1

"Intelligent Compliance"

(https://doi.org/10.47907/livro2021_4c2)

Pedro Maia[1]

Abstract:
Compliance and Artificial Intelligence (AI) are now at the center of banking regulation and banking activity. The way these two realities combine raises a variety of questions, challenging both corporate law and banking law. We try to identify and analyze some of those questions.

Keywords: artificial intelligence; banks; compliance

INTRODUCTION

Ensuring compliance by way of artificial intelligence (AI)[2], which I refer to as "intelligent compliance", is a crossroads of several (r)evolutions which are either underway in the banking sector or which it's keeping track of.

On the one hand, the emergence and growth of a kind of compliance subject to a framework and to a breadth and set of demands

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

[2] The expression appears to first have been used by John McCarthy, in 1956. *See* Scopino, Gregory, *"Key Concepts: Algorithms, Artificial Intelligence, and More"*, in Algo Bots and the Law. Technology, Automation, and the Regulation of Futures and Other Derivatives, Cambridge University Press, Cambridge, 2020, p. 19.

without parallel in the past. Globalization first contributed to this by forcing countries to face added difficulties with regard to the control and prevention of economic crimes, something which shaped the need to call on the banking sector to cooperate in the fight against money laundering and the financing of terrorism ('AML compliance'). This was joined by a new circumstance, which one might say *appeared from within the banking sector itself*, stemming from the regulatory framework come out of the 2007-2008 financial crisis. With the colossal growth of regulatory demands targeted at credit institutions, the re--dimension of the internal system in each of them, so as to ensure the control of and compliance with all the demands imposed on them (regulatory compliance), became imperative.

To this effect, the growth of compliance is a direct reflection of the regulatory structure's huge expansion. The current pandemic now stands side-by-side with the legacy of the financial crisis: until August 2020, over 1330 regulatory measures had been announced by regulators (internationally) and around 15% of prudential regulation was either altered or affected. On April the 2nd, 2020, over 75 publications[3] were made in 24 hours. Technological solutions which allow for the identification of the origin, the classification and the forwarding of regulatory changes to the relevant persons in charge of handling them within a financial institution have become valuable in meeting the demands of regulatory compliance[4].

On the other hand, the growing use of technology, including AI, for compliance resonates both with the function's own capabilities and with the associated risks. "Intelligent compliance" incorporates external risks connected to the technology and to the data used in the function itself.

On another hand still, the emergence of new compliance centralities, whether by turning to non-financial companies for help with the activity (service providers whose scope of business is strictly technological) or by the activity's mentioned re-centering: instead of being centered on knowing the client ('know your client' – KYC), a new

[3] *See* JWG, "Out of the window: COVID-19 prompts unexpected regulatory change for 2020 compliance, risk management work plans", 2020 (available at https://www.corlytics.com/newsreleases/out-of-the-window-covid-19-prompts-unexpected-regulatory-change-for-2020-compliance-riskmanagement-workplans).

[4] *See "2021: A Critical Year of RegTech"*, in The Global City, 2021, p. 19.

spotlight shines on data ('know your data' – KYD)[5]. From this evolution, a new stage of *RegTech* will emerge: *RegTech 2.0* will become *RegTech 3.0.*

Problems specific to the banking sector – related to the function which compliance plays therein – are joined by the countless challenges posed by the use of Artificial Intelligence, which the scientific community and authorities are rapidly becoming aware of [6].

First of all, I will present the compliance function by briefly describing its origin, evolution, and current framework. Thereafter, I will succinctly describe the importance of technology to the banking sector in general, after which I will again succinctly present some of the elements necessary to the understanding of AI and, more generally, of automation technologies. A description of the usefulness of such technologies to banking compliance will follow. Lastly, I will reflect on the risks and challenges posed by AI on several different levels.

I. DEFINITION AND EVOLUTION OF COMPLIANCE

The definition of "compliance", in the sense of *observance of the law* (understood in a broad sense) or of "acting in observance of the law", appears at first sight to be nothing more than a truism[7]: the duty to observe the law (in a broad sense) undoubtedly comes from the *principle of the rule of law* and, as such, compliance is neither a recent evolution[8]

[5] *See* Jung, John Ho Hee, *"RegTech and SupTech: the future of compliance"*, in FinTech – Law and Regulation, Elgar Financial Law and Practice, United Kingdom, 2019, p. 260, Arner, Douglas W., Barberis, Jànos, and Buckley, Ross P., *"Fintech and Regtech in a Nutshell, and the Future in a Sandbox"*, in CFA Institute Research Foundation, 2017, p. 3, Arner, Douglas W., Barberis, Jànos, and Buckley, Ross P. *"FinTech, RegTech, and the Reconceptualization of Financial Regulation"*, in Northwestern Journal of International Law & Business, Vol. 37, No. 3, 2016, p. 405, Arner, Douglas W, Barberis, Janos Nathan and Buckley, Ross P, *"The emergence of RegTech 2.0: From know your customer to know your data"*, in Journal of Financial Transformation, vol. 44, 2016, p. 7.

[6] *See*, for example, Arner, Douglas W., Barberis, Jànos, and Buckley, Ross P., *"Fintech…"*, cit. p. 6 ff.

[7] In this sense, *see* Uwe Schneider, "Compliance als Aufgabe der Unternehmensleitung", *ZIP*, 2003, p. 646.

[8] In the sense that, as a duty to observe the law, compliance is inherent to the principle of the rule of law, *see Hauschka/Moosmayer/Lösler Corporate Compliance*, 3. Auflage, 2016, annot. 2.

nor possesses its own or specific content. All entities, including those of the banking sector, must therefore observe the law.

But that's neither the current specific meaning of compliance nor the meaning with which it came to be. Indeed, the fact that that's not its meaning is precisely the reason why compliance progressively moved further away from *legal departments*, so as not to be confined to a strict assessment of legal compliance[9].

Compliance may be defined in different ways, holding different characteristics or resulting from different perspectives. It may be defined as a system and set of processes through which an organization undertakes to ensure that its employees and other persons in charge act in accordance with the *"rules"*; besides the law in a strict sense, within these rules one finds the whole regulatory catalogue and the organization's own internal rules such as codes of conduct. Or it may be defined as the "set of internal processes used by a company to *adapt its actions to the applicable rules"*[10]. It may be connected to the "*effort* to ensure that the company and its employees follow legal and regulatory requisites, industry practices, and the company's own policies and internal regulations[11]. Or it may be connected to the "company's set of systems and processes created with the objective of avoiding civil or

[9] The advantages and inconveniences of separating compliance from legal services have been highly debated. *See* ARMOUR, JOHN, GARRETT, BRANDON L., GORDON, JEFFREY N. and MIN, GEEYOUNG, *"Board Compliance"*, in Minnesota Law Review, Vol. 104, 2019, p. 1210 ff., and Mcneece, John B., *"The Ethical Conflicts of the Hybrid General Counsel and Chief Compliance Officer"*, in Georgetown Journal of Legal Ethics, Vol. 25, 2012, p. 677 ff. The matter must be taken into account within the scope of *innkeepers* as *gatekeepers* (but it's a debatable subject: critically, *see* Gadinis, Stavros and Miazad, Amelia, *"The Hidden Power of Compliance"*, in Minnesota Law Review, Vol. 103, 2019, p. 2154 ff.). On this matter, *see* Simmons, Omari Scott and Dinnage, James D., *"Innkeepers: A Unifying Theory of the In-House Counsel Role"*, in Seton Hall Law Review, Vol. 41, No. 1, 2011, p. 77 ff. (with the eloquent use of the expression "innkeeper" as a reference to persons who act as gatekeepers from within the organization itself).

[10] *See* Griffith, Sean J., *"Corporate Governance in an Era of Compliance"*, in William & Mary Law Review Online, Vol. 57, No. 6, 2016, p. 2082. In a very similar sense, Baer, Miriam Hechler, *"Governing Corporate Compliance"*, in Boston College Law Review, Vol. 50, 2009, p. 958, Orozco, David, *"A Systems Theory of Compliance Law"*, in University of Pennsylvania Journal Business Law, Vol. 22, No. 2, 2020, p. 250 ff.

[11] *See* Martinez, Veronica Root, *"The Compliance Process"*, in Indiana Law Journal, Vol. 94, 2019, p. 205.

criminal liability by the organization or its bodies”[12] (italics have been used as a way of highlighting the elements particular to each of the definitions).

Although each of these definitions emphasize different characteristics, none takes on compliance based on the *outcome*: it is not, therefore, about ensuring that *the law is complied with* – including regulatory and recommendatory dispositions and internal regulations, in a very broad sense – but rather about *creating a system* (made up of means, processes, and procedures) with the goal of both avoiding the breach of the legal framework within the company and of ensuring that, should a breach occur, it is detected. Compliance’s current theoretic framework is essentially procedural in nature[13], which of course drives it away from a substantial result. Compliance is thus directed at the *prevention of risk* and, because it is so, its worth isn’t measured by a case of breach of law (always in a broad sense) that may actually occur, but instead by any breach of law that may *probably* occur in face of the existing system and processes of prevention. The occurrence of a particular breach within the company isn’t in and of itself evidence of compliance’s fragility – much less of a breach of compliance duties[14]. Conversely, the non-occurrence of a normative breach by itself doesn’t mean that no compliance duties have been breached.

Since compliance (much like other control functions in any credit institution) is linked to *risk*, and since a company’s resources are limited, the past several years have seen what some authors call a “risk revolution” in internal and external control[15]: the design of internal control systems, including compliance, now consists of a risk evaluation which, after completed, is abided by. This is entirely understandable given that the existing means are finite and must be allocated to areas where a greater risk is detected. This “risk-based approach” has the advantage of allowing the company to essentially focus on the features where there

[12] *See* Gunnar Groh, in Creifelds kompakt, Rechtswörterbuch, 4. Auflage, 2021, Beck-online.

[13] *See* Orozco, David, *“A Systems...”*, cit., p. 254 ff. and the very recent *Principles of Law Compliance, Risk and Management, and Enforcement*, of the American Law Institute (§3.01).

[14] Insofar as such a duty exists.

[15] *See* Miller, Geoffrey Parsons, *“Compliance: Past, Present and Future”*, in University of Toledo Law Review, Vol. 48, 2016, p. 446.

is a greater risk of a harmful event occurring, although it's important to acknowledge that the approach itself entails a risk, in that it relies on an inadequate assessment of risk. With that being the case, the systems, which were built on top of a mistake, aren't suitable to prevent the occurrence of a harmful event[16].

This has another highly relevant implication still. A so-called "zero tolerance" to breaches of compliance has repeatedly been heard in the discourse of politicians, regulators, and even regulated entities. This approach is in and of itself *conceptually incompatible* with the officially adopted "risk-based approach". "Zero tolerance" would literally entail something which is unreachable and economically unsustainable: the company being absolutely certain at all times of not being in breach of any rule (in a broad sense) with regard to all of its actions. Such an approach is not only impossible; it would actually be the opposite of a "risk-based approach", which consists exactly of weighting a risk and then determining which issues compliance control should be directed at and which means it should make use of[17].

Compliance also appears to be undertheorized[18]: *compliance law*[19] *is still little studied and little defined as a theoretic unity*, ultimately being determined by somewhat isolated legislative or regulatory interventions and led by practical developments that at any given moment direct its normative content.

[16] The path leading to the financial system's sub-prime crisis appears to prove not only a possibly incorrect perception of risk – in general – but also the inability of control systems of preventing that damaging event. *See* MILLER, GEOFFREY PARSONS, "*Compliance...*", cit., p. 447 ff. Another example may surely be found in the (already materialized) risk of a global pandemic, which although possible was not identified.

[17] *See* MILLER, GEOFFREY P., *"Risk Management and Compliance in Banks: The United States and Europe"*, in European Banking Union, Oxford, United Kingdom, 2015, p. 211.

[18] *See* GRIFFITH, SEAN J., *"Corporate..."*, cit., p. 2081, and OROZCO, DAVID, *"A Systems..."*, cit., p. 246.

[19] We will not delve deeper into the hotly debated issue of knowing whether compliance is an independent field of study. *See*, for example, SOKOL, D. DANIEL, *"Twenty-Eighth Annual Corporate Law Center Symposium: Rethinking Compliance"*, in University of Cincinnati Law Review, *V*ol. 84, No. 2, 2016, p. 401 ff. (highlighting the huge variety of understandings when it comes to compliance and the resulting difficulty in creating a field of law), MARTINEZ, VERONICA ROOT, *"The Compliance..."*, cit., p. 244, and OROZCO, DAVID, *"A Systems..."*, cit., p. 251 ff.

Compliance's somewhat theoretic vagueness may be attributed to its origin, wherein two distinct paths of evolution can be found: one of a *practical* and *managerial* nature, dictated by the convenience of creating a specific function for internal control independent from legal departments; another of a *regulatory* or *legislative* nature, dictated by the (legislators' and regulators') need to introduce within organizations a body meant to either ensure the observance of the applicable normative structure or prevent transgressions within the company. The first corresponds to what may be referred to as compliance's *positive side*, in which it acts as an instrument or element which strengthens the business and allows for its success; the second corresponds to compliance's *negative side*[20]*, in which it serves the purpose of avoiding or preventing the organization from breaching its legal background. This negative side* may in turn take very different characteristics depending on the regulators' approach: it can be more *prescriptive*, imposing contents *specific* to internal control on the entities supervised; or it can be more *flexible*, granting companies ample freedom in deciding their own systems.

