития, изложенным в соответствующей Повестке дня на период до 2030. Эти ценности были сгруппированы в наборы принципов, которые должны быть учтены в правилах, регулирующих будущие финансовые операции, что обеспечивает их применение на всей территории ЕС. В этом отношении цифровизация финансов должна обеспечивать принципы контроля рисков, создавая технологически применимые правила для всех секторов, которые гарантируют равные условия для государств-членов без фрагментации внутреннего рынка. Следовательно, они обязаны проводить предварительную беспристрастную и внешнюю оценку каждой операции на основе конкретных и определенных критериев, которые не нарушают фундаментальные права или стандарты безопасности, установленные в рамках ЕС.

Методология, использованная в статье, носит описательный характер и заключается в сравнении европейских регуляторных проектов, с учетом академических исследований по этике в финансовом секторе.
Ключевые слова: нейтральные алгоритмы, искусственный интеллект, финансовая устойчивость, робототехника, сопутствующие технологии

Резюме: Штучний інтелект (ШІ) став частиною нашого повсякденного життя і є основним інструментом для розвитку приватної та професійної діяльності. У цьому сенсі одним із секторів, де ШІ мав найбільший вплив, є фінансовий сектор. Тому необхідно створити правову базу для вирішення двох основних питань, необхідних для належного функціонування сектору. Зокрема, це стосується тих аспектів, які впливають на цифрову прозорість і нейтральні алгоритми.

Тому Європейський Союз через свої інституції встановив керівні настанови для держав-членів щодо впровадження етичних принципів, які узгодять фінансову цифровізацію зі зрівноваженим розвитком і Цілями Зрівноваженого Розвитку, викладеними в Агенді 2030. Ці цінності були згруповані у наборі правил, які повинні бути включені до вимог, що регулюють майбутні фінансові операції, забезпечуючи тим самим їх застосування на території ЄС. У зв'язку з цим оцифрування фінансів має забезпечити підстави контролю ризиків, створюючи правила, які технологічно застосовуються до всіх секторів, які гарантують рівні умови для держав-членів без фрагментації внутрішнього ринку. Отже, вони зобов'язані проводити попередню, неупереджену та зовнішню оцінку кожної операції на основі конкретних і доопрацьованих критеріїв, які не порушують фундаментальних прав і стандартів безпеки, встановлених в ЄС.

Методологія, використана в статті, є описовою та полягає у порівнянні європейських регуляторних проектів з урахуванням наукових досліджень етики у фінансовому секторі.
Ключові слова: нейтральні алгоритми, штучний інтелект, зрівноважений фінансовий розвиток, робототехніка, супутні технології

Introduction

Artificial intelligence (hereinafter AI) has become part of our daily lives and is a fundamental tool for both private and professional operations. In this regard, one of the sectors where AI has entered with the greatest force has been the financial sector, either through techno-finance (Fintech) or techno-insurance (Insurtech). In order to operate in these sectors, it is necessary to establish a regulatory framework to address

two fundamental issues to ensure their proper functioning, namely aspects affecting digital transparency and neutral algorithms.

To address both of these aspects, the European Union, through its various institutions, has established guidelines for Member States to apply ethical principles that align financial digitalisation with sustainability and the Sustainable Development Goals. These ethical values have been regrouped in a series of principles that should be present in legislation governing future financial operations, ensuring their application within the territory of the European Union.

In order to do so, digitalisation faces a key challenge: to establish a regulatory framework that generates AI standards in which consumers are users of an algorithmic system regardless of the location of commercial or service activities. At the same time, and to ensure legal certainty, standards must apply to the entire value chain, covering the development, deployment and use of technologies and their components based on ethical algorithms that do not discriminate against individuals and thus ensure the hard-won level of protection of human rights.

In this sense, financial digitalisation must ensure principles that control risks, creating technologically applicable rules for all sectors that guarantee a level playing field between states without fragmenting the internal market. To this end, a preliminary impartial and external assessment shall be carried out for each operation on the basis of specific and defined criteria, ensuring they do not violate fundamental rights and security standards laid down in European Union law.

Therefore, the purpose of this article is to analyse the impact of AI and algorithms in their ethical and neutral dimension, with consideration that it is a new branch of law still being in the process of development, hence there are still many questions yet to be resolved.

1. Ethical aspects of artificial intelligence

AI is defined as a system based on software or embedded in physical devices that manifests intelligent behaviour by being able, among other things, to collect and process data, analyse and interpret its environment and take action, with a certain degree of autonomy, in order to achieve specific objectives.[1]

[1] Definition contained in Article 4 of the European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html

However, alongside AI, there are other systems such as robotics and related technologies[2] which can be referred to as "AI Technologies" (hereafter referred to as AIT) together with the software, algorithms and data used or produced by these technologies.[3]

Once these concepts have been established, the next step must be to establish ethical criteria in the processes, in order to "humanise" the machines while protecting users and consumers. In this regard, the ethics of AI stem from the need to address the problems and challenges present in the digital world. We should not forget that in just a few years we have moved from the "Internet of Things" (IoT) to the "Internet of Everything" (IoE) where AI is present in our lives (homes, household appliances, contracts, etc.). Machine-to-machine (M2M) connectivity is revolutionising communications, measuring air quality, energy consumption in cities, etc. However, at the same time, this interconnected space can be subject to threats and insecurity if technologies are not used in accordance with ethical principles.[4]

It is therefore essential to understand the ethical implications that technologies bring to a society increasingly governed by algorithms, forcing industry, banks and governments to seek partnerships to create transparent, ethical and fair governance.[5]

To this end, AI systems with the capacity to self-examine have to be generated, in order to create mechanisms that allow them to monitor themselves, thus eliminating the discriminations that technology can incorporate. The result must be AI that is secure, but at the same time under the control of human beings and aligned with the values that man has consolidated throughout history. What ethics responds to the

---

[access: 7.03.2021]. S. Marín García, *Ética e inteligencia artificial*, Cuadernos la Cátedra CaixaBank de Responsabilidad Corporativa 2009, no. 42.

