4

The Last Cocktail - Economic and Financial Crime, Corporate Criminal Responsibility, Compliance and Artificial Intelligence

(https://doi.org/10.47907/livro2021_4c5)

Anabela Miranda Rodrigues[1]

Abstract:
In the current global economic and financial scenario, in which corporations are the main protagonist, the issue of making them and/or their administrators, managers and employees responsible for crimes committed in the business sphere emerges. Compliance has been the "Columbus egg" for regulators and those subject to regulation in recent decades. This statement hides its potentialities and weaknesses, especially when criminal compliance is taken into account, as is the case with this study. Its socializing function is opposed to a security vision of compliance, which recovers the corporation as a «total institution». With AI systems that now combine compliance, it also becomes an "intelligent corporation". Still poorly redone from the trapdoors of vicarious responsibility and ambiguities of the organization defect, finding models of responsibility for corporate's crimes is, for criminal law scholars, again urgent.

Keywords: compliance; intelligent corporation; predictive process; corporate criminal liability.

[1] Full Professor of Law. Univ. Coimbra, University of Coimbra Institute for Legal Research, Fac. Law.

I. INTRODUCTION

In the current global economic and financial scenario, in which corporations are the main protagonist, it is not difficult to see how their activity can verge on the criminal, even giving rise to a new phenomenology of it. With their very complex organizational structures and them acting in contexts of increasing risk, the issue of making them and/or their administrators, managers and employees responsible for crimes committed in the business sphere emerges.

Compliance, as a law enforcement strategy and one of the pillars of corporate governance, is assumed as a vector for the assessment of criminal responsibility, and determination of the legal consequences arising from the practice of illicit activities, whose importance varies depending on the model of responsibility adopted by the corporation. In turn, the statement that we are living today in an era of a new business reality made possible not only by the enormous computational development, but above all by Systems of Artificial Intelligence (AI), whose application is enhanced by the enormous development of computing and cognitive communication – the "Internet of Things" (IoT) – will not come as a surprise to anyone. In such a scenario, networked "things" – machines and systems – communicate and interact with each other, showing themselves capable of predicting productive acts and processes in a very effective and efficient way, or preventing or detecting errors harmful to the company. Thus, such an algorithm has the advantage of increasing security in a business context by predicting, preventing and designing harmful acts or values, and monitoring the space and the people who intervene in it. The digital transition also favours the transfer of decisions in the business context to complex computer systems. Partially at least, several options taken throughout the production process are already decided by "things". That is, many of the tasks decided, assigned and previously performed by humans are now assigned to, decided on and performed by machines. However, an erroneous decision by an algorithm, causing injury to legal assets, is in critical conflict with a model of criminal liability built on the performance of a person, human or fictional, or in this case, the legal entity, in any of its models, which we will appreciate in this study.

II. COMPLIANCE - SOCIALIZING FUNCTION AND RISK MANAGEMENT

It is important to remember that the issue of good corporate governance and compliance arises in a most unusual context – that of regulated self-regulation. This involves self-regulation by private entities being subordinated to the purposes and interests of the state. This development means that calls for a need for regulatory intervention are heard ever more loudly, and, in the last resort, these must involve sanctions under the criminal law. Under such a regulatory strategy, the criminal law is like the last guest to arrive at a party, but without whose indispensable presence the festivities cannot start. The purpose of establishing measures of internal organisation of a corporation is not to create a normative programme that favours its activity 'on a knife edge' and allows it to evade criminal liability, but to delimit the perimeter of prohibited conduct, so that practices contrary to the defined rules of conduct can be prevented and suppressed. The possibility of criminal sanctions is a way of encouraging business leaders to establish effective control mechanisms. The motivation to ensure compliance with the control rules is thus the result of corporations overestimating the possibility of non-criminal prosecution and the establishment of procedural agreements or the provision for the exclusion or mitigation of their criminal liability.

In this regard, it should be noted that the compliance strategy, in the light of modern self-regulation, lives with a degree of state intervention different from what it classically was, in this sense, "less co-active and more dialogue". It is a question of focusing intervention, in particular administrative or even criminal, more on the quality and effectiveness of the internal self-regulation system and less, in accordance with the traditional public control model, on the repression of non-compliance with the rule by its addressee. It is a question of avoiding a method of action based on severe sanctions from the outset. In other words: the focus is on preventing corporate misconduct.