The first mentioned path of evolution is guided by the company's interests and, because it is developed from a judgement of *opportunity* and *convenience of management*, leaves compliance subject to the *management's discretion* in light of the interests pursued by the company and, more important, of its shareholders. In this path, compliance is also an instrument destined to satisfy the interests pursued by the company and is thus *in line with* one view of corporate interest – coinciding with that of the shareholders (profit or maximization of value), should that be the case. From this perspective, compliance is, after all, the *management of corporate risk*[21] *– in this case, the risk of breaching the*

[20] Also making this distinction, *see* Cunningham, Lawrence A., *"The Appeal and Limits of Internal Controls to Fight Fraud, Terrorism, Other Ills"*, in The Journal of Corporation Law, Vol. 29, 2004, p. 267 ff., and Chiu, Iris H-Y, *"Regulating (From) the Inside. The Legal Framework for Internal Control in Banks and Financial Institutions"*, Hart Publishing, Oxford, 2015, p. 8 ff.

[21] The management of corporate risk may be defined as the process through which the management body delineates the strategy and objectives that will allow the company to reach an optimal balance between growth, return, and related risks. *See* Bainbridge, Stephen M., *"Caremark and Enterprise Risk Management"*, in The Journal of Corporation Law, Vol. 34, 2008, p. 967. In a similar sense, *see* Der Elst, Christoph and Van Daelen, Marijn, *"Risk Management in European and American Corporate Law"*, in ECGI-Law Working Paper, No. 122, 2009, p. 6.

law and of having to face the consequences arising therefrom – and ends up overlaying or falling within so-called risk management: the system designed to handle all risks which a company is exposed to[22].

The second path of evolution, dictated by legislators and regulators and appearing at a later stage, most notably after the 2007-2008 financial crisis, is of a completely diverse nature. It's not about compliance as an instrument aimed at the pursuit of corporate interests, but instead as a safeguarded set of (legal and regulatory) dictates: a way of *ensuring* that the company's business does not harm the interests that such dictates seek to protect; interests which naturally do not coincide with those of the company but (as well) with those of *third parties*, with *public interest*, with the interests of certain categories of persons[23]. In this second path of evolution compliance is no longer an *instrument in the satisfaction of corporate interest* – therefore of a discretionary nature, defined and limited by each company's freedom in management – but instead an instrument designed to satisfy interests foreign and unavailable to the company – therefore of an *imperative* and *hetero-determined* nature[24].

It truth, besides these two paths of evolution, a third, more visible in jurisdictions such as the United States of America, may still be identified. In it, compliance plays a rather indirect and instrumental role, although still with great practical relevance with regard to one point in particular: that of the *accountability*, above all criminal, of

[22] *See* Bainbridge, Stephen M., *"Caremark..."*, cit., p. 968 (defending that between risk management and compliance there is no difference of nature, only a difference of level).

[23] Defending the dimension of social responsability, *see* Rodrigues, Anabela Miranda, *Direito Penal Económico: Uma Política Criminal na Era Compliance*, 2nd Ed. Almedina, Coimbra, 2021, p. 91 ff. For a different understanding (compliance as a function *of the company* and *for the company*), although much earlier than the function's recent evolution, *see* Labareda, João, *"Contributo para o estudo do sistema de controlo e da função de cumprimento ("Compliance")"*, in Direito dos Valores Mobiliários, 2016, p. 364.

[24] *See* Lösler, Thomas, *"Das moderne Verständnis von Compliance im Finanzmarktrecht"*, in NZG, 2005, p. 106, Weber-Rey, Daniela, *"Der Aufsichtsrat in der europäischen Perspektive – Vorschläge und Ideen für eine wirksame Corporate Governance"*, in NZG, 2013, p. 766 (which even refers that the evolution came at the cost of "corporate freedom"), Gebauer/Niermann, in *Hauschka/Moosmayer/Lösler...,* cit., § 48, annot. 19, and Maia, Pedro, *"Direito das Sociedades Bancárias"*, in Revista de Legislação e de Jurisprudência, Year 149, No. 4023, 2020, p. 398.

company directors. Starting in the 1990's, the existence of a compliance function within companies began being taken into account for the purposes of criminal, or even civil, liability. Some authors even identify 1991's *Sentencing Guidelines for Organizations* as the beginning of the current stage of compliance, in that they represent the first indicators of the relevance attributed to the existence of an "effective compliance program" within companies in reducing penalties[25].

Case law[26] soon followed by recognizing the existence of a duty to implement a reports and information system by the company's management body. And should the system signal a problem – a so-called "red flag" – the management body must act in a way that gathers the facts and takes the appropriate measures. It's important to underline that although public intervention left a mark of its influence (particularly when it comes to criminal prosecution), in this path of evolution the state neither *imposed* nor *determined* the existence of corporate programs of compliance. A program was not seen as a company's *legal duty*, despite an advantage – an indirect incentive – being offered by its implementation: the benefits which would come to the company and its directors should an event give rise to liability. These were therefore "explicit incentives" given by the state to the implementation of compliance programs seen as mitigating factors in the sentencing of corporations[27].

[25] *See* Griffith, Sean J., *"Corporate..."*, cit., p. 2084, Hess, David, *"Ethical Infrastructure and Evidence-Based Corporate Compliance and Ethics Programs: Policy Implications from the Empirical Evidence"*, in New York University Journal of Law and Business, Vol. 12, 2015, p. 318, and Langevoort, Donald C., *"Cultures of compliance"*, in American Criminal Law Review, Vol. 54, 2017, p. 940 ff., Garrett, Brandon L. and Mitchell, Gregory, *"Testing Compliance"*, in Law and Contemporary Problems, Vol. 83, No. 4, 2020, p. 49 ff. Amongst ourselves, *see* Rodrigues, Anabela Miranda, *Direito...* cit., p. 116 ff., and Sousa, Susana Aires de, *"A colaboração processual dos entes coletivos: legalidade, oportunidade ou "troca de favores"?"*, in Revista do Ministério Público, n.º 158, 2019, pp. 9ff. (with an important assessment of the evolution and of its implications for penal law and penal procedure). The reduction of sentencing due to the existence of an effective compliance program could be as far as 95% (*see* Gadinis, Stavros and Miazad, Amelia, *"The Hidden..."*, cit., p. 2146).

[26] In the 1996 case *In re Caremark Int'l Inc. Derivative Litig.*, tried in Delaware.

[27] *See* Armour, John, Garrett, Brandon L., Gordon, Jeffrey N. and Min, Geeyoung, *"Board..."*, cit., p. 1195, Gadinis, Stavros and Miazad, Amelia, *"The Hidden..."*, cit., p. 2148 ff.

This evolution was made complete by the United States Department of Justice's guidelines regarding the relevance of "effective" programs of compliance[28] in the potential prosecution of companies. And in the first years of the new millennium, in the midst of new frauds and scandals of accounting and auditing, the *Brooklyn Plan* was set in motion: in exchange for non-prosecution agreements, companies would pay penalties and fines and adopt rigorous programs of compliance[29]. It was in the context of these agreements of non-prosecution or of deferred prosecution[30] – the effects of which have been highly criticized[31] – that it became common to demand companies to implement programs of compliance typically centered on the approval of policies and processes directed at employees subject to training and monitoring[32].

[28] A matter which I will not delve into has been a special subject of debate: that of knowing which requisites are necessary to consider a compliance program "effective". This matter is very relevant because it's about knowing if the program's effectiveness is assessed by its *result* – by its efficiency – or solely by its *structure* and allocated *means*. Some authors point the risk (or even fact) that some compliance programs may become nothing more than "box-ticking" exercises – a simple demonstration that a compliance program exists – wherefrom the advantages expected from the organization's effective compliance and from a culture supportive of it did not result, or may not have resulted. This even justifies calling such programs "always elusive", or evasive (the origin of this expression is Martinez, Veronica Root, *"The Compliance..."*, cit., p. 205). On this matter, *see*, for example, Langevoort, Donald C., *"Monitoring: the behavioral economics of inducing agents' compliance with legal rules"*, in Georgetown University Law Center Business, Economics and Regulatory Policy, Law and Economics Research Paper, No. 276121, 2001, p. 933 ff., Armour, John, Gordon, Jeffrey and Min, Geeyoung, *"Taking Compliance Seriously"*, in Yale Journal on Regulation, Vol. 37, No. 1, 2020, p. 15 ff., Griffith, Sean J., *"Corporate..."*, cit., p. 2105 ff. (the metrics on evaluating the effectiveness take into account the *activity* instead of the *impact*, "showing that compliance should be busy but not necessarily effective"), Gadinis, Stavros and Miazad, Amelia, *"The Hidden..."*, cit., p. 2139, and Garrett, Brandon L. and Mitchell, Gregory, *"Testing..."*, cit., p. 56 ff.

[29] In this regard, *see* Garrett, Brandon L, *Too Big to Jail*, Harvard University Press, Cambridge, 2014, p. 54 ff. (which establishes a connection between the evolution of compliance and the criminal investigation of companies).

[30] *Deferred Prosecution Agreements* ('DPA') and *Non-Prosecution Agreements* ('NPA').

[31] *See* Langevoort, Donald C, *"Cultures..."*, cit., p. 970 ff.

[32] *See* Griffith, Sean J., *"Corporate..."*, cit., p. 2088 ff.

Although the rise of compliance as a sectorial regulatory reality had already occurred before[33], the determining factor in its *significant progress* was the 2007-2008 financial crisis: the relevant regulatory framework had been "bare-boned" until then[34]. After identifying the breach of credit institutions' internal policies – governance rules[35] – as the explicit cause of the crisis, supervisors (and legislators) moved decisively forward and *imposed* specific compliance duties to the financial sector. Which may define the new framework of compliance has a "reactive process", determined by the occurrence of scandals and crimes which propel legislators and legislators to intervene[36]. The legal and regulatory framework of this new outlook

[33] In April, 2005, the Basel Committee on Banking Supervision published it's report titled "Compliance and the compliance function" and, also in that year, the Bank of Portugal published Instruction 20/2005, which amended Instruction 72/96 by expressly pointing out the risk of compliance. Curiously, that risk was then inserted in "risk management", where it was defined as "the risk of an institution being subject to legal or regulatory sanctions or financial or reputational losses as a result of not having abided by the laws, norms, codes of conduct, or standards of "good practice" – as may be read in the Instruction's introduction. In this regard and on compliance's progressive reception by the Portuguese regulatory system, *see* Labareda, João, *"Contributo..."*, cit., p. 296 ff. and, more recently, Bastos, Nuno Moraes, *"Corporate Governance, Compliance e a Função Compliance nos Setores Bancários e Segurador"*, in A Emergência e o Futuro do Corporate Governance em Portugal, Vol. II, Almedina, Coimbra, 2018, p. 207 ff.

[34] The expression is from Chiu, Iris H-Y, *"Regulating…"*, cit., p. 6.

[35] This is a controversial matter where two theories collide: the "theory of irrelevance", which doesn't see failures in governance as the origin of the crisis, and the "theory of *force majeure*", according to which those failures are the crisis' major cause. The right position seems to be recognizing that although governance was *one* of the key factors of the crisis, it was not the *determining* factor, or even *the most important*. *See* Maia, Pedro, *"Direito..."*, cit., p. 379 (and the bibliography referred therein).

[36] In this regard, *see* Orozco, David, *"A Systems..."*, cit., p. 254 ff. But the quality of this approach's result is highly debatable and, on the plane of theoretical analysis itself, highly open to criticism, especially due to the fact that it ignores the influence the social and economic context has in the behavior of individuals, organizations, and institutions as a determining factor of compliance's result. *See* Orozco, David, *"A Systems..."*, cit., p. 257 ff. For an analysis of the issue of legislation passed as a reaction to crises and scandals (in the words of Arner, Douglas W., Barberis, Janos Nathan and Buckley, Ross P., *"The emergence of RegTech 2.0: From know your customer to know your data"*, cit., p. 8, "the history of global financial institutions is the story of regulatory initiatives in response to crisis"), *see* Banner, Stuart, *"What causes new*

of compliance – or better still, of this new nature of compliance and new connection to corporate governance – arrived as part of the "legislative tsunami" or "regulatory deluge" that the 2007-2008 financial crisis unleashed[37]. In European and Portuguese law, one should highlight Directive 2013/36/EU (known as 'CRD IV'[38]) and the accompanying Regulation (EU) No. 575/2013 (known as 'CRR'[39]). Though CRD IV practically doesn't address the issue, with the exception of an indirect reference to "compliance functions" in Article 92, Paragraph 2, Section f) of the directive's Portuguese version, the basis for the regulation of internal control and for an intervention by the EBA are set therein (*see* Article 74, Paragraph 1) – an intervention which at any rate had already taken place in 2011, with the publication of the *Guidelines on Internal Governance* ('GL 44'[40]), where the existence of an *autonomous* internal control function – the compliance function – which may only be combined with the risk management function in smaller or less complex institutions (*see* Paragraph 24.5[41]), is determined. The compliance function is regulated

securities regulation? 300 years of evidence", in Washington University Law Quarterly, 75, No. 2, 1997, p. 849 ff., Coffee, John C. Jr., *"Political Economy of Dodd-Frank: Why Financial Reform Tends to be Frustrated and Systemic Risk Perpetuated"*, in Cornell Law Review, Vol. 97, No. 5, 2011, p. 1020 ff. (who identifies the regulation of the financial system as a "sine curve" – a repetitive and soft oscillation).

[37] *See* Maia, Pedro, *"Direito..."*, cit., p. 372 (where an annotation containing a description of the most important normative instruments on which that tsunami was based can be found).

[38] Amended by Directive (EU) 2019/878 of the European Parliament and of the Council, of May 20th, 2019 (sometimes referred to as 'CRD V'), in the meanwhile.