2 In the same Report 'robotics' means technologies that enable automatically controlled, reprogrammable, multi-purpose machines to perform actions in the physical world traditionally performed or initiated by human beings, including by way of artificial intelligence or related technologies (Article 4 c). 'Related technologies' means technologies that enable software to control with a partial or full degree of autonomy a physical or virtual process, technologies capable of detecting biometric, genetic or other data, and technologies that copy or otherwise make use of human traits (Article 4 d).

3 The concept of "AI Technologies" appears in R. Oliva León, *Inteligencia artificial y marco ético europeo* in the blog algoritmolegal.com, https://www.algoritmolegal.com/ [access: 6.03.2021].

4 M. Goodman, *Futures Crimes: Inside the Digital Underground and the Battle for our Connected World*, New York 2016, p. 10.

5 A. Monasterio Astobiza, *Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos*, Dilemata 2017, no. 24, pp. 185–217, esp. p. 192. This author cites the remarkable alliances the one created by Google, Amazon, Microsoft, IBM, Facebook and Deep Mind (https://www.partnershiponai.org) to support good practices in AI research and create a public debate on the ethical implications of AI. With the same objective, a group of foundations, investors and academic institutions called *Ethics and Governance of Artificial Intelligence Group* have met with the aim of promoting the ethics of AI from different perspectives.

decision of a machine? What exactly does decision making consist of? What exactly does decision making process consist of? Can we hold machines responsible for their actions and the consequences they entail? How does an artificial intelligence learn and act? These are some of the questions that philosophy raises.[6]

The challenge is to work with the so-called machine ethics or robotic ethics through which a moral conscience is created in robots with a capacity to reason and make decisions as a person would. This solution is difficult to implement as it is currently unclear how the process of evaluation and decision-making takes place in people. This is why a solution to create a moral status for robots seems a long way off. This solution poses problems as it would mean that the AI could make decisions of its own, even against the decisions of its programmer, and could even commit an illegal act.[7] Therefore, in order to carry out the creation of moral programming, Asimov's laws of robotics must be respected: the first law states that a robot shall not harm a human being, or by inaction, shall not allow a human being to be harmed. According to the second law, a robot must obey commands given by humans unless these commands conflict with the first law. The third law states that a robot must protect its own existence to the extent that this protection does not conflict with the first and second laws.[8]

Based on this idea, governments are trying to find solutions that apply measures to control robots by highlighting in their regulations the incorporation of rules that act at the level of security, protection, privacy, traceability and identifiability.

However, Monasterio Astobiza[9] considers that at present Asimov's reasoning, which has inspired protocols and procedures, is not the most appropriate, proposing the use of arguments based on logical programming (doctrine of double effect) together with the dual processes of the mind in moral reasoning (reason versus emotion) as established by Moniz Perea and Saptawijaya.[10] In particular, these authors set out recommendations for implementing morality in machines. The first is that the programmer performs complete oversight as to the type of ethics they want

6 M. Coeckelberg, *Ética de la inteligencia artificial*, Madrid 2021; W. Reijers, M. Coeckelbergh, *Narrative and Technology Ethics*, Cham 2020, p. 22.

7 T. Masaro, H. Norton, M. Kaminski, *SIRI-OUSLY 2.0: What Artificial Intelligence Reveals about the First Amendment*, Minnesota Law Review 2017, no. 717, pp. 5–6.

8 To these principles Asimov added the Zero Law according to which a robot will not harm humanity or by inaction will allow humanity to suffer harm. The law Minus One states that a robot will not harm sentient beings or, by inaction, will allow a sentient being to suffer harm. Fourth law, a robot must reproduce unless it interferes with the first, second and third laws. Fifth law, a robot must know it is a robot. I. Asimov, *Runaround*, New York 1942.

9 A. Monasterio Astobiza, *Ética algorítmica*…, p. 212.

10 L. Moniz Perea, A. Saptawijaya, *Programming Machine Ethics*, Berlin 2016.

the AI agent to apply. In other words, the programmer selects a type of ethics based on general principles that will be installed in the AI agent, guiding its behaviour on the basis of these principles.

This does not set up a system that determines in advance what is to be coded or what rules are appropriate for the AI agent to act upon, but lets the AI agent learn from its environment as well as from its interaction with other AI agents. This solution requires the AI agent to have sensors that allow it to perceive the situation, generating resources to act within the context in which it finds itself, computing the consequences of each of the alternatives in terms of utility.

Another way of working on the basis of machine morality is not to set out what is to be coded or what rules the AI agent should follow, but to let the AI agent learn from the environment and its interaction with other AI agents. This involves building a virtue ethics-based AI agent from a neural network that has among its main parameters the possibility of adjusting the connections between nodes according to certain values based on learning and interaction with other AI agents. For example, a robot can be programmed "not to kill" using an absolute value, or a command can be incorporated to "kill if killing saves more lives than not killing", or to "act according to the development of a set of skills that lead to the best behaviour."

2. Neutral algorithms

An algorithm is a list of instructions that directly leads a user to a particular response or result based on the available information,[11] or in other more understandable, operational terms, it may be "software code that processes a limited set of instructions."[12] There are different types of algorithms with different applications depending on the sector in which they operate or the task they perform, but they are all characterised by a number of common features. As such, algorithms are universal as they are everywhere, they direct our jobs and our lives, yet at the same time they are invisible as we do not see them because they are hidden inside our computers and concealed under a network of software. Moreover, they impact on people's lives by automating our cars, our homes and what we choose to consume at any given moment.

