ON THE POTENTIALITIES AND LIMITATIONS OF AUTONOMOUS SYSTEMS IN MONEY LAUNDERING CONTROL

By Leonardo Simões Agapito [*], *Matheus de Alencar e Miranda*[**] *and Túlio Felippe Xavier Januário*[***]

Abstract

This paper analyses the potential gains and eventual difficulties using autonomous systems – such as artificial intelligence (AI) mechanisms – to prevent, detect and investigate money laundering. As it is well-known, new technologies have been applied in the most varied social contexts, being no different in the case of the FIUs, especially when receiving and processing reports of suspicious activities from obligated entities. However, in addition to the already identified difficulties imposed by new technologies, the specific scope of money laundering presents particular challenges. Potential guidelines are proposed for a better interaction between AI and money laundering prosecution. For that, is is initially analysed what is effectively meant by AI and autonomous systems and how they are effectively used in this scope. Subsequently, some of the difficulties encountered in this context are demonstrated, ranging from insufficiency, low quality and inaccuracy of data that feed the systems, to the difficulties in understanding, explaining and allowing the refutation of the conclusions reached by them. From this analysis and through a deductive methodology, possible solutions are proposed that allow a better and more efficient interaction between humans and autonomous systems in the field of money laundering and its prosecution.

1 Introduction

It is currently undeniable that facing drug trafficking, terrorism and other misconducts related to organized criminality depends to a great extent on public instruments capable of preventing the circulation not only of the proceeds of crime, but also of the capital needed for its commission. It is in this context that criminal prosecution of money laundering reached a larger international consensus in terms of criminal policy in the 20th Century.[1]

[*] PhD Student in Latin American Integration, University of São Paulo. For correspondence: <leoagapito@gmail.com>.

[**] PhD Candidate in Criminal Law, State University of Rio de Janeiro. For correspondence: <matheus.alencarm@gmail.com>.

[***] PhD Fellow, Fundação para a Ciência e a Tecnologia (FCT), University of Coimbra. For correspondence: <tuliofxj@gmail.com>.

[1] See: Pierpaolo Cruz Bottini, 'Aspectos Conceituais da Lavagem de Dinheiro' in Gustavo Henrique Badaró and Pierpaolo Cruz Bottini (eds), *Lavagem de Dinheiro: Aspectos Penais e Processuais Penais: Comentários à Lei 9.613/98, com alterações da Lei 12.683/12* (4th edn, Thomson Reuters Brasil 2019) 25-29; Benjamin Vogel, 'Introduction' in Benjamin Vogel and Jean-Baptiste Maillart (eds), *National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection* (Intersentia 2020) 1.

The globalization experienced in money laundering, the trend toward crime professionalization and especially the complexity and ability to adapt and create new methods of committing these misbehaviors[2] are some of the challenges that require constant attention from the policymakers, when defining preventive and repressive strategies.[3-4]

As one example of such policies, the unification of security and inspection standards of banking systems became imperative with the intensification of international financial operations. In this scope, while international cooperation treaties on transnational and organized crime took a few years to be properly internalized and operationalized in the different signatory countries, the FATF recommendations and the articulation of the Egmont system were rapidly assimilated, imposing rigorous information standards from obligated entities. However, these recommendations do not always consider the diversified actuation of banking entities in their respective countries and may be ineffective in identifying possible criminal conducts.

The present work starts from the premise that ignoring local particularities may end up affecting the quality of data that foster autonomous systems used by the Financial Intelligence Units (FIUs), reducing their effectiveness and increasing the risk of false positives and false negatives. Furthermore, it is undeniable that autonomous systems and artificial intelligence (AI) mechanisms still have some inherent limitations, such as the opacity of their proceedings and the consequent difficulties in understanding (and sometimes refuting) their conclusions.

In view of these difficulties, the main goal of the present article is to understand how data- and regulation-related issues can affect the efficiency of money laundering prosecution, even with the employment of AI and autonomous systems for its detection and prevention. Aiming at proposing some guidelines for a better interaction between these sectors, we will initially describe what we can understand by AI and autonomous systems and how these technologies are effectively applied in the prevention, detection and

[2] Isidoro Blanco Cordero, *El Delito de Blanqueo de Capitales* (2nd edn, Aranzadi 2002) 51-55.