[39] Amended by Regulation (EU) 2019/876 of the European Parliament and of the Council, of May 20th, 2019 (referred to as 'CRR II').

[40] It's important to clarify that the EBA's *Guidelines*, although apparently nothing more than recommendatory soft law, end up representing what some authors call "hoft law", in the sense that they appear to be soft law when issued but turn into hard law when national regulatory supervisors convert the recommendations therein into orders which regulated entities are subject to. In this regard, *see* Maia, Pedro, *"Direito..."*, cit., p. 400.

[41] The fact that compliance might sometimes not be autonomous at the organizational plane explains why the legislator and the European regulators do not refer to a "compliance department" but to a "compliance function": the latter is *mandatory*, without any exceptions, but it's assignment to an *autonomous department* is not. In this regard, *see* Gebauer/Niermann, *"Hauschka/Moosmayer/Lösler..."*, cit., p. 22, § 48, annot. 6.

thereafter (*see* Paragraph 28 and following). A new version of the *Guidelines* was published in 2018[42].

In a way, this evolution represents a veritable *transmutation* of compliance, which, no longer confined to the company's circle of *autonomy of* (risk) *management*, becomes (at least to some extent) part of the domain of legislative or regulatory intervention. While appealing to variable terms and distinct measures, legislators and regulators imposed on financial sector companies the duty of setting up an (internal) compliance function. As mentioned before, the development of compliance had already received *external boosts*, but now its existence became *externally determined*. Though developed and secured *internally* – one must not forget that compliance is an *internal* control function –, it presently has an *exogenous* origin when it comes to banking companies, in the sense that it took from the management body the freedom not only to decide on its existence, but also on multiple aspects of its structure and operation[43]. It's the legislator and the regulator who determine them. This governance is therefore *internal* to the company but imposed on it by *external* sources[44].

While needfully brief and even incomplete, the framework presented above allows the understanding of the new context which compliance is a part of within baking sector companies. A function of *internal* control which, while taking place *within the company*, serves purposes that are not exclusively inherent to the company itself when understood as an instrument at the service of shareholder interests[45].

[42] *Guidelines on Internal Governance* (EBA/GL/2017/11, of March 21st, 2018, available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2164689/151a6ca3-31ae-40b0-9f55-9d6c65b86b00/Guidelines%20on%20Internal%20Governance%20%28EBA-GL-2017-11%29_PT.pdf?retry=1). In this regard, amongst ourselves, *see* Fonseca, Patrícia Afonso, *"As Novas Orientações da EBA em Matéria de Governo Interno"*, in A Emergência e o Futuro do Corporate Governance em Portugal, Vol. II, Almedina, Coimbra, 2018, p. 235 ff.

[43] Highlighting the *exogenous* origin of compliance, which contrasts with the function's *internal* nature, *see* Griffith, Sean J., *"Corporate..."*, cit., p. 2078 ff.

[44] *See* Griffith, Sean J., *"Corporate..."*, cit., p. 2079 ff.

[45] What I stated above does not contend with the heated discussion which has been taking place amongst authors (and even amongst the public) on the issue of companies' purpose – do they follow their shareholders' selfish interests or others beyond that? If so, which ones and on which terms? –, a discussion stimulated by the "corporate purpose" current of thought. Should one follow this tendency there will be some facets of compliance found to overstep a company's corporate purpose. On

II. TECHNOLOGY IN BANKING

Banking has always been particularly open to technical innovation and progress[46]. In some cases, instead of merely *accepting* this innovation and progress, it went so far as *promoting* it (as *creating* it, in a sense). One need only think of the *telegraph*, introduced in 1838 and promptly incorporated in the daily activity of banks. And of the first *transatlantic cable*, laid in 1866 and soon after already facilitating intense financial exchanges between Europe and the United States of America – and driving the first globalization of financial activity at the end of the nineteenth century, through the rapid transmission of information, transactions and payments. In 1958, *Bank of America* and *American Express* introduced the *credit card*, a technology-based revolution in lending and payment systems.

In 1964, *Xerox* introduced the first commercial fax machine (under the name *Long Distance Xerography*, or 'LDX'), which would become widely used in the financial sector; in 1966, a global telex network that ensured the quickness and safeness of communications in financial transactions was already in place.

In 1967, *Barclays Bank* introduced a ground-breaking system of automatic cash withdrawal and money transfer – the *Automatic Teller Machine*, or 'ATM' –, one of the most consequent technology-based revolutions in banking until the present day. *Calculators*, invented by *Texas Instruments* also in 1967, were immediately adopted by the sector.

This stage, which came to an end in the 1960's and may be called *FinTech 1.0*, rested on *analogical* technology. What followed was a

the matter of "corporate purpose" and the intense debate surrounding it, *see*, with particular relevance and disagreeing positions, Mayer, Colin, *"The future of the corporation: Towards humane business"*, in Journal of the British Academy, Vol. 6, No. 1, 2018, p. 1 ff., Bebchuk, Lucian A. and Tallarita, Roberto, *"The Illusory Promise of Stakeholder Governance"*, in Paper SSRN, 2020, p. 1 ff., Rock, Edward B., *"For Whom is the Corporation Managed in 2020?: The Debate over Corporate Purpose"*, in European Corporate Governance Institute – Law Working Paper, No. 515, 2020, p. 1 ff., and Lipshaw, Jeffrey M., *"The False Dichotomy of Corporate Governance Platitudes"*, in The Journal of Corporation Law, Vol. 46, No. 2, 2021, p. 346 ff.

[46] This is stated by the European Commission in its *FinTech Action Plan: For a more competitive and innovative European financial sector*, 2018, p. 2.

shift to *digital* technology until the late 1980's, intensified by the crash of the New York Stock Exchange in 1987 – a stage which some authors identify as *FinTech 2.0*. With the development of the *World Wide Web* in the 1990's, the first online banking service was launched by the North American bank *Wells Fargo*. The first online banks without traditional brick-and-mortar branches, such as *ING Direct* or *HSBC Direct*, appeared in 2005[47].

This very brief historical overview of the development of technology in banking helps to understand that the technological evolution brought about by Robotics and AI isn't in and of itself an *irregular*, *strange* or even *novel* situation in the industry: financial activity has always promoted and surrounded itself with the most developed tools and instruments that technology has to offer at each point in time[48].

Although the incorporation of new technical or technological means in the financial business isn't a novelty, the current situation is new mostly because of *two aspects*[49]. *The first of these concerns is the fact that new technologies, which are undoubtedly being assimilated by companies within the sector, are mostly used by non-financial companies* – or companies not financial in nature. These aren't financial companies taking advantage of a *new technology* to conduct their *old trade*; in most cases, they're companies technological in nature taking advantage of technology (already existent to them) to conduct a *new trade*. *FinTech*

[47] An historical overview of the financial sector's technological evolution can be read, for example, in Arner, Douglas W., Buckley, Ross P. and Barberis, Janos N., *"The Evolution of Fintech: A New Post-Crisis Paradigm?"*, in Georgetown Journal of International Affairs, Vol. 47, 2016, p. 1274 ff., and in Jung, John Ho Hee, *"RegTech..."*, cit., p. 257 ff.

[48] It need only be said that *Goldman Sachs* employs 33 thousand engineers, more than those employed by *Twitter*, *Facebook*, or *LinkedIn*, something that is quite revealing of the technological level already reached by the banking sector. *See* Arner, Douglas W., Buckley, Ross P. and Barberis, Janos N., *"The Evolution..."*, cit., p. 1291. Or that *JP Morgan Chase* is estimated to have more software developers than *Google* or *Microsoft* (*see* Lin, Tom C. W., *"Compliance, Technology, and Modern Finance"*, in Brook. J. Corp. Fin. & Com. L., Vol. 11, 2016, p. 161).

[49] The fact that the financial sector has always adopted technical innovations so quickly does not mean that it's quick to receive "technological disruptions", as is the case. In the sense that the financial sector has always resisted and suspected disruptive innovations, *see* Anagnostopoulos, Ioannis, *"Fintech and regtech: Impact on regulators and banks"*, in Journal of Economics and Business, Vol. 100, 2018, p. 11.

and *TechFin* companies, to those who know the difference, are precisely that[50].

As it's been frequently highlighted, technological evolution is *opening up* the financial sector – *opening up* also in the sense of *freeing* the activity, at least temporarily, because the traditional legal framework isn't capable of regulating and supervising these new forms of financial activity. These so-called *FinTech* companies – *Fin* (Financial) + *Tech* (Technology), which consists of using technology to provide all manner of financial services[51] – under many ways escape the existing legal and regulatory framework. And what's more, despite technology being what *operatively* supports them, it's the *legal framework* which at least partially stimulates them *economically*. As a matter of fact, the activity's boom after the financial crisis is no *mere coincidence*: the great crisis fostered a significant reinforcement of the regulatory framework and consequently occasioned an equally significant rise in the associated costs incurred in by companies having to comply with it, so that conducting the activity "absent of regulation" became a major competitive advantage[52].

This represents a very relevant profile for the analysis and debate of technological evolution: in which way it should be made a part of the regulatory framework, should that framework be shared or separated, how should the regulatory entities themselves evolve, and how can they be made capable of handling these new phenomena[53]. This

[50] On the matter of *FinTechs*, among an extensive bibliography but discussing some conceptual aspects only, *see* Bradley, Christopher G., *"Fintech's Double Edges"*, in Chicago-Kent Law Review, Vol. 93, No. 1, 2018, p. 77 ff., Brummer, Chris and Yadav, Yesha, *"Fintech and the Innovation Trilemma"*, in The Georgetown Law Journal, Vol. 107, 2019, p. 241, annot. 18, and Baumanns, Charlotte, *"Fintech als Anlageberater? Die aufsichtsrechtliche Einordnung von Robo-Advisory"*, in BKR, 2016, p. 366 ff.

[51] *See*, for example, Arner, Douglas W., Buckley, Ross P. and Barberis, Janos N., *"The Evolution..."*, cit., p. 1272.

[52] *See* Arner, Douglas W., Buckley, Ross P. and Barberis, Janos N., *"The Evolution..."*, cit., p. 1286. The history of the financial system's regulation and of its tendencies and interactions must inform the decisions that require in response to new tendencies. For a history from this perspective, *see* Marco, Lamandini and Munoz David, Ramos, *"A brief history of the evolution of financial institutions and of their regulation"*, in EU Financial Law. An Introduction, Cedam, Padova, 2016, p. 3 ff.

[53] On this matter, *see*, for example and among many others, Fein, Melanie L., *"How Should Robo-Advisors Be Regulated? Unanswered Regulatory Questions"*, in Allianz Global Investors, 2017, p. 1 ff.

naturally comes in addition to the assessment of the economic and social impacts which the adoption of these new technologies entails at various levels: the reduction of financial companies' operating costs, the democratization of services (allowing them to reach sections of the population where resources are not as available, although with that favoring a better allocation of significantly valued economic resources), the improvement of investment decisions (based on more rationally processed and technically capable information), the increase of market efficiency, etc.[54] To some, the length and depth of what is called the financial industry's "technological revolution" commands the phenomenon's analysis in a way that's not merely micro-transactional but also systemic, due to the fact that its impacts have even been felt at the level of politics and power relations[55]; to this, the realization that "software eats the world", i.e. that it subjugates all other industries – the financial services industry is but one example – and forces their total reconversion[56], must be added. In the 1940's, Schumpeter theorized about the gale of "creative destruction" in the economy[57]: regardless of the theory's correctness, the concept may surely be used to illustrate the implications associated with the use of software (including robotics and AI) in the financial industry.

This is not, however, the object of this study.

The other feature where the situation is new concerns the *speed* with which the evolution is happening[58]. And one must not think that this is purely related to time and in no way relevant beyond that;

[54] On these implications, *see*, for example, Lin, Tom C. W., *"Artificial Intelligence, Finance, and the Law"*, in Fordham Law Review, Vol. 88, 2019, p. 531 ff. (especially highlighting the assessment and analysis of the risks and dangers inherent to the use of robotics and AI by financial services).

[55] *See* Omarova, Saule T., *"New Tech v. New Deal: Fintech as a Systemic Phenomenon"*, in Yale Journal on Regulation, Vol. 36, 2019, p. 735 ff.

[56] The expression belongs to Marc Andreessen, "Why software is eating the world", in *Wall Street Journal* (20.08.2011).

[57] *See* Schumpeter, Joseph, *Capitalismo, Socialismo e Democracia*, Actual Editora, Coimbra, 2018, p. 119 ff. Although the expression most recently used is "disruption" or "disruptive effect" (for example, Piri, Michael M., *"The Changing Landscapes of FinTech and RegTech: Why the United States Should Create a Federal Regulatory Sandbox"*, in Business & Finance Law Review, Vol. 2, No. 2, 2019, p. 236), the general meaning remains the same.

[58] *See* Arner, Douglas W., Buckley, Ross P. and Barberis, Janos N., *"The Evolution..."*, cit., p. 1276.

evolution at a very rapid pace itself represents an *increased risk* for incumbent companies, challenged (competitively *attacked*, strictly speaking) by new players which themselves pose several other risks: of companies failing in the face of competition – thus compromising the stability of the financial sector; of rigid and inadequate legal output, incapable of handling new phenomena; or of legal output which, faced with the need to respond quickly to new situations, may be rushed and inconsistent and thus give way to undesirable consequences[59].