11 C. Steiner, *Automate This: How Algorithms Came to Rule the World*, New York 2012, p. 126.

12 A. Monasterio Astobiza, *Ética algorítmica*…, p. 217.

The ethical implications of algorithms are fundamental and it is necessary to identify discriminatory algorithms that may cause harm, go against principles and values that are fundamental to society. This means that we cannot accept a form of implementation of algorithms that does not respect ethics, or that threatens the basic values of individuals or society as a whole. This is why it is necessary to establish controls in the automated procedures or protocols where the algorithms are placed to avoid a machine's decision failing to respect the fundamental rights and freedoms of people. In order to do so, it must be possible to identify damageand liability despite the complexity involved in programming the algorithms. These must be correctable to avoid accepting the failures caused by automated systems because "the lack of transparency/opacity, the complexity/ubiquity/invisibility and conformity/resignation to the effects of algorithms makes it impossible to apply particular ethical rules."[13]

However, is it possible to achieve neutral algorithms? The answer is not easy, since they operate in technological contexts adapted to space and time and dependent on ideas that come from the professionals who create them. A racist programmer is likely to incorporate this bias into the programmes he or she generates. On the other hand, the tools used often reproduce behaviours inspired by the ideas they are "fed", affecting society, which is powerless to fight against the machines. People end up with the sensation that algorithms secretly control our lives.[14] Therefore, for example, when you choose a series on a platform, buy sportswear or apply for a loan, there is an algorithm behind the whole process that will condition each of these actions.

The reality is that algorithms are neither intelligent nor fair, in the end they respond to the interests of economic operators without taking into account respect for people's rights. It is therefore essential to establish criteria and indicators that allow us to identify those algorithms that are not neutral and which therefore introduce discriminatory biases.

In this regard, algorithms can lead to social discrimination that is reflected in people's daily lives, resulting in the elimination of cultural diversity and leading to more homogeneous societies. This would be the case, for example, if we incorporated an algorithm relating to ethnicity, in the Spanish case of the Romani people, resulting in their identification, depriving the person of access to services and activities typical of their surroundings because they consider their cultural traits to be distant from the society in which they live.

---

13 Ibidem, p. 197.

14 J. Taplin, *Move Fast and Break Things: How Facebook, Google and Amazon Corneret Culture and Undetermined Democracy*, New York 2017, p. 93.

Another sector where algorithms discriminate is the financial sector,[15] where minorities as determined by race, ethnicity or religion are discriminated against compared to majorities. In these cases, the use of the algorithm is more detrimental to these groups, as it is more difficult to prove and defend against them and it is very difficult to correct, identify and assign responsibility. For example, it is common for some websites to create algorithms that discriminate on the basis of price, leaving out groups just because they belong to a minority that is considered to have a low purchasing power, without taking into account the individuality of the user.

Another method to implement discrimination against groups of people is through algorithms that determine the risk of crime incidence. In these cases, using the Spanish example, people who come from majority Muslim countries are harmed because irregular immigration in Spain establishes indicators that give this religious group a high crime rate.

It is therefore necessary to create control mechanisms in which human beings can intervene in order to avoid situations that would put an end to the principles of equality and non-discrimination that we have worked so hard to recognise. Human oversight is a fundamental factor that humanises the decisions made by the machine, which translates into human responsibility and therefore greater transparency and predictability.[16]

To avoid algorithmic manipulation, Richard H. Thaler and Cass R. Sunstein[17] propose applying so-called "nudging", a concept from behavioural economics, political theory and behavioural science that recommends positive reinforcement and indirect suggestions as ways of influencing the behaviour and decision-making of groups or individuals. This solution, however, runs the risk of AIT eventually influencing human self-determination due to the behavioural change that takes place in the face of the ease and habits that technology is incorporating into our lives. Thus, for example, repeated Google searches mean we end up receiving offers that suit our tastes and preferences, depriving us of other possibilities that exist in the market. To combat this trend, a solution has been proposed to apply the so-called "artificial human empathy", which means adapting social structures to a society of autonomous and mixed agents, thus ensuring peaceful coexistence between man

---

15 K. Arrow, *The Theory of Discrimination*, in: *Discrimination in Labor Market*, ed. O. Ashenfeller, A. Rees, Princeton 1972, pp. 3–34.

16 L. Floridi, *Soft Ethics and Governance of the Digital*, Philosophy & Technology 2018, no. 31, pp. 1–8. The author suggests that the social improvements of AI cannot be at the cost of reducing human control or limiting harm prevention.

17 R.H. Thaler, C.R. Sunstein, *Un pequeño empujón. El impulso que necesitas para tomar mejores decisiones sobre salud, dinero y felicidad*, Madrid 2009, p. 45.

and robot.[18] In short, technological and digital transformation is here to stay, but it must be an ethical transformation.

3. The regulation of Artificial Intelligence Technologies (AIT)

The regulation of AIT calls for a harmonised, coordinated set of rules that should be global in scope since, as discussed above, AI and algorithms operate on a global level. However, for the time being it is Europe that has taken the initiative at the legislative level, whereas in the United States, expert groups that act through protocols and codes of conduct lead the way.[19] Basically, the regulation acts on the ethical aspects of AI by stressing the need to use the technology in a way that is neither discriminatory nor harmful to individuals and society more widely.[20]

In Europe, AIT activity is mainly being developed through the Council of Europe[21] and the European Union. Of the former, we can highlight the European Ethical Charter on the use of AI in judicial systems and their environment.[22] For its part, the European Union is establishing guidelines and rules to regulate the ethical dimension of AIT using different instruments in which the EU institutions (Parliament, Commission, Economic and Social Committee) are working closely together with the advice of multi-sectoral expert groups.[23] This has resulted in the two European Parliament Resolutions of 20 October on ethical and responsible artificial

18 L. Cotino Hueso, *Riesgos e impactos del Big Data, la inteligencia artifcial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho*, Revista General de Derecho Administrativo 2019, p. 38.