In this context, in which compliance is particularly important, the prevention of offence to legal values becomes a duty and a responsibility for corporations and gains a socializing sense – it is the socialization of modern times[2]. Compliance programmes aim to promote an ethical

[2] See Rodrigues, Anabela Miranda, *Direito Penal Económico - uma Política na Era Compliance*, Almedina, Coimbra, 2021, 2ª ed., p. 28s.

business culture and legal compliance, and their ultimate objective is to avoid the injury of legal values and the corresponding administrative, civil and ultimately, but above all, criminal liability. This compliance strategy uses a new type of law enforcement in which state action involves introducing a (new) level of law enforcement between the (violation of) the standard and the (application of) sanction or punishment. It is therefore not directed so much to sanction or punish as to "seek the cooperation and participation of infringers, with the aim of correcting the defects that led to the violation of a rule""[3]. In essence, it is a question of making them able to avoid similar behaviours in the future. In the context of business activity, this means that state intervention through compliance fulfils a socializing function.

The effectiveness of compliance thus understood takes into account an aspect that should not be over-ensured. And that lies in the finding that compliance with standards, in the context of the risk in which corporations currently carry out their activity, can involve real difficulties. It is here that the prodigious technological evolution that we are experiencing is felt, by favouring the appearance of algorithms capable of extracting and structuring, from big data, information relevant to business management[4]. One of its most common applications is based on the enormous capacity for business risk assessment, management and control. The most complex deep learning and AI-based technology solutions are of particular importance for their enormous analytical capability and the high capacity of accuracy and anticipation that they are recognized to have. Risk management by the 'machine' covers areas as diverse as the prevention and fight against fraud and the monitoring of the operation of a corporation - acting in the context of product and supplier management or even compliance with legal and regulatory obligations - and of its workers, and several advantages in reducing the enormous costs of regulatory compliance are recognized[5].

[3] See Martín, Adán Nieto, "Autorregulación, 'compliance' y justicia restaurativa", *Autorregulación y sanciones, Luis Arroyo Jimenez/Adán Nieto Martin* (Directores), Thomson Reuters, Aranzadi, 2ª Edición, 2015, p.117s (see, also, p.102).

[4] See Rodrigues, Anabela Miranda/ Sousa, Susana Aires, "Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal", *Julgar*, Nº45, Set-Dez., 2021 (ongoing publication), II, 2., 2.1

[5] See, in a developed way, Butler, Tom / O'Brien, Leona, "Artificial intelligence for regulatory compliance: Are we there yet?", *Journal of Financial Compliance*, Vol. 3, N 1, 2019, p. 44.

In the context of preventing and combating fraud, there are several concrete examples of practical applications that have been developed by financial institutions in order to meet requirements imposed by regulators, for example on money laundering. AI solutions promise continuous monitoring of the company, in turn facilitating the regulator's rapid access to information in the event of non-compliance. *Buttler and O'Brien*[6] refer to a revolution capable of transforming risk and compliance monitoring into a predictive process. The continuous monitoring of the company allows problems to be identified and solved in advance, providing "compliance breaches" and thus preventing the entity regulated (the corporation) from having to answer to the regulator and other judicial authorities. As the organization and analysis of data becomes more targeted and focused through AI, real-time information will enable the self-anticipation of risks and reach the "holy grail" of an intelligent compliance system, as *Aziz* and *Dowling*[7] point out. The prevention and fight against fraud also includes the application of new AI techniques as guarantors of the security and integrity of the financial system, preventing cyberattacks and signalling illegal or criminal situations. The critical software market capable of preventing and detecting fraud is expanding, with more and more companies specializing in the supply of these products. Take the case of *Feedzai*[8], a Portuguese financial technology *start-up*, specializing in fraud detection and cybercrime prevention in the financial and banking sector, using AI and machine learning techniques.

III. COMPLIANCE AND CRIMINAL LIABILITY OF LEGAL PERSONS

1. Compliance relief and intelligent algorithm

Assuming that the sanctioning, inter alia criminal, of much economic and financial behaviour was an overriding necessity, the

[6] See Butler /O'Brien, *Journal of Financial Compliance* (note 5), p. 45.