III. ARTIFICIAL INTELLIGENCE AND *REGTECH*

There is no consensual and widely accepted definition of AI[60]. For the purposes of this study, the definition used in the European Commission's proposal for an Artificial Intelligence Act[61] (Article 3, Paragraph 1), issued on April, 2021, will be adopted: "[an] 'artificial intelligence system' (AI system) [is a] software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". In turn, the proposal's Annex I identifies the following AI techniques and approaches: "(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference

[59] An interesting analysis resting on the understanding that the evolution brought about by *FinTechs* differs from the ones preceding may be read in Brummer, Chris and Yadav, Yesha, *"Fintech..."*, cit., p. 242 ff.

[60] *See* Scopino, Gregory, *"Key..."*, cit., p. 19, and Yang, Yueh-Ping (Alex) and Tsang, Chengyun, *"RegTech and the New Era of Financial Regulators: Envisaging More Public-Private-Partnership Models of Financial Regulators"*, in University of Pennsylvania Journal of Business Law, 2018, p. 363 ff., where two different definitions, corresponding to two different visions, are confronted: one which connects *RegTech* to the technologies which facilitate *communication* between regulators and regulated entities; another which connects it to the *development of the regulatory system*.

[61] Available at https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206.

and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods"[62].

AI itself isn't something new – it was first referred to in 1956 and effectively developed in the 1970's; but the pace at which it has evolved recently is unprecedented. A confluence of factors helped this radical acceleration: the extraordinary growth of *data* accessible by computer[63] – to which the massive use of internet was decisive, leading some to say that "digitalization is everything"[64]; its *storage* – through the development of clouds which enable the storage of colossal amounts

[62] The definition used in the proposal is based on studies promoted by the European Commission with regard to this matter. *See* the *High Level Expert Group on Artificial Intelligence* ("A definition of AI: Main capabilities and scientific disciplines") (available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341), of 2019, where the following definition was proposed (p. 6): "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)." At an institutional level, *see* the 2018 *OECD Council Recommendation on Artificial Intelligence* (available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449), adopted by the G20 in 2019 (available at https://www.mofa.go.jp/files/000486596.pdf).

[63] The European Commission estimates that 175 zettabytes of data (over five times more than the 33 zettabytes of data produced in 2018) will be produced in 2025. *See "Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança"*, in European Commission, 2020, p. 4. A zettabyte corresponds to 1 trillion (1.000.000.000.000) gigabytes.

[64] *See* Buckley, Ross P., Zetzsche, Dirk A., Arner, Douglas W. and Tang, Brian W., *"Regulating Artificial Intelligence in Finance: Putting the Human in the Loop"*, in Sydney Law Review, Vol. 43, No. 1, 2021, p. 46, quoting Schwab, in respect of a "Fourth Industrial Revolution". There is even talk of the emergence of a "data economy", an activity of great value consisting in the collection and monetization of data. In this regard, *see* Magnuson, William, *"A Unified Theory of Data"*, in Harvard Journal on Legislation, Vol. 58, 2021, p. 24 ff.

of information at a very low cost[65]; *communication* – data exists in and flows through computers, smartphones, social networks, search engines, etc., widely used all around the world; and *computing power* – according to Moore's law, the number of transistors in a microchip doubles every two years[66], to the point where *quantum computing* is already under way.

The arrival of AI not only allowed persons to be replaced when performing certain tasks, but also made available services that persons would never be able to provide, no matter how many of them or how well prepared they might have been. Therefore, it's not about replacing persons by performing tasks *exactly how they would perform them* – although surely quicker, with less variations in quality and with less mistakes –, but about providing a service which *exceeds human capacity*. AI not only surpasses a human person in *how* – first and foremost with regard to speed –, but in *what*, the end result of the activity. In its current stage of development, AI already offers a wide array of uses[67].

In 2015, the term *RegTech* first appeared, used by Philippe Treleaven[68] and defined by the *Financial Stability Board* ('FBS') as a subset of *FinTech* corresponding to technologies which may facilitate compliance with regulatory demands in a more efficient and effective way than allowed by existing capacities[69]. Still, *RegTech* is not always a part of *FinTech* – that is, it isn't necessarily a part of the latter and therefore is not one of its subsets – because, unlike *RegTech*, it entails a disruptive use of technology. *RegTech* helps companies (whether they are *FinTech* companies or not) comply with regulatory demands through the use

[65] According to "Kryder's Law", the quality and capacity of data storage has drastically increased while at the same time costs have decreased, meaning there has been a constant growth in the volume of data collected and stored. *See* Buckley, Ross P., Zetzsche, Dirk A., Arner, Douglas W. and Tang, Brian W., *"Regulating..."*, cit., p. 46.

[66] A comprehensive account of the reasons which propelled AI's evolution can be read in Buckley, Ross P., Zetzsche, Dirk A., Arner, Douglas W. and Tang, Brian W., *"Regulating..."*, cit., p. 46.

[67] *See* the very significant data gathered by the *Bank of England* and the FCA in *Machine learning in UK financial services*, 2019, p. 8 ff.

[68] *See* Treleaven, Philip, *"Financial regulation of FinTech"*, in Journal of Financial Perspectives, 3, 2015, p. 114 ff.

[69] *See* Authority, Financial Conduct, *"Call for Input: Supporting the development and adoption of RegTech"*, available at https://www.fca.org.uk/publication/call-for-input/regtech-call-for-input.pdf, 2015.

of technology. In this sense, *RegTech* and *FinTech* differ in their origin, goals and scope[70].

But the use of Technology as an instrument of compliance came much earlier than the emergence of *RegTech*. The increasing regulatory demands and above all the prevailing regulatory model had already occasioned a growing use of technology, endorsed by the regulators themselves.

To understand the relevance that the regulatory model may have in the use of technology it must be kept present that regulation may target one of three levels of activity of the regulated entity: *planning*, *performance* (action), or *result* (whether positive or negative)[71]. When it targets the *result* (which corresponds to the *"performance-based"* model) the regulator will set rules imposing a certain result. Contrarily, if instead it targets the *performance* (action) the regulator will set rules imposing the use of specific technologies or behaviors to be followed by the regulated entity when performing its activity (*"technology-based"* models).

In turn, the so-called "process-based" or "management-based" model (the latter expression belonging to Cary Coglianese and David Lazer)[72] is characterized by imposing on regulated entities the *flexible* fulfillment of *public interest objectives*, while granting them the freedom (but also the responsibility) to create plans which, in light of the specific information available to them about their own organization, allow them to reach the targets set by the regulator[73]. Thus, risk, which is contextual and expresses itself differently in heterogeneous companies, may be more adequately mitigated by decisions made by each regulated

[70] *See* Arner, Douglas W., Barberis, Janos and Buckey, Ross P., *"FinTech..."*, cit., p. 371.

[71] In this regard, *see* Coglianese, Cary and Lazer, David, *"Management-based regulation: Prescribing private management to achieve public goals"*, in Law & Society Review, 37, 4, 2003, p. 693 ff.

[72] *See* Coglianese, Cary and Lazer, David, *"Management-based regulation: Prescribing private management to achieve public goals"*, cit., p. 692 ff. (highlighting that other authors have used distinct expressions to refer to understandings close to each other in meaning, such as "enforced self-regulation", "mandated self-regulation", "reflexive regulation", or "process-based regulation"). The expression "management-based" has a wider scope since it includes a group of processes, systems, and internal management policies that the regulator demands from regulated entities.

[73] *See* Coglianese, Cary and Lazer, David, *"Management-based regulation: Prescribing private management to achieve public goals"*, cit., p. 694 ff.

entity with the aid of the specific information available to them about themselves – instead of by imperative rules uniformly and generally dictated by the regulator[74]: the regulator doesn't determine in which way the regulated entity should comply but instead demands that it set up its own compliance systems and prove that these are adequate to the fulfillment of the objectives[75]. It may be added that, regardless of its theoretic merits, this approach is a *practical inevitability* – regulatory compliance rests on the regulated entity's systems and can't be guaranteed by the regulator –, so that in the end it's about consciously recognizing this reality as an element of the regulator's strategy[76].

A so-called "meta-regulation"[77] or "regulation of self-regulation"[78] was thus born: the regulator creates a general, not too prescriptive outline of a structure and sets certain objectives which must be reached. In turn, the regulated entity keeps its discretion when choosing how to implement the systems and processes necessary to reach the relevant objectives. The regulator intervenes only at a "meta-level", which consists of evaluating plans and subsequently verifying that the regulated entity has followed the plans that it has created itself.

In the field of finance, "meta-regulation" has spread in such a relevant way that it became a *model*: for example, the evolution of the Basel I capital requirements to the Basel II, where instead of a prescriptive approach, simple and common to all banking institutions, a model of

[74] *See* Bamberger, Kenneth A, *"Technologies of compliance: Risk and regulation in a digital Age"*, in Tex. L. Rev., 88, 2009, p. 672 ff.

[75] *See* Black, Julia, *"Paradoxes and Failures: New Governance Techniques and the Financial Crisis*" in The Modern Law Review, Vol. 75, No. 6, 2012, p. 1045 ff.

[76] *See* Black, Julia, *"Paradoxes… ", cit.*, p. 1046.

[77] On meta-regulation, *see* Coglianese, Cary and Mendelson, Evan, *"Meta-regulation and self-regulation"*, in The Oxford Handbook of Regulation, Oxford, Oxford University Press, 2010 (comparing traditional "command and control-based" regulation to "meta-regulation" and "self-regulation", whose non-consensual definitions are then presented), and Scott, Colin, *"Regulating everything: From mega- to meta-regulation"*, in Administration, Vol. 60, 2012, p. 57 ff.

[78] The expression belongs to Parker, Christine, *The Open Corporation: Effective self-regulation and Democracy*, Cambridge University Press, Cambridge, 2002, p. 245 ff., in which the author defends the so-called "open corporation", a company that "democratically self-regulates" in a fusion of management, democracy, and law. *See* also Parker, Christine, *"Meta-Regulation: Legal Accountability for Corporate Social Responsibility?"*, in The New Corporate Accountability: Corporate Social Responsibility and the Law, Cambridge University Press, Cambridge, 2007, p. 3.

adjustment was adopted on the basis of a process of interaction with the institution itself[79]. On a national level, one finds that the example of the legal framework built around the prevention of money laundering (*i.e.* Law 83/2017) unquestionably follows this model: each entity must effectively create and apply the policies, procedures and control mechanisms adequate to the capable management of risks related to money laundering which the company is or may find itself to be exposed to [Article 12, Paragraph 1, Section a)]. And it's the entity's own duty to identify, evaluate and mitigate such risks, for the purpose of which it must take into account its own specific characteristics (such as the size and complexity of its activity, its clients and their own activity, the countries or territories of origin, etc.) (*see* Article 14 of Law 83/2017). In its wake, several normative instruments issued by the Bank of Portugal, such as Notice 2/2018 – observe the vast array of rules therein appealing the entity to carry out an adequacy finding with regard to procedures, processes, means, etc. [*e.g.* Article 1, Paragraph 1, Sections c) and j); Article 7, Paragraph 1; Article 10, Paragraph 1; Article 15, Paragraph 2, Section c); and Article 19, Paragraph 2] – and Instruction 2/2021 [*e.g.* Article 5, Paragraph 3, Section c) and Article 17, Paragraph 1] rest on the same model by calling on the entity to set up the processes, procedures, and means adequate to reach the objectives laid down by the regulator.

In effect, insofar as it dictates that the regulated entity must lay down plans which adequately deal with its risk environment, this ("management-based") regulatory model has meant the increasing adoption of technology with the view of handling and creating the information necessary to model the risk in each organization and keep the processing of said information permanently updated.

Yet, *RegTech*'s large development within the span of the last decade is the result of specific reasons. First and foremost, it's a result of the *2007-2008 financial crisis*, which brought about a lot of regulatory demands that could be fulfilled (only) through the use of technology[80]. It's also a result of *financial regulation's own complexity*, which has

[79] *See* Chiu, Iris H-Y, *"Regulating…"*, cit., p. 22 ff. (with several examples).

[80] Highlighting this reason in particular as the reason for *RegTech*'s development, *see* Arner, Douglas W., Barberis, Janos and Buckey, Ross P., *"FinTech…"*, cit., p. 395, and Arner, Douglas W., Barberis, Janos Nathan and Buckley, Ross P.,

meant increased demands on compliance[81]. Secondly, the great developments in the field of *data science*, namely the possibility of transferring computing to "cloud" infrastructures, also boosted *RegTech*. Thirdly, the pressure to *reduce costs* has equally meant opting for *RegTech* due to the savings it enables[82] – one ought to keep in mind that the estimated cost of AML compliance programs in the European Union already totaled 83 billion dollars in 2017[83]. All of this is taking place at a stage when banks are providing an increasingly digital experience, from which AI may emerge[84].

"The emergence of RegTech 2.0: From know your customer to know your data", cit., p. 9 ff.

[81] In this regard, *see* Lin, Tom C. W., *"Compliance..."*, cit., p. 166 ff., and Arner, Douglas W., Zetzsche, Dirk A., Buckley, Ross P. and Weber, Rolf H., *"The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II"*, in Stanford Journal of Law, Business & Finance, Vol. 25, No. 2, 2020, p. 247.

[82] Kurum, Esman, *"RegTech solutions and AML compliance: what future for financial crime?"*, in Journal of Financial Crime, ahead-of-print, 2020, p. 3, identifies two reasons for the massive adoption of *RegTech*: not only cost reduction but also the long-term value it creates for institutions.