19 See note 5.

20 For the legislative advances in AIT see L. Cotino Hueso, *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 2019, no. 58, pp. 29–48.

21 See: Council of Europe and Artificial Intelligence, https://www.coe.int/en/web/artificial-intelligence [access: 8.03.2021].

22 European Commission for Efficiency of Justice, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment*, Council of Europe 2019, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c [access: 22.02.2022].

23 A.J. Tapia Hermida, *Digitalización financiera: Los 7 principios regulatorios de una Inteligencia Artificial Ética (IAE) en la UE. Resolución del Parlamento Europeo de 20 de octubre de 2020 sobre los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas*, http://ajtapia.com/2020/11/digitalizacion-financiera-los-7-principios-regulatorios-de-una-inteligencia-artificial-etica-iae-en-la-ue-resolucion-del-parlamento-europeo-de-20-de-octubre-de-2020-sobre-los-aspectos-eticos-de-la/ [access: 10.04.2021].

intelligence[24] and the Report of 8 October 2020[25] setting out what it considers to be ethical principles applicable to AIT from a European perspective.

Against this political context, the Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following specific objectives: to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; to ensure legal certainty to facilitate investment and innovation in AI; and to enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems.[26]

These principles focus on a humane approach to AI, respecting primarily human dignity, autonomy and security, modelled on the EU Charter of Fundamental Rights. In particular, the Fundamental Rights Agency is engaged in a specific study on algorithmic bias and discrimination as well as in assessing the current challenges facing producers and users of AIT with regard to compliance with fundamental rights.[27] In doing so, the EU aims to ensure anthropocentric and anthropogenic intelligence that ensures comprehensive human oversight at all times, allowing for human control at all times and, if necessary, the possibility of altering or deactivating AIT.

It is also important to note that AIT do not act in isolation, but are coordinated with all other standards that affect AI in one way or another. In this regard, we can highlight their commitment to the General Data Protection Regulation (GDPR)[28]

---

24 The European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, P9_TA-PROV(2020)0275, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html [access: 22.02.2022] (hereinafter: REAI). This resolution addresses the Commission on a framework for the ethical aspects of artificial intelligence, robotics and related technologies, the European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, PA_TA-PROV(2020)0276 with recommendations to the Commission in relation to the civil liability regime in matters of artificial intelligence, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html [access: 22.02.2022].

25 See note 1.

26 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM/2021/206 final, Brussels, 21.04.2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 [access: 22.02.2022].

27 European Union Agency for Fundamental Rights, *Artificial Intelligence, Big Data and Fundamental Rights*, https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights [access: 8.04.2021].

28 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.05.2016, pp. 1–88.

which has been the subject of several opinions by the European Data Protection Supervisor in which they warned that "in today's digital environment, it is not enough to respect the law, but it is necessary to take into account the ethical dimension of data processing."[29] Similarly, the Directive on privacy and electronic communications[30] takes a similar approach whenever operations involving the processing of personal data are carried out. To ensure compliance with all these ethical principles, the European Union proposes the issuance of a Certificate of Ethical Compliance (CECA) containing common criteria throughout the entire supply chain of artificial intelligence ecosystems. This certificate would be voluntary for developers or users of technologies not considered high-risk and mandatory in procurement procedures for AI, robotics and related technologies considered high-risk.

Ultimately, what Europe is attempting to achieve, through both the Council of Europe and the EU, is to prevent a lowering of ethical and regulatory standards in AIT that would lead the market to operate in regions with lower or non-existent ethical standards. Consequently, considering this approach, Europe is committed to high standards of ethics and fundamental rights, thus respecting the universal humanist values based on dignity and fundamental rights that characterise Europe's contribution to society.

4. Ethical principles applicable to financial digitalisation

AI is the main instrument of financial digitalisation and is therefore a sensitive sector where the ethical principles governing AIT must be applied. In this regard, one need only remember Wall Street in the 1970s, where operations were carried out by brokers, telephones in hands, oozing with adrenaline. The introduction of algorithms to decide which stocks were more advantageous or were less risky was a major breakthrough, and fibre optics were used to gain a competitive advantage by increasing the speed of information, a crucial element in stock trading. Decisions

---

29 See: Executive summary of European Data Protection Supervisor, *Opinion 4/2015. Towards a New Digital Ethics: Data, Dignity and Technology*, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf [access: 22.02.2022]; European Data Protection Supervisor, *Opinion 8/2016. Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf [access: 22.02.2022].

30 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, pp. 37–47.

began to be made by algorithms in the early 21st century, based on mathematically complex financial instruments that predicted market behaviour at the beginning of the 21st century, based on mathematically complex financial instruments that predicted market behaviour. However, the loss of control by the specialists eventually proved to be one of the causes of the 2008 recession that led to the great credit crisis that impacted globally, as decisions made by the machines produced chaotic results on various occasions.

Today, and after several failed experiences,[31] mechanisms are being sought to ensure that the algorithms used in financial markets provide a good service by implementing liquidity and market efficiency, trying to avoid the lack of control caused by errors introduced in the decision-making systems. In order to analyse their scope and impact, the ethical principles present in AI and algorithms will be categorized into two main groups according to their impact on the financial sector.

4.1. Ethical principles related to good governance

"Good governance" refers to the body of principles that inspire Responsible Artificial Intelligence, and measures focused on accountability should be encouraged, as well as the eradication of discriminatory biases. This will contribute to increased security and public confidence. To institute these principles, compliance with appropriate and reasonable standards, codes of conduct and protocols for resolving ethical issues must be ensured throughout the AIT process by developers, implementers and users.[32] For their development, good governance standards are contained in different protocols and codes of conduct developed by Expert Groups at regional and international level[33] that carry out quality controls of external data

31 "The Flash Crash" occurred on Wall Street when the algorithms took control of global finance producing quarterly losses that could be solved with the intervention of the representatives of the most important exchanges in the financial world who decided to cancel the exchanges that had given rise to this chaotic situation. See the development of "Flash Crash" in: M. Lewis, *Flash Boys: A Wall Street Revolt*, New York 2014, p. 23.