[7] See Aziz, Saqib / Dowling, Michael, "Machine Learning and AI for Risk Management", *Disrupting Finance*, Palgrave Macmillan, 2019, p. 47.

[8] The company has earned media attention for its international valuation of about $1 billion, giving it "unicorn start-up" status. In 2018, *Feedzai* had been considered one of the 50 most promising companies in the field of financial technology by *Forbes*, having received several international distinctions. See https://feedzai.com/about-us/

criminal law faced the first difficulties of accountability in relation to the aggression of legal values in 'collective action contexts[9]. The issue of criminal liability in this criminal field is a significant aspect in the conferral of this responsibility on so-called legal persons. This is what has largely fuelled the doctrinal discussion that has been waged around the possible imputation models of corporate criminal liability. These models can conform to two major systems: the vicarious or heteronomous model, in which the responsibility for the conduct of an administrator, manager or employee is transferred to the collective entity; and the other, which is based on corporate self-responsibility and the possibility of the company being liable for criminal liability for "organisational defect".

It is known that in continental Europe, contrary to the classical theory of criminal law based around the individual agent, an idea of criminal responsibility of collective entities has been established and gradually expanded. If the French criminal law of 1994 and the Belgian law of 1999 are referred to as having enshrined a regime regarded as exceptional and extravagant, it is a fact that the political-criminal solution of the criminal liability of legal persons was deserving of acceptance in criminal codes, even in countries traditionally averse to criminal liability of this nature, such as occurred in 2010 under the Spanish Penal Code. In Portugal, it was in 1984, with legislation regarding infringements against the economy and against public health[10], that the first steps were taken in the establishment of criminal liability of legal persons. Since then, the imputation of criminal responsibility to legal persons has gradually intensified, exponentially increasing the range of crimes that can be committed by them.

It is within an autonomous model of criminal liability that it has been considered that the adoption of compliance programmes can take on importance for corporations. Moreover, today, when considering this relevant fact, the use of intelligent algorithms in the field of self-regulation needs to be taken into account[11]. It is true that a

[9] See Sousa, Susana Aires, *Questões Fundamentais de Direito Penal da Empresa*, Almedina, Coimbra, 2019, p. 84s; see also, Rodrigues, Anabela Miranda, note 2, p. 110s.

[10] Law Decree nº28/84, the 20th January.

[11] See Rodrigues, Anabela Miranda/Sousa, Susana Aires, *Julgar* (note 4), III, 1., 1.1.

'smart enterprise' - capable of acting in continuous communication with and impervious to the organisation, to the extent that such defects would be corrected in advance by the algorithm - is still a vision situated in an uncertain future. An algorithmic-based compliance system that automates a company in fulfilling the obligations imposed by regulators, and thus capable of excluding its eventual liability, while an ongoing challenge being tackled by some corporations, is yet to be realized. In legal systems that include models in which the imputation of a criminal act to a legal entity is based on a defect in organization, as happens in Italy or Spain, the "intelligent" compliance software is presented with the promise of being a powerful tool to exclude the legal entity from responsibility, by first of all furnishing the proof that the company organized itself in such a way as to comply with the law. On the corporate side, the advantages of an intelligent compliance system are thus, at first sight, of a dual nature, tangible and normative: the first, concerned with the mitigation or elimination of error and a the consequent increase in security; the second, bringing the business activity closer to a strict regulatory compliance framework capable of excluding the company from any liability.

2. Responsibility of legal persons: again?

There is in general a problematic side to compliance, which translates as the distrust of the justice system in relation to it, considering it an "invention of the business world"[12]. What is said is that the corporations with the greatest bargaining power, large companies, have the increased capacity to convince the criminal investigation bodies – sometimes, with little information and knowledge in these matters – that the system of organisation they have adopted is sufficiently effective to prevent the commission of crimes, and that any crime committed is the result of purely isolated and individual behaviour, of a managing director or employee. From pointing to a scapegoat to avoiding criminal liability is a small step for the corporation. This is especially true for legal regimes that accept corporate self-responsibility or even mixed models of liability. The particularly perverse effect of this strategy,

[12] See Rodrigues, Anabela Miranda (note 2), p. 115, with bibliographical references.

known as '"reverse whistleblowing'"[13], is that the company, in order to give consistency to its version of the facts that it is well organized – with cosmetic use of compliance programmes - seeks an individual on whom it can pin the blame. Adoption of such a strategy is additional harmful to the legal system if the collective entity is offered immunity from or mitigation of punishment, or even a non-criminal persecution in exchange for the naming of the individual responsible. In this regard, the paradoxical effect of corporate autonomous criminal liability has been denounced[14] and it is termed an ongoing creation of a 'friend's criminal law' for businesses[15].