[83] *See* Kurum, Esman, *"RegTech solutions and AML compliance: what future for financial crime?"*, cit., p. 2. Other authors also state that, in the United States of America, the costs of fines imposed on financial institutions after the 2007-2008 financial crisis were over 200 billion dollars (*see* Arner, Douglas W., Barberis, Janos Nathan and Buckley, Ross P., *"The emergence of RegTech 2.0: From know your customer to know your data"*, cit., p. 2.); other sources say the cost went as high as 321 billion dollars in the years between 2008 and 2016 (43 billion dollars in 2016 alone) (*see* Fruth, Joshua, *Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states*, March, 2018, p. 3; *see also* Jung, John Ho Hee, *"RegTech..."*, cit., p. 258 ff., containing information with regard to the United Kingdom). In 2018, *Deloitte* estimated that the cost of compliance was 25 billion dollars in the United States of America alone (*see "The case for artificial intelligence in combating money laundering and terrorist financing. A deep dive into the application of machine learning technology"*, in Deloitte, 2018, p. 4) and *JP Morgan* spends about 600 million dollars a year on technology used for compliance (*see* Lin, Tom C. W., *"Compliance..."*, cit., p. 166). Today, the costs of "governance, risk, and compliance" ('GRC') represent 15% to 20% of the total costs of major financial institutions (*see* Jung, John Ho Hee, *"RegTech..."*, cit., p. 258). For a general sense of the costs associated with regulation, *see* Arner, Douglas W., Barberis, Janos and Buckey, Ross P., *"FinTech..."*, cit., p. 388 ff. And, most recently, the EBA's *Study of the Cost of Compliance with supervisory reporting requirements*, 2021 (Report EBA/Rep/2021/15).

[84] Noting this, *see* Armstrong, Patrick, *"Developments in RegTech and SupTech"*, in European Securities and Markets Authority, 2018, p. 2.

According to the data available, *RegTech* is in marked expansion. In the United Kingdom, for example, about 10 companies were started in that field in the year 2000; between 2010 and 2020, a minimum of 15 such companies were started in each year, with some years (such as 2016) seeing the start of almost 30 new companies. A steep decline in new companies has been seen recently, which may be attributed to the fact that the already existing ones are gaining a relevant size. The market is composed of an increasingly larger percentage of mature companies (more than 5 or even 10 years old)[85]. *FinLab*, the platform created by the Portuguese financial supervisors (the Bank of Portugal, the Securities Exchange Market Commission, and the Supervising Authority for Insurance and Pension Funds) identified 16% of projects in the field of *RegTech* in its report of the second edition of *Portugal FinLab*, in 2020 (in its first edition, in 2019, it had identified 13% of projects)[86].

The areas served by *RegTech* are mostly concentrated around matters of compliance: 32% of products regard financial crimes (AML) – for instance, HSBC recently announced an agreement with "Silent Eight" for the development of AI mechanisms; *Standard Chartered* announced a similar agreement with "Quantexa"[87]; 16.5% regard data protection and privacy; and 9% regard management and regulatory compliance[88]. According to other sources, over half of all *RegTech* companies in 2017 focused on AML compliance. In the *RegTech 3.0* era, it's expected that the focus will be on the increasing importance of data for AML compliance ('know your data')[89].

[85] All these elements may be found in *"2021: A Critical..."*, cit., p. 17.

[86] *See Portugal Finlab Report*, 2nd Edition, 2020, p. 8 (available at https://8080dd92-d6fc-49d9-a97eb24c8f013bb2.filesusr.com/ugd/ca9a53_217c4187d5b-d4a5a9b377c6f6500e0ff.pdf).

[87] *See "2021: A Critical..."*, cit., p. 16

[88] *See "2021: A Critical..."*, cit., p. 13 ff., and *"There's a revolution coming. Embracing the challenge of RegTech 3.0"*, in KPMG, 2018, p. 1 ff.

[89] In this regard, *see* Kurum, Esman, *"RegTech solutions and AML compliance: what future for financial crime?"*, cit., p. 2. A description of the areas where *RegTech* most intervenes and of the technologies it most uses [such as AI, machine learning, robotic process automation ('RAP'), natural language processing ('NPL'), big data, cloud computing, etc.] may be read in Jung, John Ho Hee, *"RegTech..."*, cit., p. 265 ff., and also in the important report *"Machine learning in UK financial services"*, in Bank of England, 2019.

IV. TECHNOLOGY (*INTER ALIA*, AI) IN BANKING COMPLIANCE

Unsurprisingly, the financial sector, which has always been an avid user of technical and technological innovations[90], is at the forefront of developing uses for them. And the advantages that the sector may reap by using AI are clear[91]. The fact that AI is particularly suitable to be used by the financial sector explains the significant attention recently paid by national and international entities, by regulators, etc., to this matter in specific[92].

Compliance is commonly named as one of the areas of banking activity *most suitable to the use of AI* – what's more, compliance has always had a close bond with technology due to it being a "back office"

[90] In this regard, *see* Maia, Pedro, *"A robotização do mundo financeiro: reflexões introdutórias"*, in Estudos de Direito do Consumidor, No. 16, Centro de Direito do Consumo - Instituto Jurídico, Coimbra, 2020, p. 273 ff.

[91] *See, for example, "EBF position paper on AI in the banking industry"*, in European Banking Federation, 2019, EBA, *Report on big data and advanced analytics*, 2020, p. 43 ff., EBA, *EBA Analysis of Regtech in the EU Financial Sector*, 2021.

[92] As an example, *see* the EBA *Report on automation in financial advice*, 2016, (available at https://esasjointcommittee.europa.eu/Publications/Reports/EBA%20BS%202016%20422%20(JC%20SC%20CPFI%20Final%20Report%20on%20automated%20advice%20tools).pdf), the EBA *Report on big data and advanced analytics*, 2020 (available at https://www.eba.europa.eu/sites/default/documents/files/document_library//Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf), the ESMA – *Joint Committee Final Report on Big Data*, 2018 (available at https://www.esma.europa.eu/sites/default/files/library/jc-2018-04_joint_committee_final_report_on_big_data.pdf), the *EBF position paper on AI in the banking industry*, 2019, (available at https://www.ebf.eu/wp-content/uploads/2020/03/EBF_037419-Artificial-Intelligence-in-the-banking-sector-EBF.pdf), the *Machine learning in UK services*, 2019, issued by the *Bank of England* and the FCA (available at https://www.bankofengland.co.uk/report/2019/machinelearning-in-uk-financial-services), Calzolari, G., *Artificial Intelligence market and capital flows, Study for the Special Committee on Artificial Intelligence in a Digital Age*, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2021 (available at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU(2021)662912_EN.pdf). For an approach that's not purely sectorial, *see Livro Branco da Comissão Europeia sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança*, 2020 (available at https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11eaaece-01aa75ed71a1), the recent proposal of the European Commission for an *Artificial Intelligence Act* (available at https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF).

function[93]; this is first and foremost true of AML compliance, but also of regulatory compliance[94]. Entities are gradually subject to more KYC ('know your customer') duties, whose efficiency can be greatly increased if the information on which they rest – to know a client is to know *information* about the client – can be cross-checked and cross--referenced between different sources (beginning with the information provided by the client themselves) on a large scale in a short period of time, or even almost instantaneously. Moreover, the paradigm has shifted as AML compliance's methodology ceased to rest on the *client* and turned to *data* – "data is king"[95]. Since credit institutions possess an (exponentially) increasing volume of data which they have the burden of adequately using – starting with assessing its quality and authenticity[96] –, technological solutions have become crucial and of growing usefulness. In this regard, application programming interfaces are able

[93] *See* Fanto, James A., *"The Professionalization of Compliance: Its Progress, Impediments, and Outcomes"*, in Notre Dame Journal of Law, Ethics & Public Policy, Vol. 35, No. 1, 2021, p. 223.

[94] *See*, for example, Magnuson, William, *"Artificial Financial Intelligence"*, in Harvard Business Law Review, Vol. 10, 2020, p. 350, Kaya, Orçun, *"Artificial intelligence in banking: A lever for profitability with limited implementation to date"*, in Deutsche Bank Research, 2019, p. 5, and *see*, most recently, the empirical data in *"2021: A Critical..."*, cit., p. 13 ff., as well as EBA, *EBA Analysis...* cit., p. 42 ff.

[95] *See* Arner, Douglas W., Barberis, Janos Nathan and Buckley, Ross P., *"The emergence of RegTech 2.0: From know your customer to know your data"*, cit., p. 16 ff., and Kurum, Esman, *"RegTech solutions and AML compliance: what future for financial crime?"*, cit., p. 3. Besides, from a very interesting perspective, computers have something in common with cells and with the human brain: in different ways, all are processors of *information* (*see* the inspiring work of Oliveira, Arlindo, *The Digital Mind: How Science is Redefining Humanity*, MIT Press, Cambridge, 2017, p. 1).

[96] It's important to keep in mind that, under the terms of the Bank of Portugal's Notice 2/2018, institutions have the *duty* of resorting to various sources of information (Article 6), first and foremost internal ["Analysis and internal documents of financial entities, including information collected during the procedures of identification and diligence and the lists and databases internally produced and updated – Paragraph 2, Section g)], but also external, where "Independent and credible information from civil society or international organizations [Paragraph 2, Section h)] is included, and "Information gathered from the internet and mass media, as long as belonging to a credible and independent source" [Paragraph 2, Section i)], the information contained in databases, lists, risk reports, and other analysis originating in commercial sources available in the market [Paragraph 2, Section j)], official statistical data from national or international sources [Paragraph 2, Section k)].

to produce great results not only at onboarding [Article 23, Paragraph 1, Section a) of Law 83/2017] but also with regard to the permanent *update* of the information which bounds entities (*see* Article 40 of Law 83/2017).

Likewise, credit institutions have in *RegTech* a valuable ally in defining and updating each client's *risk profile* [Article 18, Paragraph 2, Section c) of Law 83/2017] based on the information collected.

Still in connection with the prevention of money laundering, pursuant to Article 39 of Law 83/2017 credit institutions hold duties in respect of "politically exposed persons"[97]: they're charged with identifying a politically exposed person [Article 39, Paragraph 1, Section a) of Law 83/2017] and thereafter subject that person's operations to the very strict applicable law and jurisdiction. Further duties regard "entities to which sanctions have been applied", whose funds and economic resources have been subject to restrictive measures by the United Nations or European Union (*see* Article 13 and following of Law 97/2017). The challenges posed to banks are truly massive[98] due to the necessity to screen the names of the transacting parties and to cross-check those with the ones included on the lists: contrary to the names used on the lists (of politically exposed persons or of persons to whom sanctions have been applied), in transactions names may appear as abbreviations, initials, with or without full last names (or even in reverse order) – one must not forget these are worldwide lists, made up of persons of all nationalities and languages –, together with the use of homonyms (the more incomplete the name used in the transaction is, the greater the use will be) , which all in all makes AI's ability to make the screening more flexible all the more useful. A "rule-based" system is either too strict – and will no longer detect the entity should even the slightest difference exist in its identification – or too comprehensive, in which case it will generate an inordinate amount of false positives.

Given the constant change of the universe of persons qualifiable as politically exposed and to whom sanctions have been applied, and the fact that their number is vast to begin with, it's easy to understand

[97] Defined by a (decisive) list, in Article 2, Paragraph 1, Section cc) of Law 83/2017.

[98] For an international reference to the challenges and costs of implementing these regimes, *see* Arner, Douglas W., Barberis, Janos and Buckey, Ross P., *"FinTech..."*, cit., p. 391.

RegTech's usefulness in ensuring compliance. As a matter of fact, given that a person's qualification as politically exposed determines which legal framework will be applied to the transaction itself, it can be said that credit institutions would find it difficult to screen operations within a reasonable timeframe should they simply have do it by hand.

Furthermore, again in connection with the prevention of money laundering *RegTech* has increasingly (and even decisively) assisted in fulfilling the duty to analyze, exam [Article 11, Paragraph 1, Section g) and Article 52 of Law 83/2017] and report suspicious operations [Article 11, Paragraph 1, Section c) and Article 43 and following of Law 83/2017] by allowing entities, mostly through the use of AI (of a subset of AI in particular: *machine learning*[99]*), to identify their clients' suspicious activities*[100] *and, making use of ample databases, anomalies as well. AI is almost unavoidable in precluding the difficulties associated with automated systems (whose assessments and warnings are the result of a closed set of rules): they generate a huge number of "false positives"*[101]*, leaving a rather significant number of operations to be assessed by human persons*[102].

The (growing) use of technology is not only partially spontaneous, a result of the credit institution's need to meet its operative interests, but also to a great extent the regulator's de facto imposition, in the sense that it imposes on the institution demands which can only be met with the use of AI. A persuasive example of this was seen when the German regulator demanded that, in a relatively short period of time, a credit institution reassess 20 million financial operations it had made in the

[99] An explanation of machine learning may be found in Domingos, Pedro, *The master algorithm: How the quest for the ultimate learning machine will remake our world*, Basic Books, 2015, p. 5 ff. ("Every algorithm has an input and an output: the data goes into the computer, the algorithm does what it will with it, and out comes the result. Machine learning turns this around: in goes the data and the desired result and out comes the algorithm that turns one into the other. Learning algorithms — also known as learners — are algorithms that make other algorithms"). Given its great development and importance for AI, there is a tendency to associate one with the other, although this assimilation is incorrect. *See* Scopino, Gregory, *"Key..."*, cit., p. 23.

[100] *See*, for example, *"The case..."*, cit., p. 9.

[101] *See* Fruth, Joshua, *Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states*, cit., p. 3.

[102] *See* Kurum, Esman, *"RegTech solutions and AML compliance: what future for financial crime?"*, cit., p. 5.

past from a money laundering perspective[103]. It would only have been feasible to comply with the order by creating an AI-run tool, which is what ended up being done.