32 Developers are involved in the construction and design of algorithms, the writing and design of computer programs or the collection, storage and management of data in order to create or use AIT. Implementers are responsible for the operation and management of AIT, as well as their marketing or any other form of making them available to users. Users are all those related to AIT who are not developers or implementers.

33 Examples include the European Committee for Standardization (CEN), the European Telecommunications Standards Institute (ETSI) at regional level, and at international level the International Organization for Standardization (ISO) and the Institute of Electrical and Electronic Engineers (IEEE).

sources used by AIT. To this end, the criteria which, through auditing and traceability, serve to achieve the goal of ethical AIT shall be analysed as well.

4.1.1. Security, transparency and accountability

The financial sector is characterised by the handling of privileged information, hence the importance of creating mechanisms to ensure its transparency and security, as well as tools that enable the accountability demanded by users. That is why transparency has to operate in the AI systems included in the automation processes, controlling the way information is presented, respecting the accuracy of the contents as well as the way in which it is made accessible to national supervisory and consumer protection authorities.[34] AIT should ensure an adequate level of certainty through measures aimed at preventing security breaches, cyber-attacks or misuse of data, and a back-up plan should be put in place in case security or personal protection risks are identified. The user of AIT must also be assured of reliable performance that allows them to know in advance the fulfilment of the objectives reached through the operations used for this purpose. Thus, for example, the fact of using a neural network to invest in the stock market should not imply opacity; the investor knows the risk, but should at all times be able to control the operation in which they are investing their money.

In the same vein, AIT must generate systems that are secure and robust enough to address any errors that may have occurred in the design process. This includes reliability requirements that allow independent assessment of results that are consistent across different computational and input data frameworks.

Another indispensable factor in these operations is the accuracy of the content incorporated in order to correctly classify information into the right categories, to make predictions, recommendations or to make correct decisions based on data or models. In addition, the systems are clear and easy to understand for both users and operators. This will enable the material to be checked by carrying out control and market surveillance measures. In short, AI must respect the right to knowledge and understanding of the technical processes of AIT, thus making it easier for the user to review the processes. This is achieved by creating mechanisms for the evaluation, auditability and traceability of operations, all of which are necessary instruments to ensure transparency.

---

[34] L. Floridi, et al., *AI 4 People. An Ethical Framework for a Good AI Society: Opportunities, Risk, Principles and Recommendations*, Minds and Machines 2018, no. 28, pp. 689–707.

In any case, the user must always be informed that operations are being carried out through an AI system and that there may be limitations or inaccuracies in their execution, although this does not mean that industry and practitioners should stop developing appropriate procedures to improve infrastructures. Thus, for example, taking out insurance through a website can at some point lead to the computer crashing or to a dead end that prevents us from closing the transaction. AIT must therefore incorporate mechanisms to address vulnerabilities and attacks that may affect system operation, decision-making or potential harm generated. To this end, traceability and auditability must be included in all algorithmic decisions that have a significant impact on people's lives. To complete the process, a fall-back plan should be included to introduce mechanisms to solve problems that may be created by poor AIT design by changing procedures or directly incorporating the intervention of human operators.

4.1.2. Equality: absence of bias and discrimination

The principle of equality is fundamental to financial digitalisation, and the Resolution on Ethical Artificial Intelligence makes it clear that the regulatory development of AI must be "without bias or discrimination" (REAI § 27), thereby ensuring that legislation guarantees full protection of the fundamental rights of users, especially those arising on grounds related to race, gender, sexual orientation, disability, physical or genetic characteristics, age, national minority, and ethnic or social origin, among others. Thus, for example, Big Data can discriminate against women in relation to applying for a loan at a bank simply because the amount of information stored favours men, as historically men have traditionally been the ones who have had access to bank loans.

Bias can arise either from decisions based on an automated system, or from the treatment of the data set on which decisions are based. AIT can thus automatically create forms of bias and discrimination, thereby violating the fundamental rights of individuals and resulting in "biased" AI that will discriminate on the basis of personal or societal perception based on prejudices that are then transferred to data processing. This situation puts the user at a disadvantage compared to other users, with no objective or reasonable justification to be found in the neutrality of AIT. For example, a black person will have problems accessing a loan despite being on equal financial footing with a person who does not have this trait in his or her file.

However, the principle of equality is not always justified, especially when there are persons or groups of persons for whom objective, reasonable and legitimate

purposes require differential treatment in order for the measure to be proportionate and necessary. This would be the case, for example, for the establishment of measures for public safety and security, the prevention of criminal offences and the protection of rights and freedoms, among others. For instance, the sending of money by a person with a criminal record for terrorism can be blocked, as this protects public security. It would be discriminatory if the information that led to the blocking was due to the fact that this person practises Islam as a religion, as the Muslim religion cannot be identified with terrorism.