As for a model of heteronomous responsibility, failures can be pointed out especially in large companies, where it is more difficult, by virtue of their complexity, to find an individual responsible, and basing the responsibility of the corporation on an action or omission of an individual. To condition the company's responsibility to demonstrate, for example, that any manager of the organisation, in relation to a specific criminal act and a subordinate, has breached his or her supervisory duties, would mean desecrating a model of corporate responsibility that would benefit large companies and harm smaller ones, since in these it is much easier to locate responsibility or the concrete lack of vigilance of a superior, administrator or manager. In any case, this form of imputation of criminal liability to companies - which runs the risk of translating, in judicial practice, into an objective imputation of liability that derives automatically from individual responsibility - promotes a business reaction of concealment of crime and alliance with the offender, which reaches the level of obstruction of justice: the

[13] The expression is from Kimberley, D. Krawiec, "Cosmetic Compliance and the Failure of Negotiated Governance F. Hodge O'Neal Corporate and Securities Law Synposium – After the Sarbanes-Oxley Act: The Future of the Mandatory Disclosure System", *Wash U.L.Q.,* 81, 2003, p. 487s.

[14] See Laufer, William S., last, in 2018, "A very special regulatory milestone", *Univ.Pa.J. Bus.Law,* Vol. 20.2., p.391s. See also, Mendes, Paulo Sousa, "*Law Enforcement & Compliance*", *Estudos sobre law enforcement,* Almedina, 2018, p. 26s e Sousa, Susana Aires, *Questões Fundamentais, cit.,* p. 127 e 128

[15] About this, see Rodríguez, Laura Zuñiga, "Responsabilidad penal de las personas jurídicas y derechos humanos. Una valoración desde la reforma de 2015 de la legislación española", *Derecho Penal Económico y Derechos Humanos,* Eduardo Demetrio Crespo, Adán Nieto Martín (Directores), Manuel Maroto Calatayud, Mª Pilar Marco Francia (Coordinadores), Tirant lo blanch, Valencia, 2018, p. 106s.

company is not interested in assisting the investigation, as ultimately its discovery may translate into its conviction. Its fortune is united with that of the person responsible, who turns into its ally.

The introduction of AI into business activity introduces new difficulties to the difficulties already known about from the models of imputation to legal persons, through both individuals and collective individuals.

The issue lies in so-called "intelligent" algorithms, technologically complex, capable of autonomously classifying qualifying options as criminal, but which had not been pre-programmed in this sense even when such decisions were predictable to the programmer (*cognitive robots*)[16]. The novelty is then in the fact that the machine, as a machine that learns", obtains a new result that is, in a sense, its own. As an artificial intelligence system, a "learning machine" must not be confused with a complex data processor, that is, it is not limited to calculating the best option among the thousands of items of data that have been introduced to it, such analysis being inaccessible or very difficult for a human. Rather, the algorithm, powered by data, continually adjusts itself in order to decrease the margin of error and create its own decision. It is this dynamic nature of the machine – its autonomy – that challenges the attribution of responsibility to the people behind the machine, whether physical or legal[17].

It is in this context that the most difficult issues of imputation of corporate criminal liability are identified[18]. In a vicarious model, the question is how to impute the criminally relevant decisions and actions carried out by the machine, under the conditions described, to individuals. In an autonomous model of responsibility, difficulties arise to the precise extent that the "defect" of the algorithm is not

[16] On the distinction between cognitive robots and deterministic robots - pre--programmed for the practice of a given criminal activity - clearly, in the context of robots, see *Report of COMEST on Robotic Ethics*, 2017, p. 48, https://unesdoc.unesco.org/ark:/48223/pf0000253952

[17] On the difficulties present here in the area of the imputation of penal responsability, see Sousa, Susana Aires, "'Não fui eu, foi a máquina': teoria do crime, responsabilidade e inteligência artificial", *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), Almedina, Coimbra, 2020, p. 65s with bibliographical references.