Besides, the goal of inducing credit institutions to use AI for the purpose of AML compliance is freely acknowledged in the field of regulation[104], without prejudice to the *principle of technological neutrality*. Such principle may take three different directions: (i) it can mean that the technical requisites for avoiding negative externalities (such as pollution, radio interference, etc.) are designed by defining the end result, all the while granting companies the freedom to choose the technology most appropriate to reach it; (ii) it can mean that those same regulatory principles are applicable regardless of the technology used by the regulated entity; or (iii) it can mean that regulators themselves should avoid using regulation as a means of steering the market to a certain structure which they deem optimal[105]. When taking into account the economic implications of the intensive use of technology – due to the scale economies it enables –, regulatory demands imposing the use of such technologies may surely lead to changes in the market's structure. It is therefore possible that the principle of technological neutrality will be reviewed and made flexible in a way that limits it to neutrality with regard to the "seller of technology" but not with regard to any other aspects[106]. *RegTech*'s advances in regulatory compliance and the increased use of technology articulated between the regulators and the regulated entities may in future require a certain harmonization of technological solutions, which will somewhat limit the principle of technological neutrality.

The benefits linked to AI and its associated technologies are many: AI offers the possibility of analyzing, screening, etc., the *complete*

[103] *See* Zimiles, Ellen, "How AI is transforming the fight against money laundering", *World Economic Forum*, 2019 (available at https://www.weforum.org/agenda/2019/01/how-ai-can-knock-thestarch-out-of-money-laundering).

[104] A report regarding the position of various regulators of favoring or stimulating the use of AI in AML compliance can be read in Estrada, Juan Carlos, *"The AML Arms Race: How Artificial Intelligence and Machine Learning Will Combat Money Laundering"*, in Rutgers Bus. LJ, 16, 2020, p. 393 ff.

[105] *See* Maxwell, Winston J and Bourreau, Marc, *"Technology neutrality in internet, telecoms and data protection regulation"*, in Computer and Telecommunications Law Review, 31, 2014, p. 1.

[106] *See "2021: A Critical..."*, cit., p. 19 ff.

universe of operations – regardless of their amount, the place where they're ordered, the jurisdiction to which their beneficiaries belong, the time and day of the week when they take place, etc. – *in real time* – for example, by blocking a credit card payment operation – through a collection of data ('big data') inaccessible to human knowledge. It is not just a benefit; it's also an *inevitability* if AML compliance is to be in any way effective in the face of the current financial situation: fully global, facing a growing use of electronic payments, and with an exponentially increased flow of goods. One should bear in mind the occasion when sales on *eBay*, paid for with *PayPal* and used to launder money for the Islamic State, went undetected[107]. It's simply not possible to fulfill the objective of AML compliance using human resources only. It may therefore be said that the development of technology both fuels money laundering and offers a solution to the problem[108].

V. RISKS AND CHALLENGES OF AI IN BANKING COMPLIANCE

Now that it has been established that the use of AI in AML (and regulatory) compliance tends to be inevitable[109], the risks[110] associated

[107] The evolution of the methods used by criminal networks for money laundering (namely, to upload it to the financial system) is huge and poses immense challenges to both the financial sector and compliance systems. For a description of these methods, *see* Miller, Geoffrey P., *"The Role of Risk Management and Compliance in Banking Integration"*, in NYU Law and Economics Research Paper, 14-34, 2014, p. 44 ff.

[108] *See* Estrada, Juan Carlos, *"The AML Arms Race: How Artificial Intelligence and Machine Learning Will Combat Money Laundering"*, cit., p. 386.

[109] Expressly in this sense, *see* Estrada, Juan Carlos, *"The AML Arms Race: How Artificial Intelligence and Machine Learning Will Combat Money Laundering"*, cit., p. 400, and, in respect of the use of *RegTech* for compliance, *see* Kurum, Esman, *"RegTech solutions and AML compliance: what future for financial crime?"*, cit., p. 3.

[110] The *risks* and, in truth, the *limitations* as well: as writes Packin, Nizan Geslevich, "*RegTech, Compliance and Technology Judgment Rule"*, in Chicago-Kent Law Review, Vol. 93, No. 1, 2018, p. 194, *RegTech* is not a cure-all for every problem. Artificial Intelligence systems used for compliance may succeed in identifying and reporting (regulatory or money laundering) breaches, but are very limited in creating a culture of compliance. And they may even become what the author calls *"anti-regtech" – the manipulation of technology to forge compliance with regulatory demands.*

with such use must be outlined. These risks have different natures and are at different levels.

Firstly, there exists the risk of the algorithm malfunctioning[111] as a result of a flawed or incorrect design. It's true that with algorithms, as with any other good or service, an error may occur. But here two significant particularities greatly aggravate the risk of that happening.

Secondly, the effects of an algorithm's imperfection tend to be exponentially aggravated: unlike human error[112], which is inclined to be limited to a (minority) share of each person's actions and is therefore *individual* and *partial*, an algorithm's error is inclined to be *universal* and *whole* since it will affect all of its activity and not just one part of it. If the same algorithm is already prevalent in the market and is used by several credit institutions, one sole mistake can have systemic repercussions. Technology's deficiencies or compromises may thus have universal consequences[113].

Thirdly, and of equal importance, detecting an error may be much harder – in some cases, it may even be impossible. Since AI feeds off big data, whose true extent is inaccessible to human knowledge, it becomes very difficult to recognize that, based on the information available ("unknown" to human persons on account of its magnitude), the algorithm has made wrong or inappropriate decisions.

This is one of the chief risks of AI: the data used to make decisions. The issues are many: the data might be incomplete because it was collected from a limited universe of samples, in which case the algorithm will be compromised due to the fact that, for example, it will draw conclusions about a certain universe from a distinct or far

See Packin, Nizan Geslevich, *"RegTech..."*, cit., p. 212 ff. On the risks of AI in the financial sector, *see*, most recently, EBA, *EBA Analysis...,* cit., p. 38 ff.

[111] In layman's terms, "an algorithm is a sequence of instructions telling a computer what to do" (*see* Domingos, Pedro, *The master algorithm: How the quest for the ultimate learning machine will remake our world*, cit., p. 1).

[112] The risk of AI elevating human errors may also be identified. In this sense, *see* Magnuson, William, *"Artificial..."*, cit., 125), p. 340 ff. ("the greatest danger of artificial intelligence is not that of exceeding human intelligence, but of exacerbating human error").

[113] *See* Bamberger, Kenneth A, *"Technologies of compliance: Risk and regulation in a digital Age"*, cit., p. 710 ff. (highlighting that the effects of "codifying" the algorithm are much like those of the law itself, which generalizes its applicability, creating a framework which persists over a long time).

away universe of samples; the data might contain *mistakes*[114] *(which of course harms the quality of AI's output: "garbage in, garbage out"*[115]*); the data might be (partially) false*, whether it be because fake news have been spreading on social media or because hackers have "poisoned data" so as to influence the AI's judgement – problems which can only be overcome by way of cleansing processes, exceedingly expensive because of the need to use massive human resources and therefore with a tendency to be avoided[116]; data might be *outdated*, in the sense that it does not correspond to the current reality; data might be a "compromised piece" of reality conveying the views or perceptions of society, or of a part of society – if the data includes news reports (and for the purpose of AML compliance it usually does) it's important to consider that mass media follows editorial guidelines, that journalists choose what to report, etc. A very telling example is that of the algorithm which, while using big data to recruit an employee, presumed that the employer preferred to hire men over women and thus proceed to reject every female candidate to the job. It all depends on data and on the conclusions – the patters and models – drawn from it by the algorithm[117]. The risk that AI may create instances of discrimination have been highlighted by theorists[118], with some authors going as far as saying that this side-effect is intrinsic to the prediction itself.

[114] The number of errors in reports from technical sources is surprising: in 2004, the *National Association of State Public Interest Research Groups* assessed that 79% of reports contained mistakes, 25% contained serious mistakes, 54% contained imprecise personal information, and 30% listed closed accounts as still active. *See "The case..."*, cit., p. 522 ff.

[115] *See* BUCKLEY, ROSS P., ZETZSCHE, DIRK A., ARNER, DOUGLAS W. and TANG, BRIAN W., *"Regulating..."*, cit., p. 50.

[116] *See* BUCKLEY, ROSS P., ZETZSCHE, DIRK A., ARNER, DOUGLAS W. and TANG, BRIAN W., *"Regulating..."*, cit., p. 51.

[117] Data related to *Enron* – the company which was at the center of one of the biggest and most serious scandals of accounting fraud and information forging – was used to feed compliance algorithms. *See* ENRIQUES, LUCA and ZETZSCHE, DIRK A., *"Corporate Technologies and the Tech Nirvana Fallacy"*, in European Corporate Governance Institute (ECGI), No. 457, 2019, p. 25.

[118] *See*, with updated information, MAGNUSON, WILLIAM, *"A Unified..."*, cit., p. 25 ff.

It's important to note that, when handling "big data", AI doesn't use information *as it is*, in its context[119]: algorithms necessarily disaggregate information into "pieces" only to re-aggregate it immediately afterwards and establish links between features which are in no way interconnected in real life. For example, absurd though it might sound, if an analysis of data demonstrates that more suspected money laundering operations take place between eight-thirty and nine-thirty in the morning, the algorithm will establish a link between time and money laundering and will start to consider the time when the operation takes place as an assessment criteria. Many more examples (even stranger and more absurd) may be thought of. Strictly speaking, the information dealt with by AI isn't *existing information*; it's *constructed information*, in the sense that associations which do not *actually* exist are created and established – associations which amount to an intellectualization of reality. What's more, information, in its full dimension and completeness, is something which exists *only for the machine*; it does not exist for human persons because they are incapable of knowing, processing and associating it with the vastness of data that, aided by supercomputers, the algorithm takes into account when making decisions.

In addition, although "big data" is information – which in and of itself doesn't represent anything new or specific – its characteristics greatly differ from those of common (traditional) information, something which makes them qualitatively different and poses specific problems: their *magnitude* – there is more data than ever before and it's being produced at an unprecedented rhythm; their *permanence* – data persists in time and may be stored indefinitely; and their *portability* – data may be copied, transferred, shared, and stolen[120].

One must not presume that the existence of a great magnitude and quantity of information means it's freely accessible. The fact that accessing to (constructed, aggregated, etc.) information tends to come at

[119] It must be highlighted that the data used by AI is not limited to existing or available data; data may be created for this purpose. For example, when a start-up company employs about 30 thousand workers to catalogue real-life images and then sells the data thus created to be used by artificial intelligence systems such as self-driving. *See* Magnuson, William, *"A Unified..."*, cit., p. 32.

[120] *See* Magnuson, William, *"A Unified..."*, cit., p. 29 ff.

an expensive price[121] in and of itself raises questions, especially when the access might be relevant to public interest, as is the case with AML compliance.

Besides risks related to *data*, there are (many) more related to the *algorithm* itself. AI is capable of learning *supervised* or *unsupervised*. Learning is *supervised* when the algorithm learns from a previously catalogued collection of data: for example, when the operations recorded in the database which the algorithm used as a starting point had already been classified as suspicious or not[122]. In a system such as this, the quality of the information (of the classification) is essential: if the information used for learning is incorrect or incomplete the algorithm may ultimately draw wrong conclusions[123].

On the other hand, learning is *unsupervised* when it rests on free data and takes place without previous training[124]. Although the risks associated with this method are clear, it ought not to be rejected on account of that because supervised learning will, in principle, prevent the algorithm from learning and identifying standards *different* from those underlining the collection of data used for training. Returning to the example used above, if criminal networks resort to a new method of money laundering – and they are always seeking to devise new ways unknown to authorities – that means the algorithm which

[121] *See* Buckley, Ross P., Zetzsche, Dirk A., Arner, Douglas W. and Tang, Brian W., *"Regulating..."*, cit., p. 49 ff.

[122] A common example found in literature, in the instance where it's intended that the algorithm identifies the image of a cat, consists of creating a database of images classified as "cat" or "non-cat" so that the algorithm then classifies other images. The programmer does not indicate the meaning of cat, or the determining elements of a cat's image; he or she simply ensures that the images used for "learning" have been correctly classified as "cat" or "non-cat". *See* Scopino, Gregory, *"Key..."*, cit., p. 30 ff.

[123] *See* Scopino, Gregory, *"Key..."*, cit., p. 32. The following example is given: if, in the collection of data made available to the system, all words ending with "ing" are classified as verbs – because the collection neither contain nouns (such as "king") nor adjectives (such as "interesting") ending with "ing" –, then the system will classify all words ending with "ing" as verbs in the future.

[124] In this regard, *see*, for example, Johnson, Kristin, Pasquale, Frank and Chapman, Jennifer, *"Artificial intelligence, machine learning, and bias in finance: toward responsible innovation"*, in Fordham L. Rev., 88, 2019, p. 506 ff., and Scopino, Gregory, *"Key..."*, cit., p. 30 ff. (who further differentiates "reinforcement learning").

learned under supervision will not (or will hardly be able to) identify an operation as suspicious, since an operation of that kind and the corresponding standard of suspicion were not present in the database which it was provided.

In addition, AI is rather *complex* and *opaque*, with its working model being called a "black box"[125] which poses the serious risk of resting on processes and operations unknown to persons (or even inaccessible to human knowledge) and therefore out of their respective control[126]. In truth, algorithms go through a huge collection of data, identify certain relationships or patterns, generate new standards with which to assess new data, etc. This working model makes it very difficult or even impossible to tangibly reconstruct the process leading up to the algorithm's decision[127]: this is what's called AI's *unpredictability*, also known as *unknowability* or *cognitive unaccountability*[128]*. Two risks arise therefrom: on the one hand, the inability of absolutely predicting* or anticipating the algorithm's future behaviors – there are no 100% safe algorithms[129]. On the other hand, the risk inherent to the (eventual) inability to demonstrate the reasoning behind the algorithm's decision creates many problems. First and foremost, it creates the problem of controlling the quality of its performance. Secondly, it creates a

[125] *See "The case...",* cit., p. 507 ("an effort to explain [AI's] «reasoning» would be about as useful as a map of all the synapses and other chemical reactions in the brain that occur when, say, a manager decides whether to grant or deny an employee's request for a vacation day").