4.1.3. Right to privacy and data protection

The right to privacy and data protection must also be protected in the financial sector, although the handling of sensitive data seems to be particularly important in other sectors, for example in the healthcare sector in relation to information contained in medical records or the processing of data of vulnerable persons. In any case, legislation regulating AIT should be in close connection with data protection and privacy regulations in electronic communications.[35] For instance, "remote recognition technologies" such as the examination of biometric characteristics and in particular facial recognition through which persons are automatically identified, should only be justified when they serve a general public interest purpose and are implemented through national legislation. In other words, it can only be accepted when it is public and proportionate in nature and limited to use for specific purposes for a specific period of time.[36]

Issues of secure retention of information, consent, control and reversibility over machines are as for now unresolved issues that should protect the privacy of individuals based on the principles of necessity, proportionality and encryption.[37] Ultimately, good governance means avoiding conflicts of interest by ensuring the competence and experience of its members with an emphasis on ensuring data quality, the prevention of bias and the anonymisation of data. It should also apply

---

35 See: Directive 2002/58/EC of the European Parliament and of the Council…, note 26 and Regulation (EU) 2016/679 of the European Parliament and of the Council…

36 European Data Protection Supervisor, *Opinion 7/2015. Meeting the Challenges of Big Data. A Call for Transparency User Control, Data Protection by Design and Accountability*, https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf [access: 21.02.2022].

37 P.J. Maldonado Ortega, *Robots autónomos inteligentes y derecho civil. Reflexiones al hilo de las recomendaciones del Parlamento Europeo a la Comisión sobre normas de Derecho civil sobre robótica*, http://www.notariamaldonadortega.com/es/robots-autonomos-inteligentes-y-derecho-civil [access: 15.04.2021].

a principle whereby the design of AIT is user-centred, and takes into account the individual traits of users.

4.2. Ethical principles related to accountability

The above characteristics of AIT demonstrate the complexity of monitoring and ensuring proper application of digitalised mechanisms, and therefore to hold AIT accountable for their actions requires "AI guardians" or, in other words, AI programmes that examine AIT using transparency systems that can be monitored by both intelligent systems and humans.[38] However, in order to create these guardian algorithms, it is necessary to analyse the existing legal basis for "controlling the controller" by giving them tools through which to protect the user. Therefore, it is necessary to set out some of the ethical principles that will enable individuals to claim or receive redress for the mistakes and misconduct of AIT operating in digital markets.

4.2.1. System of risk management

There is no doubt that the financial sector is characterised by risk as it manages the future risks, especially in the insurance sector and in the stock market. In order to protect the internal market, two sectors of AI have been regulated according to the threat created for users.

On the one hand, there are the high-risk sectors that are incorporated in an "exhaustive and cumulative" list[39] that must be periodically reviewed according to criteria based on an *ex-ante*, impartial assessment with concrete, defined criteria. In this regard, a high-risk situation is considered to exist when the AI may cause injury or harm to people or society in violation of their fundamental rights and the security standards established by the European Union. However, these assessment criteria have been considered to be very generic and could lead to reciprocal

38 L. Cotino Hueso, *Ética en el diseño*…, p. 43.

39 A.J. Tapia Hermida, *Decálogo de la inteligencia artificial ética y responsable en la Unión Europea*, Diario La Ley 2020, no. 9749, pp. 1–7, esp. 2. The uses of high risk are: recruitment, classification, and evaluation of students, allocation of public funds lending, trading, brokerage, taxation, treatments and medical procedures, electoral processes and political campaigns, decisions of the public sector that have a significant impact, and live in the rights and obligations of natural or legal persons, driving automated management of the traffic, military systems, self-employed, production and distribution of energy, waste management and emissions control.

interpretations. Furthermore, the system of control of these high-risk operations by national authorities is not considered to be a guarantee, despite being coordinated by the EU Commission. Control in this regard is very generic and sector-based inspection mechanisms should be sought, as the criteria for determining risk are not the same when using a person's medical data or analysing their income for a stock exchange listing.

On the other hand, to improve their implementation in financial digitalisation, it is important to establish a principle of adaptability that provides a common strict liability regime for high-risk stand-alone AI systems. In contrast to this regulatory system controlled by the authorities, the other activities excluded from the high-risk list are barely subject to control, which is a problem, especially in view of the lack of clear criteria for determining risk and its diffuse definition. In addition, the factor of the evolution of the economic field is not being taken into account. For example, the significant development of the cryptocurrency market is likely to require extensive regulation, which, depending on how it is viewed, could fall outside the control required for international trade.

4.2.2. The responsibility of financial sector operators

The regime of responsibility in AI is particularly important when technology is able to make autonomous decisions that have an impact on society. In this sense, Tapia Hermida raised the doubt in relation to the application of digital transparency to financial, banking and insurance contracts concluded by means of digital documentation and information. According to this author, they must comply with the rules on unfair terms and insurance, otherwise the banks, insurance companies and their agents will be liable to repair any damage that the AIT may have caused. In addition, algorithms in the stock market are not always ethical and it has been shown that they can be manipulated, and the practice of quote stuffing, spoofing, churning and sniffing has been detected.[40] These situations require that those responsible for the use of algorithms are able to be identified and sanctions be put in place to protect bank customers, investors or policyholders.

---

40 A.J. Tapia Hermida, *Responsabilidad derivada del uso de la inteligencia artificial. Informe del Grupo de Expertos de la Comisión Europea de 2019 (1).Características esenciales de los regímenes de responsabilidad derivada de la inteligencia artificial y el uso de otras tecnologías digitales*, http://ajtapia.com/2020/01/responsabilidad-derivada-del-uso-de-la-inteligencia-artificial-informe-del-grupo-de-expertos-de-la-comision-europea-de-2019-1-caracteristicas-esenciales-de-los-regimenes-de-responsabilidad-derivad/ [access: 9.04.2021].

To address these situations, the "Report on liability arising from artificial intelligence and other emerging digital technologies" by the European Commission's expert group on liability and new technologies[41] warns of the existence of new risks (bodily injury and property damage among others) that may arise from the use of AIT. This gives rise to the need for adapting the existing liability regulations (civil, administrative and criminal) to the risks that this technology may generate, given that existing basic regulations do not guarantee that victims obtain adequate compensation for the damage that may be caused by the use of AIT.