[18] See Rodrigues, Anabela Miranda/Sousa, Susana Aires, *Julgar,* (note 4), III, 1., 1.1.

known and, as such, preventable and avoidable. The cognitive ability of the machine makes it unpredictable, able to react to the unexpected, and removes its decision from the mastery of predictability of the programmer. It is this space of freedom that is granted to the machine, exploiting its learning abilities, which cannot be determined (or prevented). The "defect" in the algorithm does not exist; it is a future defect and therefore escapes self-organization ... of the algorithm... and thus also the corporation! At least in an abstract sense, if the offence caused by learning of the algorithm leads to an unpredictable outcome, one can hardly blame the corporation for not avoiding a risk it could not know.

At the present time, intelligent business self-organization will not eliminate wrong decisions made by intelligent software, which are proven examples of discriminatory options in hiring or firing workers, price combination situations or phantom financial transactions[19].

In fact, digital transformation of the corporation evidences a patent non-conformity between the technological evolution of corporations and the models legally provided to assess their criminal liability, in turn unveiling a gap already identified by some discourse on the subject. The various proposals for a solution call for an extension or reconfiguration of the assumptions of criminal liability. Faced with the manifest difficulty in making a human, natural, person responsible, the hypotheses oscillate between the modification and updating of the assumptions of corporate responsibility to the most radical ones that propose making the machine responsible.

Referring specifically to this problem, *Mihailis Diamantis* seeks to propose making a corporation responsible, exploring a model that consists of adapting to the business context of "extended mind thesis"[20]. From this perspective, in the process of automating the company, algorithms integrate the way the company thinks and takes decisions and,

[19] On the problem involved here and the crimes of market abuse committed by artificial agents, see RODRIGUES, Anabela Miranda, "Os crimes de abuso de mercado e a "Escada Impossível" de *Escher* – o Caso do *Spoofing*)", *Julgar*, Nº45, Set.-Dez. 2021 (ongoing publication), *passim*.

[20] DIAMANTIS, Mihailis E., "The Extended Corporate Mind: When Corporations Use AI to Break the Law", 98 N.C. L. Rev. 893 (2020); also, BRYSON / DIAMANTIS/ GRANT, "Of, for, and by the people: the legal lacuna of synthetic persons", *Art. Intelll Law* (2017), p. 273 e ss.

thus, constitute an extension of its mental state and will, linking it thus with its criminal responsibility.

On the other hand, the supposed insufficiency of the classic legal schemes of attribution of criminal liability have constituted a decisive impulse for the emergence of theoretical proposals that advocate an electronic legal personality, on the civil plane, and a consequent direct criminal liability of the machine as a response to the responsibility / accountability gap. For example, *Gabriel Hallevy* proposes the seemingly simple idea that if the assumptions of criminal liability in an entity are verified, it must be held accountable, be it a physical entity, a collective entity or an artificial entity[21]. In a clear utilitarian understanding of criminal liability, the extension of criminal law to autonomous and intelligent machines would not require, in the author's view, major changes to the assumptions required by this responsibility, it being possible to identify, in the performance of AI, the external (*actus reus*) and mental (*mens rea*) elements required by criminal liability.

IV. CORPORATE CRIME, ACCOUNTABILITY, COMPLIANCE AND AI: THE LAST COCKTAIL

Talking about *compliance* means having in mind the possibility of conceiving two standard models of programmes: one, which may consist of promoting an ethical culture and legality; and another, which is rooted in surveillance or control mechanisms.

Thus[22], according to the first model, the compliance program, whose central element is the ethical code, is oriented towards the promotion of values. It relies, of course, on control measures, which are seen as the normal internal procedures for the operation of a corporation focused on business ethics, namely due diligence, which is

[21] Hallevy Gabriel, "The Criminal Liability of Artificial Intelligence Entities – From Science Fiction to Legal Social Control", *Akron Intellectual Property Journal* Vol. 4, Issue 2 (2010), p. 199; *id*, *Liability for crimes involving artificial intelligence systems*, Springer, 2015, p. 61. For a critical assessment of the construction of this author, Sousa, Susana Aires, (note 17), p. 77s. In critical sense, see also Rodrigues, Anabela Miranda, "A justiça preditiva entre a americanização e a europeização", *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), Almedina, Coimbra, 2020, p. 52s.