[126] his leads some authors to claim the need of including humans in the circuit of artificial intelligence. *See* Buckley, Ross P., Zetzsche, Dirk A., Arner, Douglas W. and Tang, Brian W., *"Regulating...",* cit., p. 44 ff.

[127] *See*, for example, Estrada, Juan Carlos, *"The AML Arms Race: How Artificial Intelligence and Machine Learning Will Combat Money Laundering"*, cit., p. 401 ff. Setting "rule-based" AI – which rests on pre-determined rules and therefore allows for the explanation of decisions – against "machine learning" AI – which doesn't allow for the explanation of the reasoning behind its decisions, which are taken based on the identification of statistical correlations among the data –, *see* Kingston, John, *"Using artificial intelligence to support compliance with the general data protection regulation"*, in Artificial Intelligence and Law, Vol. 25, No. 4, 2017, p. 431 ff.

[128] *See* Yampolskiy, Roman V., *"Unpredictability of AI"*, in Cornell University, 2019, p. 2 (highlighting that the concept of artificial intelligence's *unpredictability* is related to, but not to be confused with, *unexplainability or incomprehensibility).*

[129] In this sense, *see* Yampolskiy, Roman V., *"Unpredictability...",* cit., p. 5.

regulatory problem: banks must be able to prove that they comply with regulatory demands. If it's not possible for them to demonstrate the reasoning behind the algorithm's decision that ability is compromised. For that reason, a previous commitment by the regulators to consider the use of AI as the fulfillment of certain regulatory demands has been needed in some cases. What some authors call legal risk (or "translation problem"[130]) is different from this: regulations aren't "machine-readable", meaning that they must always be translated into the algorithm, at the risk of the regulator's deficient – or discrepant – interpretation and the subsequent contamination of all compliance activity with an interpretation against the regulatory framework[131]. And problems pertaining to the General Data Protection Regulation are plentiful as well, namely the data subject's right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" (Article 22), or the right to be forgotten[132].

AI is but a piece of a *system* ("AI's ecosystem")[133], which has been experiencing an unparalleled technological development and which is already is widely used in the financial sector. But this new technology is so disruptive that it will entail new approaches in regulation – it's demanded that the regulators themselves take up AI when performing their duties – and in controlling the competitive effects that said new technology might generate. And it will also entail the creation of a

[130] The expression belongs to Bamberger, Kenneth A, *"Technologies of compliance: Risk and regulation in a digital age"*, cit., p. 706.

[131] In this regard, *see* Chiu, Iris H-Y and Lim, Ernest Wk, *"Managing Corporations' Risk in Adopting Artificial Intelligence: A Corporate Responsibility Paradigm"*, in Wash. U. Global Stud. L. Rev., 20, 2021, p. 366 ff.

[132] On questions raised by the general framework of data protection, *see* Buckley, Ross P., Zetzsche, Dirk A., Arner, Douglas W. and Tang, Brian W., *"Regulating..."*, cit., p. 58 ff., Arner, Douglas W., Zetzsche, Dirk A., Buckley, Ross P. and Weber, Rolf H., *"The Future..."*, cit., p. 256 ff., Kingston, John, *"Using..."*, cit., p. 439 ff., Kaya, Orçun, *"Artificial..."*, cit., p. 6, Chiu, Iris Hy and Lim, Ernest Wk, *"Managing Corporations' Risk in Adopting Artificial Intelligence: A Corporate Responsibility Paradigm"*, cit., p. 367, and Lee, Joseph, *"Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry"*, in European Business Organization Law Review, Vol. 21, 2020, p. 745.

[133] *See* Giuffrida, Iria, *"Liability for AI Decision-Making: Some Legal and Ethical Considerations"*, in Fordham Law Review, Vol. 88, 2019, p. 442.

legal framework which regulates the use of AI while both assuming its inevitability and the need to safeguard certain essential values[134] (already under preparation, as evidenced by the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence, *i.e.* the Artificial Intelligence Act).

A final reference should be made with regard to the risks of the (*RegTech*) market on which the provision of AI-related services rests. As previously stated, these can threaten the financial system. There's a strong tendency towards concentration in these markets, whether because financial institutions give preference to larger or more "mature" service providers – so as to reduce the risk posed by the service's shutdown[135] – or due to the existence of scale economies on the side of the provider: in 2018, the four largest cloud service providers held an 80% share of the world market and 25% of banks' core systems were stored in clouds[136]. There's a fear that the collapse of only one of these service providers may cause a worldwide disruption of banking systems. Usually, the extraordinary complexity of AI services and the outsized cost of developing them mean that they tend to be outsourced by institutions, which increases the risk of dependence on third parties, all the greater due to the market's concentration. Even though several steps were taken towards minimizing the systemic risks of financial institutions after the 2007-2008 financial crisis, it may be that a larger and unmitigated risk is developing with regard to the outsourcing of AI systems, clouding, etc. These risks are also intimately linked to intelligent compliance and need to be mitigated.

The evolution of traditional banking into "data-driven finance"[137] entails structural changes to the operation of banks, to the risks they are exposed to, and (maybe above all) to the risks which they expose

[134] The need to establish a framework of principles which artificial intelligence must abide by has been welcomed and stated by many. For an updated report and discussion on the possible or already implemented frameworks, *see* Buckley, Ross P., Zetzsche, Dirk A., Arner, Douglas W. and Tang, Brian W., *"Regulating..."*, cit., p. 57 ff., and Solow-Niederman, Alicia, *"Administering Artificial Intelligence"*, in S. Cal. L. Rev., 93, 2019, p. 635 ff.

[135] Identifying this fact and its implications, *see "2021: A Critical..."*, cit., p. 41.

[136] *See* Jung, John Ho Hee, *"RegTech..."*, cit., p. 269.

[137] The expression has been used by Arner, Douglas W., Zetzsche, Dirk A., Buckley, Ross P. and Weber, Rolf H., *"The Future..."*, cit., p. 245 ff.

third parties to, namely clients and citizens. This new stage is characterized by a strong interdependence between operation and frameworks: data protection frameworks, open banking frameworks, digital identification frameworks, and regulatory frameworks. Considering the European Union's all-encompassing interventions in 2018, it's not out of line to talk of a "Big Bang" in *RegTech* and "data-driven finance"[138].

In spite of having technology – namely AI – progressively more at its service, compliance will not go without the persistence of human intervention when it comes to two key aspects: the interpretation of regulatory frameworks – which withstand the "encoding" of algorithmic systems –, the observance of a culture of compliance within the organization, and the interpretation of compliance's development needs[139]. An (urgent) awareness of the risks associated with the massive introduction of AI (machine learning, in particular) in banking is necessary. Because of its complexity, speed, opaqueness, and interconnection, AI exposes the financial system to new and significant risks and thus makes it even more fragile, a "driverless" financial system with all associated risks[140].

REFERENCES

Allen, Hilary J., "Driverless Finance", in *Harvard Business Law Review*, Vol. 10, 2020, 158-206

Anagnostopoulos, Ioannis, "Fintech and regtech: Impact on regulators and banks", *Journal of Economics and Business*, Vol. 100, 2018, 7-25

Armour, John / Garrett, Brandon L./ Gordon, Jeffrey N. / Min, Geeyoung, "Board Compliance", *Minnesota Law Review*, Vol. 104, 2019, 1191-1273

[138] *See* Arner, Douglas W., Zetzsche, Dirk A., Buckley, Ross P. and Weber, Rolf H., *"The Future..."*, cit., p. 247 ff.

[139] *See* Chiu, Iris H.-Y. and Lim, Ernest W. K., *"Technology vs Ideology: How Far will Artificial Intelligence and Distributed Ledger Technology Transform Corporate Governance and Business?"*, in Berkeley Business Law Journal, Vol. 18, No. 1, 2021, p. 14.

[140] *See* Allen, Hilary J., *"Driverless Finance"*, in Harvard Business Law Review, Vol. 10, 2020, p. 158 ff.

Armour, John / Gordon, Jeffrey / Min, Geeyoung, "Taking Compliance Seriously", in *Yale Journal on Regulation*, Vol. 37, No. 1, 2020, 1-66.

Armstrong, Patrick, "Developments in RegTech and SupTech", in European Securities and Markets Authority, 2018, 1-7.

Arner / Barberis / Buckley, "The emergence of RegTech 2.0: From know your customer to know your data", *Journal of Financial Transformation*, vol. 44, 2016, 79-86

Arner, Douglas W., / Barberis, Jànos / Buckley, Ross P., "FinTech, RegTech, and the Reconceptualization of Financial Regulation", *Northwestern Journal of International Law & Business*, Vol. 37, No. 3, 2016, 371-414.

Arner, Douglas W. / Barberis, Jànos / Buckley, Ross P., "Fintech and Regtech in a Nutshell, and the Future in a Sandbox", *CFA Institute Research Foundation*, 2017, 1-20

Arner, Douglas W./ Buckley, Ross P./ Barberis, Janos N., "The Evolution of Fintech: A New Post-Crisis Paradigm?", *Georgetown Journal of International Affairs*, vol. 47, 2016, 1271-1319.

Arner, Douglas W./Zetzsche, Dirk A./Buckley, Ross P./Weber, Rolf H., "The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II", in *Standford Journal of Law, Business & Finance*, vol. 25, n.º 2, 2020, 245-288.

Baer, Miriam Hechler, "Governing Corporate Compliance", *Boston College Law Review*, vol. 50, 2009, 949-1019.

Bainbridge, Stephen M., "Caremark and Enterprise Risk Management", in *The Journal of Corporation Law*, vol. 34, 2008.

Bamberger, Kenneth A, "Technologies of compliance: Risk and regulation in a digital age", in *Tex. L. Rev.*, 88, 2009, 669.

Bank Of England, "Machine learning in UK financial services", 2019.

Banner, Stuart, "What causes new securities regulation? 300 years of evidence", *Washington University Law Quarterly*, 75, N.º 2, 1997, 1-6.

Bastos, Nuno Moraes, "Corporate Governance, Compliance e a Função Compliance nos Setores Bancários e Segurador", in *A Emergência e o Futuro do Corporate Governance em Portugal*, vol. II, Almedina, Coimbra, 2018, 207-234

Baumanns, Charlotte, „Fintech als Anlageberater? Die aufsichtsrechtliche Einordnung von Robo-Advisory", BKR, 2016, 366-375.

Bebchuk, Lucian A./Tallarita, Roberto, "The Illusory Promise of Stakeholder Governance", in Paper SSRN, 2020, 1-68.

Black, Julia, "Paradoxes and Failures: New Governance Techniques and the Financial Crisis", *The Modern Law Review*, vol. 75, n.º 6, 2012, 1037.

Bradley, Christopher G., "Fintech's Double Edges", *Chicago-Kent Law Review*, vol. 93, n.º 1, 2018, 61-95.

Brummer, Chris/Yadav, Yesha, "Fintech and the Innovation Trilemma", *The Georgetown Law Journal*, vol. 107, 2019, 235-307.

Buckley, Ross P./Zetzsche, Dirk A./Arner, Douglas W./Tang, Brian W., "Regulating Artificial Intelligence in Finance: Putting the Human in the Loop", *Sydney Law Review*, vol. 43, n.º 1, 2021, 43-8.

Calzolari, G., "Artificial Intelligence market and capital flows, Study for the Special Committee on Artificial Intelligence in a Digital Age", Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2021 (available at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU(2021)662912_EN.pdf)

Chiu, Iris H.-Y. and Lim, Ernest Wk, "Managing Corporations' Risk in Adopting Artificial Intelligence: A Corporate Responsibility Paradigm", *Wash. U. Global Stud. L. Rev.*, 20, 2021, 349-389.

Chiu, Iris H.-Y., "Regulating (From) the Inside. The Legal Framework for Internal Control in Banks and Financial Institutions", Hart Publishing, Oxford, 2015.

Chiu, Iris H.-Y./Lim, Ernest W. K., "Technology vs Ideology: How Far will Artificial Intelligence and Distributed Ledger Technology Transform Corporate Governance and Business?", *Berkeley Business Law Journal*, vol. 18, n.º 1, 2021, 1-63.

Coffee, John C. Jr., "Political Economy of Dodd-Frank: Why Financial Reform Tends to be Frustrated and Systemic Risk Perpetuated", *Cornell Law Review*, vol. 97, n.º 5, 2011, 1019-1082.

Coglianese, Cary/Lazer, David, "Management-based regulation: Prescribing private management to achieve public goals", *Law & Society Review*, 37, 4, 2003, 691-730.

Coglianese, Cary/Mendelson, Evan, "Meta-regulation and self-regulation", in *The Oxford Handbook of Regulation*, Oxford, Oxford University Press, 2010, 146–168.

Comissão Europeia, Livro Branco da Comissão Europeia sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança, 2020 (available at https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11eaaece--01aa75ed71a101aa75ed71a1.0004.02/DOC_1&format=PDF)

Cunningham, Lawrence A., "The Appeal and Limits of Internal Controls to Fight Fraud, Terrorism, Other Ills", *The Journal of Corporation Law*, vol. 29, 2004, 267-336

Deloitte, "The case for artificial intelligence in combating money laundering and terrorist financing. A deep dive into the application of machine learning technology", 2018, 1-37.