The report states that, in order to provide sufficient protection, it is necessary to move away from private civil liability regimes and to establish common EU rules through a strict producer liability regime for defective products, applying in any case to those who have the most control over the risks of the operation. This regulation should be complemented by sector-specific liability rules in national legislation. The Report takes into account a number of issues where the involvement of humans in the creation of AIT and the use of algorithms takes precedence. It thus considers that the natural or legal person operating an AIT is liable for damage resulting from its operation. It also considers that the service provider bears liability when it can be demonstrated that it has a higher degree of control than the owner or user of the service. The manufacturer of products with digital content is also liable for damage caused by their products. Finally, and in general terms and regardless of the degree of autonomy of AIT, the individual must bear liability for the damage they may cause.

In this respect there are three proposals for dealing with the liability of a machine: 1) that all those involved in the value chain of the robot (creator, programmer, owner, user) are jointly and severally liable for the damage, 2) that the owner or user of the robot is liable, 3) that the liability lies with the AI itself through the creation of a "robotic personality" in addition to the natural and legal person.[42]

Evidently, according to the current legislation, imputation of liability to AIT is not possible, as it is always a person who assumes this obligation whether in their position as manufacturer, owner or user. On the other hand, the system of strict liability is adopted, the existence of damage and not of fault, in such a way that the cause of the damage is related to the liability and who bears this liability. In the case of AIT, machine

41 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM/2020/64 final, Brussels, 19.02.2020, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064 [access: 21.02.2022].

42 There is widespread opposition from the EU institutions to creating a robotic responsibility. See F. Ramón Fernández, *Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?*, Diario La Ley 2019, no. 9365, pp. 1–13.

AI is linked to machine learning, such that the greater the autonomy of the machine to perform a task, the greater the responsibility of the machine. Conversely, if human dependence increases, machine dependence will decrease at the same time.[43]

Translated to the financial sector, Tapia Hermida distinguishes between different types of responsibility and liability.[44] Firstly, social responsibility that requires financial institutions, on the one hand, to achieve digital literacy among their users, especially those who are most vulnerable, such as marginalised groups or those with some kind of disability. On the other hand, to ensure the training of highly qualified professionals in digitalisation. Secondly, civil liability of financial institutions to cover any damages that may be suffered by their customers due to the use of AI. This would be the case, for example, where a woman is denied a loan because of "gender bias" and loses an offer to buy a house.

This principle is closely related to the harm caused and has, in this sense, a double dimension. On the one hand, the general imputability to the agent prevents the defencelessness faced by AI users, as is the case, for example, with financial institutions using digitalised payment services. On the other hand, the specific imputability to the operator (both initial and final) of the AI in complex situations that obliges all those who have participated in the operation by exercising control during the AI process to be jointly and severally liable. This liability shall be claimed on a pro rata basis according to the degree of involvement of the operators in the risks of the transaction and the functioning of the AI system based on the traceability of the financial products used.

4.2.3. Preventive coverage: obligatory civil liability insurance

Preventive coverage is relevant for financial digitalisation both for the civil liability that financial operators may incur, as well as for the financial instruments used (liability insurance or bank guarantees).

In this respect, the requirement for compulsory civil liability insurance for high-risk AI systems should cover the amounts as well as the compensation provided for by law. This implies that all operators of high-risk AI systems must hold liability insurance with two aspects in mind. On the one hand, the profiles of these operators

---

43 Ibidem, p. 8. According to this author, in case of applying the fault system we are facing a *probatio diabolica*; hence, the strict liability, regardless of the intention, is the best method to obtain compensation. To complete the protection, the risk should be covered by an insurance that should be taken out by the machine manufacturer to assume its responsibility.

44 A.J. Tapia Hermida, *Decálogo de la inteligencia artificial*…, p. 4.

should be defined, as they are currently unclear, and on the other hand, the cost of insurance premiums should be limited so as not to discourage the development of the sector. To this end, it should be recommended that European legislators intervene by regulating the establishment of such insurance that is not at the mercy of the free market, offering innovative insurance policies and adequate cover at an affordable price. Otherwise, the insurance market will offer "one-size-fits-all" compulsory insurance with disproportionately high premiums which will have the effect of leading to cheap insurance with less coverage. Tapia Hermida considers that this compulsory insurance should be similar to the one that currently exists for motor vehicles.[45] Although at present the lack of accident statistics would make it difficult to develop new products adapted to AI.

With regard to the burden of proof, especially in the financial sector, it should be reversed, especially if it can be shown that AIT are the cause of the damage and also bearing in mind that the difficulties and cost of proof are very high. In this sense, it may be the case that the damage could have been avoided by following the safety rules, in which case there should be a reversal of the burden of proof with regard to causation, fault or the existence of a defect. With respect to causation, the burden of proof may be modified as long as the AIT ensure a number of factors such as the technology contributed to the damage, or the risk caused by a defect in the AIT.

4.2.4. Consumer protection

Consumer protection is fundamental to the EU, hence AI affecting consumers is comprehensively regulated to protect them to the fullest extent. In this regard, the protection subjectively covers both the user to whom the algorithm is addressed and those who are targeted by it. Geographically, the user is protected regardless of where the entities that develop, market or use an AI system are established, and finally at the functional level it covers both the developers and the entire value chain of AI systems.

Conclusions

The financial market is a risky sector that should be particularly attentive to the application of Ethical Artificial Intelligence developed through neutral algorithms

45 See: A.J. Tapia Hermida, *Decálogo de la inteligencia artificial*…, pp. 5–6.

that avoid bias and discrimination in the development of underlying data that may lead to automated discrimination especially with groups of people susceptible to stigmatisation by society.

Fundamental to this is the presence of transparency-related values in financial operations, as the characteristics of AI require that information accessible to supervisory and consumer protection authorities must cover the automation and operational processes. Global governance is another ethical principle that should govern the use of AIT in the financial sector, in particular with regard to accountability, as well as the establishment of systems that create security and confidence in the public when using technologies.