[22] See Rodrigues, Anabela Miranda (note 2), p. 105s.

fundamentally thought of as an instrument for promoting an 'illicit--free' business environment, internalised by all as a reputational added value and in terms of the value of the corporation. In this model, crime reporting is integrated into the corporate culture as a corporate civic act and not with any pejorative connotation[23]. The second is seen as a function of surveillance, and at its heart are control measures. A compliance model from surveillance and control has ingredients - such as using video surveillance circuits, phone records or internet access - that run the risk of converting the company into a kind of *panopticum* and giving the entrepreneur a *big brother* position. In the age of intelligent compliance, perhaps the most appropriate image is that of a "Ubiquitous Digital Architect", of which Soshana Zubof speaks[24]. What's more, criminal compliance becomes a source of misconceptions. The toughening of systems of detection, of reporting, of investigation, the publicity of sanctions (shaming) or the increasing criminalization of many violations of compliance duties criminalize compliance. This new near-criminal law is private. Certainly, the dangers of the privatization of criminal justice are not born out of this new compliance strategy; but it does create new problems.

In this context, it is generally observed that such a model would be incompatible with workers' fundamental rights, such as to a private life or intimacy, the secrecy of communications or the right to data protection. And it's easy to understand how scanning powers this model and powers its costs[25]. The continuous monitoring of workers facilitates

[23] The way the reporting channels work is a telling sign of the compliance model deployed. It is essential for an ethical model for channels to be anonymous and specific, enabling administrators and employees and people outside the company to communicate, under conditions of confidentiality, situations that may pose business risks. In this way, it is not necessary to foster an environment of persecution among the staff of the company and of persecution of the staff of the company. And, thus, on the one hand, preventing not only situations of complaints of bad faith, since confidentiality does not prevent the responsibility and sanctioning of the whistleblower, if this is the case; and, on the other hand, seeking to safeguard whistleblowers of good faith communications from disciplinary, professional or criminal repercussions.

[24] See Zuboff, Shoshana, "A Era do Capitalismo de Vigilância. A disputa por um futuro humano na nova fronteira do Poder", Relógio D'Água, 2020, p. 389s.

[25] See Rodrigues, Anabela Miranda/Sousa, Susana Aires, *Julgar* (note 4), III, 2.; see, also, Sousa, Susana Aires, "As diferentes faces dos programas de compliance", Legitimidade e efetividade dos programas de compliance (or. Adán Nieto Martín/Eduardo Saad Diniz), Tirant lo blanch, 2021, p.29s.

the identification of error and, above all, facilitates the pointing out individualized failure of an individual's conduct, identified and indicated by the algorithm. The presumption of liability thus established is added to the double transfer of responsibility from the corporation to individual persons, and among such transfers, from the directors to middle or lower-level management of the corporation (*top-down*). Indeed, the algorithm has the ability to accurately identify the timing of the error, disregarding the context and the "film of the event""[26]. The repercussions at the procedural level, on the presumption of innocence, are evident from this: the "photograph" of the error relieves the company and shifts the burden on to the defence of the worker. The algorithm allows the company to easily overcome the test of the abstract-concrete adequacy of the compliance program by increasing the possibility of excluding its liability at the expense of the presumption of guilt of the worker[27].

V. CONCLUSION

Compliance has been the "Columbus egg" for regulators and those subject to regulation in recent decades. This statement hides its potentialities and weaknesses, especially when criminal compliance is taken into account, as is the case with this study. Its socializing function is opposed to a security vision of compliance, which recovers the corporation as a total institution. With AI systems that now combine compliance, it also becomes an "intelligent corporation". Still poorly redone from the trapdoors of vicarious responsibility and ambiguities of the organization defect, finding models of responsibility for corporate's crimes is, for criminal lawyers, again urgent.

[26] See Rodrigues, Anabela Miranda (note 2), p. 112, note 229.