Der Elst, Christoph and Van Daelen, Marijn, "Risk Management in European and American Corporate Law", in ECGI-Law Working Paper, No. 122, 2009

Domingos, Pedro, "The master algorithm: How the quest for the ultimate learning machine will remake our world", Basic Books, 2015.

EBA Report on automation in financial advice, 2016, (available at https://esasjointcommittee.europa.eu/Publications/Reports/EBA%20BS%202016%20422%20(JC%20SC%20CPFI%20Final%20Report%20on%20automated%20advice%20tools).pdf)

EBA Report on big data and advanced analytics, 2020 (available at https://www.eba.europa.eu/sites/default/documents/files/document_library//Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf)

EBA, EBA Analysis of Regtech in the EU Financial Sector, 2021

EBA, Guidelines on Internal Governance (EBA/GL/2017/11, of March 21st, 2018, available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2164689/151a6ca3-31ae-40b0-9f55-9d6c65b86b00/Guidelines%20on%20Internal%20Governance%20%28EBA-GL-2017-

EBA, Study of the Cost of Compliance with supervisory reporting requirements, 2021 (Report EBA/Rep/2021/15)

EBF, Position paper on AI in the banking industry, 2019, (available at https://www.ebf.eu/wp-content/uploads/2020/03/EBF_037419-Artificial-Intelligence-in-the-banking-sector-EBF.pdf)

Enriques, Luca/Zetzsche, Dirk A., "Corporate Technologies and the Tech Nirvana Fallacy", *European Corporate Governance Institute* (ECGI), n.º 457, 2019, 1-51

ESMA – Joint Committee Final Report on Big Data, 2018 (available at https://www.esma.europa.eu/sites/default/files/library/jc-2018-04_joint_committee_final_report_on_big_data.pdf)

Estrada, Juan Carlos, “The AML Arms Race: How Artificial Intelligence and Machine Learning Will Combat Money Laundering”, in *Rutgers Bus. LJ*, 16, 2020, 383-408

European Banking Federation, “EBF position paper on AI in the banking industry”, 2019, 1-42.

European Commission, “FinTech Action Plan: For a more competitive and innovative European financial sector”, 2018

Fanto, James A., “The Professionalization of Compliance: Its Progress, Impediments, and Outcomes”, *Notre Dame Journal of Law, Ethics & Public Policy*, vol. 35, n.º 1, 2021, 183-240

Fein, Melanie L., “How Should Robo-Advisors Be Regulated? Unanswered Regulatory Questions”, in Allianz Global Investors, 2017, 1-14

Financial Conduct Authority, “Call for Input: Supporting the development and adoption of RegTech”, https://www. fca. org. uk/publication/call-for-input/regtech-call-for-input. pdf, 2015

Fonseca, Patrícia Afonso, “As Novas Orientações da EBA em Matéria de Governo Interno”, *A Emergência e o Futuro do Corporate Governance em Portugal*, vol. II, Almedina, Coimbra, 2018, 235-254

Fruth, Joshua, “Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states”, March, 2018.

Gadinis, Stavros/Miazad, Amelia, “The Hidden Power of Compliance”, *Minnesota Law Review*, vol. 103, 2019, 2135-2209.

Garrett, Brandon L, *Too Big to Jail*, Harvard University Press, Cambridge, 2014

Garrett, Brandon L. / Mitchell, Gregory, “Testing Compliance”, in *Law and Contemporary Problems*, Vol. 83, No. 4, 2020, 47-84.

Gebauer/Niermann, in Hauschka/Moosmayer/Lösler Corporate Compliance, 3. Auflage, 2016.

Giuffrida, Iria, “Liability for AI Decision-Making: Some Legal and Ethical Considerations”, *Fordham Law Review*, vol. 88, 2019, 439-456.

Griffith, Sean J., “Corporate Governance in an Era of Compliance”, *William & Mary Law Review Online*, vol. 57, n.º 6, 2016, 2075-2140.

Gunnar Groh, *Creifelds kompakt, Rechtswörterbuch*, 4. Auflage, 2021, Beck-online

Hauschka/Moosmayer/Lösler, *Corporate Compliance*, 3. Auflage, 2016, Beck-online

Hess, David, “Ethical Infrastructure and Evidence-Based Corporate Compliance and Ethics Programs: Policy Implications from the Empirical Evidence”, *New York University Journal of Law and Business*, Vol. 12, 2015.

Johnson, Kristin/Pasquale, Frank/Chapman, Jennifer, “Artificial intelligence, machine learning, and bias in finance: toward responsible innovation”, *Fordham L. Rev.*, 88, 2019, 499-528.

Jung, John Ho Hee, “RegTech and SupTech: the future of compliance*”, FinTech - Law and Regulation*, Elgar Financial Law and Practice, United Kingdom, 2019, 255-279

JWG, “Out of the window: COVID-19 prompts unexpected regulatory change for 2020 compliance, risk management work plans”, 2020 (available at https://www.corlytics.com/newsreleases/out-of-the-window-covid-19-prompts-unexpected-regulatory-change-for-2020-compliance-riskmanagement-)

Kaya, Orçun, “Artificial intelligence in banking: A lever for profitability with limited implementation to date”, in Deutsche Bank Research, 2019, 1-9.

Kingston, John, “Using artificial intelligence to support compliance with the general data protection regulation”, *Artificial Intelligence and Law*, vol. 25, n.º 4, 2017, 429-443.

Kpmg, “There’s a revolution coming. Embracing the challenge of RegTech 3.0”, 2018, 1-12

Kurum, Esman, “RegTech solutions and AML compliance: what future for financial crime?”, *Journal of Financial Crime*, ahead-of-print, ahead-of-print, 2020.

Labareda, João, “Contributo para o estudo do sistema de controlo e da função de cumprimento (“Compliance”)”, *Direito dos Valores Mobiliários*, 2016, 279-374.

Langevoort, Donald C, “Cultures of compliance”, *American Criminal Law Review*, vol. 54, 2017, 933-977.

Langevoort, Donald C., “Monitoring: the behavioral economics of inducing agents’ compliance with legal rules”, *Georgetown Univer-*

sity Law Center Business, Economics and Regulatory Policy, Law and Economics Research Paper, n.º 276121, 2001, 1-39.

Lee, Joseph, "Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry", *European Business Organization Law Review*, vol. 21, 2020, 731-757.

Lin, Tom C. W., "Artificial Intelligence, Finance, and the Law", *Fordham Law Review*, vol. 88, 2019, 531-551.

Lin, Tom C. W., "Compliance, Technology, and Modern Finance", *Brook. J. Corp. Fin. & Com. L.*, vol. 11, 2016, 159-181.

Lipshaw, Jeffrey M., "The False Dichotomy of Corporate Governance Platitudes", *The Journal of Corporation Law*, vol. 46, n.º 2, 2021, 346-384.

Lösler, Thomas, „Das moderne Verständnis von Compliance im Finanzmarktrecht", *NZG*, 2005, 104-108.

Machine learning in UK services, 2019, issued by the Bank of England and the FCA (available at https://www.bankofengland.co.uk/report/2019/machinelearning-in-uk-financial-services),

Magnuson, William, "A Unified Theory of Data", *Harvard Journal on Legislation*, vol. 58, 2021, 24-67.

Magnuson, William, "Artificial Financial Intelligence", *Harvard Business Law Review*, vol. 10, 2020, 338-382.

Maia, Pedro, "A robotização do mundo financeiro: reflexões introdutórias", in Estudos de Direito do Consumidor, n.º 16, Centro de Direito do Consumo - Instituto Jurídico, Coimbra, 2020, 273-306

Maia, Pedro, "Direito das Sociedades Bancárias", *Revista de Legislação e de Jurisprudência*, Ano 149º, n.º 4023, 2020, 372-411.

Marc Andreessen, "Why software is eating the world", *Wall Street Journal*, 2011.

Marco, Lamandini/Munoz David, Ramos, "A brief history of the evolution of financial institutions and of their regulation", *EU Financial Law. An introduction,* Cedam, Padova, 2016, 3-85.

Martinez, Veronica Root, "The Compliance Process", *Indiana Law Journal*, vol. 94, 2019, 203-251.

Maxwell, Winston J/Bourreau, Marc, "Technology neutrality in internet, telecoms and data protection regulation", *Computer and Telecommunications Law Review*, 31, 2014, 1-8.

Mayer, Colin, "The future of the corporation: Towards humane business", *Journal of the British Academy*, vol. 6, n.º 1, 2018, 1-16.

Mcneece, John B., "The Ethical Conflicts of the Hybrid General Counsel and Chief Compliance Officer", *Georgetown Journal of Legal Ethics*, vol. 25, 2012, 677-681.

Miller, Geoffrey P., "Risk Management and Compliance in Banks: The United States and Europe", *European Banking Union*, Oxford, United Kingdom, 2015, 200-216.

Miller, Geoffrey P., "The Role of Risk Management and Compliance in Banking Integration", *NYU Law and Economics Research Paper*, 2014, 14-34.

Miller, Geoffrey Parsons, "Compliance: Past, Present and Future", *University of Toledo Law Review*, vol. 48, 2016.

OECD, "OECD Council Recommendation on Artificial Intelligence", 2018 (available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449), adopted by the G20 in 2019 (available at https://www.mofa.go.jp/files/000486596.pdf).

Oliveira, Arlindo, *The Digital Mind: How Science is Redefining Humanity*, MIT Press, Cambridge, 2017.

Omarova, Saule T., "New Tech v. New Deal: Fintech as a Systemie Phenomenon", *Yale Journal on Regulation*, vol. 36, 2019, 735-793.

Orozco, David, "A Systems Theory of Compliance Law", *University of Pennsylvania Journal Business Law*, vol. 22, n.º 2, 2020, 244-302.

Packin, Nizan Geslevich, "RegTech, Compliance and Technology Judgment Rule", *Chicago-Kent Law Review*, vol. 93, n.º 1, 2018, 193-218.

Parker, Christine, "Meta-Regulation: Legal Accountability for Corporate Social Responsibility?", *The New Corporate Accountability: Corporate Social Responsibility and the Law*, Cambridge University Press, Cambridge, 2007, 207-237.

Parker, Christine, "The Open Corporation: Effective self-regulation and Democracy", Cambridge University Press, Cambridge, 2002

Piri, Michael M., "The Changing Landscapes of FindTech and RegTech: Why the United States Should Create a Federal Regulatory Sandbox", *Business & Finance Law Review*, vol. 2, n.º 2, 2019, 233-255.

Portugal Finlab Report, 2nd Edition, 2020 (available at https://8080dd92-d6fc-49d9-a97eb24c8f013bb2.filesusr.com/ugd/ca9a53_217c4187d5bd4a5a9b377c6f6500e0ff.pdf)

Rock, Edward B., "For Whom is the Corporation Managed in 2020?: The Debate over Corporate Purpose", in European Corporate Governance Institute - Law Working Paper, n.º 515, 2020, 20-16.

Rodrigues, Anabela Miranda, *Direito Penal Económico: Uma Política Criminal na Era Compliance*, 2.ª ed., Almedina, Coimbra, 2021.

Schneider, Uwe, "Compliance als Aufgabe der Unternehmensleitung", *ZIP*, 2003, 645-650.

Schumpeter, Joseph, *Capitalismo, Socialismo e Democracia*, Actual Editora, Coimbra, 2018.

Scopino, Gregory, "Key Concepts: Algorithms, Artificial Intelligence, and More", in *Algo Bots and the Law. Technology, Automation, and the Regulation of Futures and Other Derivatives*, Cambridge University Press, Cambridge, 2020, 13-47.

Scott, Colin, "Regulating everything: From mega-to meta-regulation", in Administration, vol. 60, 2012, 57-85

Simmons, Omari Scott/Dinnage, James D., "Innkeepers: A Unifying Theory of the In-House Counsel Role", in Seton Hall Law Review, vol. 41, n.º 1, 2011, 77-152.

Sokol, D. Daniel, "Twenty-Eighth Annual Corporate Law Center Symposium: Rethinking Compliance", *University of Cincinnati Law Review*, vol. 84, n.º 2, 2016, 399-420.

Solow-Niederman, Alicia, "Administering Artificial Intelligence", in S. Cal. L. Rev., 93, 2019, 633-696.

Sousa, Susana Aires De, "A colaboração processual dos entes coletivos: legalidade, oportunidade ou "troca de favores"?", in *Revista do Ministério Público*, n.º 158, 2019, 9-36.

The Global City, 2021, "2021: A Critical Year of RegTech", 2021, 1-76.

Treleaven, Philip, "Financial regulation of FinTech", *Journal of Financial Perspectives*, 3, 3, 2015, 1-14.

Van Der Elst, Christoph/Van Daelen, Marijn, "Risk Management in European and American Corporate Law", in ECGI-Law Working Paper, n.º 122, 2009.

Weber-Rey, Daniela, "Der Aufsichtsrat in der europäischen Perspektive - Vorschläge und Ideen für eine wirksame Corporate Governance", in NZG, 2013, 766-770

Yampolskiy, Roman V., "Unpredictability of AI", in Cornell University, 2019, 1-10.

Yang, Yueh-Ping (Alex) and Tsang, Chengyun, "RegTech and the New Era of Financial Regulators: Envisaging More Public-Private-Partnership Models of Financial Regulators", *University of Pennsylvania Journal of Business Law*, 2018, 354-404 (available at https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206)

Zimiles, Ellen, "How AI is transforming the fight against money laundering", *World Economic Forum*, 2019 (available at https://www.weforum.org/agenda/2019/01/how-ai-can-knock-thestarch--out-of-money-laundering)