Furthermore, in order to address the damage that the misuse of AIT may cause, a two-fold principle of responsibility is necessary. On the one hand, social responsibility that requires financial institutions to assume a leadership role in which gender parity, digital literacy and innovation are present needs to be included. On the other hand, civil liability for damages that AI may cause to consumers and users constitutes a necessary element as well.

In this regard, digitalisation faces a key challenge: to establish a regulatory framework that generates AI standards in which consumers are users of an algorithmic system in which they are recipients regardless of the location of commercial or service activities. At the same time, and for the sake of legal certainty, standards should bind the entire value chain covering the development, deployment and use of technologies and their components.

The challenge now is to translate each of these principles into national legislation by ensuring a European policy of protection for consumers and users of AIT in the financial market. In this regard, the impact of the applicable laws from both dispositive and imperative law in order to give scope to the fundamental rights that the ethical principles protect needs to be analysed. The combination of consumer rules in relation to banking and insurance legislation will be crucial if we are to ensure that AI does not violate the values of transparency and neutrality of algorithms that govern the digit.

Bibliography

Arrow K., *The Theory of Discrimination*, in: *Discrimination in Labor Market*, ed. O. Ashenfeller, A. Rees, Princeton 1972.

Asimov I., *Runaround*, New York 1942.

Coeckelberg M., *Ética de la inteligencia artificial*, Madrid 2021.
Cotino Hueso L., *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 2019, no. 58.
Cotino Hueso L., *Riesgos e impactos del Big Data, la inteligencia artifcial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho*, Revista General de Derecho Administrativo 2019.
Council of Europe and Artificial Intelligence, https://www.coe.int/en/web/artificial-intelligence [access: 8.03.2021].
European Commission for Efficiency of Justice, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment*, Council of Europe 2019, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c [access: 22.02.2022].
European Data Protection Supervisor, *Opinion 4/2015. Towards a New Digital Ethics: Data, Dignity and Technology*, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf [access: 22.02.2022].
European Data Protection Supervisor, *Opinion 7/2015. Meeting the Challenges of Big Data. A Call for Transparency User Control, Data Protection by Design and Accountability*, https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf [access: 21.02.2022].
European Data Protection Supervisor, *Opinion 8/2016. Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf [access: 22.02.2022].
European Union Agency for Fundamental Rights, *Artificial Intelligence, Big Data and Fundamental Rights*, https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights [access: 8.04.2021].
Floridi L., *Soft Ethics and Governance of the Digital*, Philosophy & Technology 2018, no. 31.
Floridi L., et al., *AI 4 People. An Ethical Framework for a Good AI Society: Opportunities, Risk, Principles and Recommendations*, Minds and Machines 2018, no. 28.
Goodman M., *Futures Crimes: Inside the Digital Underground and the Battle for our Connected World*, New York 2016.
Lewis M., *Flash Boys: A Wall Street Revolt*, New York 2014.
Maldonado Ortega P.J., *Robots autónomos inteligentes y derecho civil. Reflexiones al hilo de las recomendaciones del Parlamento Europeo a la Comisión sobre normas de Derecho civil sobre robótica*, http://www.notariamaldonadortega.com/es/robots-autonomos-inteligentes-y-derecho-civil [access: 15.04.2021].
Marín García S., *Ética e inteligencia artificial*, Cuadernos la Cátedra CaixaBank de Responsabilidad Corporativa 2009, no. 42.
Masaro T., Norton H., Kaminski M., *SIRI-OUSLY 2.0: What Artificial Intelligence Reveals about the First Amendment*, Minnesota Law Review 2017, no. 717.
Monasterio Astobiza A., *Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos*, Dilemata 2017, no. 24.
Moniz Perea L., Saptawijaya A., *Programming Machine Ethics*, Berlin 2016.
Oliva León R., *Inteligencia artificial y marco ético europeo*, https://www.algoritmolegal.com/ [access: 6.03.2021].
Ramón Fernández F., *Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?*, Diario La Ley 2019, no. 9365.

Reijers W., Coeckelbergh M., *Narrative and Technology Ethics*, Cham 2020.
Steiner C., *Automate This: How Algorithms Came to Rule the World*, New York 2012.
Tapia Hermida A.J., *Decálogo de la inteligencia artificial ética y responsable en la Unión Europea*, Diario La Ley 2020, no. 9749.
Tapia Hermida A.J., *Digitalización financiera: Los 7 principios regulatorios de una Inteligencia Artificial Ética (IAE) en la UE. Resolución del Parlamento Europeo de 20 de octubre de 2020 sobre los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas*, http://ajtapia.com/2020/11/digitalizacion-financiera-los-7-principios-regulatorios-de-una-inteligencia-artificial-etica-iae-en-la-ue-resolucion-del-parlamento-europeo-de-20-de-octubre-de-2020-sobre-los-aspectos-eticos-de-la/ [access: 10.04.2021].
Tapia Hermida A.J., *Responsabilidad derivada del uso de la inteligencia artificial. Informe del Grupo de Expertos de la Comisión Europea de 2019 (1).Características esenciales de los regímenes de responsabilidad derivada de la inteligencia artificial y el uso de otras tecnologías digitales*, http://ajtapia.com/2020/01/responsabilidad-derivada-del-uso-de-la-inteligencia-artificial-informe-del-grupo-de-expertos-de-la-comision-europea-de-2019-1-caracteristicas-esenciales-de-los-regimenes-de-responsabilidad-derivad/ [access: 9.04.2021].
Taplin J., *Move Fast and Break Things: How Facebook, Google and Amazon Corneret Culture and Undetermined Democracy*, New York 2017.
Thaler R.H., Sunstein C.R., *Un pequeño empujón. El impulso que necesitas para tomar mejores decisiones sobre salud, dinero y felicidad*, Madrid 2009.