[27] On this issue of particular relevance in autonomous models of criminal liability of companies, Rodrigues, Anabela Miranda, *Direito Penal Económico,* (note 2), p. 112 e s; *id*, "Compliance programmes and corporate criminal compliance", *Polar – Portuguese Law Review,* Vol. 2, January 2018, n.º 1, p. 5s. In the procedural context, it is also important to consider that the algorithm is also a means of obtaining proof, of private creation. In the Portuguese legal order, on the side of the evidential use of this information for the purposes of criminal liability, there will always be the limits insurmountable to its validity, in the light of Article 32(8) of the Constitution and Article 126 of the Code of Criminal Procedure.

REFERENCES

AZIZ, Saqib / DOWLING, Michael, "Machine Learning and AI for Risk Management", *Disrupting Finance*, Palgrave Macmillan, 2019.

BRYSON, J.; DIAMANTIS, M.; GRANT, T. D., "Of, for, and by the people: the legal lacuna of synthetic persons", *Art. Intelll Law* 25 (2017), p. 273-291.

BUTLER, Tom / O'BRIEN, Leona, "Artificial intelligence for regulatory compliance: Are we there yet?", *Journal of Financial Compliance*, Vol. 3, N 1, 2019.

DIAMANTIS, Mihailis E., "The Extended Corporate Mind: When Corporations Use AI to Break the Law", *98 N.C. L. Rev*. 893 2020.

HALLEVY Gabriel, "The Criminal Liability of Artificial Intelligence Entities – From Science Fiction to Legal Social Control", *Akron Intellectual Property Journal* Vol. 4, Issue 2 (2010).

--- *Liability for crimes involving artificial intelligence systems*, Springer, 2015.

KIMBERLEY, D. Krawiec, "Cosmetic Compliance and the Failure of Negotiated Governance F. Hodge O'Neal Corporate and Securities Law Synposium – After the Sarbanes-Oxley Act: The Future of the Mandatory Disclosure System", *Wash U.L.Q.,* 81, 2003.

LAUFER, William S., "A very special regulatory milestone", *Univ.Pa.J. Bus.Law,* Vol. 20.2., 2018.

MARTÍN, Adán Nieto, "Autorregulación, 'compliance' y justicia restaurativa", *Autorregulación y sanciones, Luis Arroyo Jimenez/Adán Nieto Martin* (Directores), Thomson Reuters, Aranzadi, 2ª Edición, 2015.

MENDES, Paulo Sousa, "*Law Enforcement & Compliance*", *Estudos sobre law enforcement,* Almedina, Coimbra, 2018.

RODRIGUES, Anabela Miranda, "Compliance programmes and corporate criminal compliance", *Polar – Portuguese Law Review,* Vol. 2, January 2018, n.º 1.

---- "A justiça preditiva entre a americanização e a europeização", *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), Almedina, Coimbra, 2020.

---- *Direito Penal Económico: Uma Política Criminal na Era Compliance*, 2ª Ed, Almedina, Coimbra, 2021.

---- "Os crimes de abuso de mercado e a "Escada Impossível" de *Escher* – o Caso do *Spoofing*)", *Julgar*, Nº45, Set.-Dez. 2021 (ongoing publication).

Rodrigues, Anabela Miranda/ SOUSA, Susana Aires, "Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal", *Julgar*, Nº45, Set-Dez., 2021 (ongoing publication).

Rodríguez, Laura Zuñiga, "Responsabilidad penal de las personas jurídicas y derechos humanos. Una valoración desde la reforma de 2015 de la legislación española", *Derecho Penal Económico y Derechos Humanos,* Eduardo Demetrio Crespo, Adán Nieto Martín (Directores), Manuel Maroto Calatayud, Mª Pilar Marco Francia (Coordinadores), Tirant lo blanch, Valencia, 2018.

Shoshana Zuboff, "A Era do Capitalismo de Vigilância. A disputa por um futuro humano na nova fronteira do Poder", Relógio D'Água, 2020.

Sousa, Susana Aires, *Questões Fundamentais de Direito Penal da Empresa*, Almedina, Coimbra, 2019.

----, "'Não fui eu, foi a máquina': teoria do crime, responsabilidade e inteligência artificial", *A Inteligência Artificial no Direito Penal* (coord. Anabela Miranda Rodrigues), Almedina, Coimbra, 2020.

----, "As diferentes faces dos programas de compliance", Legitimidade e efetividade dos programas de compliance (or. Adán Nieto Martín/Eduardo Saad Diniz), Tirant lo blanch, 2021.