[3] As pointed out by Nuno Brandão, money laundering shows itself as the dark side of the globalization process, the liberalization of international exchanges and capital movements, the opening of markets, the massive computerization and the electronic commerce. If, on the one hand, there have always been economic criminality and attempts to dissimulate illicit gains, these activities have never been of such proportion and reached so many interests as in the present time. See: Nuno Brandão, *Branqueamento de Capitais: O Sistema Comunitário de Prevenção* (Coimbra Editora 2002) 16-17. For a detailed analysis of the impacts of technological innovations on money laundering, see also: Miguel Abel Souto, 'Blanqueo, Innovaciones Tecnológicas, Amnistía Fiscal de 2012 y Reforma Penal' (2012) 14 Revista Electrónica de Ciencia Penal y Criminología 1 <http://criminet.ugr.es/recpc/14/recpc14-14.pdf> accessed 14 July 2021.

[4] On the global context of money laundering and its characteristics, see also: Anna Carolina Canestraro, 'Compartilhamento de Dados e Persecução do Crime de Branqueamento de Capitais no Âmbito dos Paraísos Financeiros' (2018) 22(35) Revista de Estudos Jurídicos Unesp 135, 137-139 <https://doi.org/10.22171/rej.v22i35.2197> accessed 12 July 2021; Anna Carolina Canestraro, 'Cooperação Internacional em Matéria de Lavagem de Dinheiro: da Importância do Auxílio Direto, dos Tratados Internacionais e os Mecanismos de Prevenção' (2019) 5(2) Revista Brasileira de Direito Processual Penal 623, 626-633 <https://doi.org/10.22197/rbdpp.v5i2.234> accessed 12 July 2021.

prosecution of money laundering. Once these concepts and their respective applications are delimited, we will investigate their main limitations and obstacles. In the end, we will demonstrate how a new structure could be designed to be able not only to mitigate the well-known issues of data bias but also make regulatory enforcement in this matter more effective.

2 Autonomous Systems, AI and their Application to Money Laundering Control

It is currently common to encourage automation of all kinds of tasks, including those related to the criminal justice system. In particular, the automation of repetitive tasks and data analysis for investigations stands out. In this context, automation still occurs mainly through *autonomous systems,* which are previously programmed for autonomous decision-making (without immediate human intervention). However, an undeniable expansion in automation is currently observed due to an increase in employment of AI.[5]

According to the European Commission, AI can be understood as 'systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals'. In the Communication 'Artificial Intelligence for Europe', the Commission explains that these systems 'can be purely software-based, acting in the virtual world' (eg voice assistants) or 'embedded in hardware devices' (eg autonomous cars).[6]

Despite this definition, there is still some confusion in criminal justice system regarding the distinction between automation and AI.[7] For the purposes of this essay, we will consider AI as machine intelligence, capable of solving problems similarly to a human being, as having the ability to understand its environment through data inputs and, based on them, to choose a course of action among several possible others, aimed at solving a posed problem.

Also for the purposes of this essay, autonomous systems are those capable of reacting to the environment without the need for human intervention (therefore, autonomous) but unable to choose a course of action or create a new solution to a problem (therefore, not

[5] According to Fabiano Hartmann and Roberta Zumblick, artificial intelligence operates through the identification of patterns in the available database, prioritizing, from them, behaviors that have positive effects related to the objective sought. Widely used to find patterns and classify documents, this technology has expanded to other functions as well. See: Fabiano Hartmann Peixoto and Roberta Zumblick Martins da Silva, *Inteligência Artificial e Direito* (Alteridade Editora 2019) 63ff.

[6] European Commission, 'Communication From the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions (Artificial Intelligence for Europe)' COM(2018) 237 final.

[7] On these concepts and distinctions, see: Amedeo Santosuosso and Barbara Bottalico, 'Autonomous Systems and the Law: Why Intelligence Matters' in Eric Hilgendorf and Uwe Seidel (eds), *Robotics and the Law: Legal Issues Arising from Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy* (Nomos 2017) 35ff.

intelligent). These systems only present a pre-programmed response according to the environment identified by them.[8]

Having in mind this distinction is important because it enables a better comprehension of the technological *state-of-art* and possible improvements in each kind of system. In this sense, AI can be seen as an 'umbrella concept', which encompasses several subfields such as robotics, machine learning and natural language processing.[9]

With specific regard to the application of these systems in criminal justice, we can observe their consolidated usage in the internationally standardized model for the prevention of money laundering. Preventive regulation of these crimes requires constant data provision from obligated agents. This data provision forms a huge database that is impossible to be manually verified in the scope of prevention, detection and repression of suspect transactions. Thus, there is a rise in demand for automation in the verification of patterns, which greatly encourages the use of autonomous systems and creates conditions for the development of massive and problem-solving AI.

Highlighting the international standardization of regulation in this matter, we must mention the Basel Capital Accord I, of 1988, whose main objectives were: a) 'to strengthen the soundness and stability of the international banking system'; and that b) 'the framework should be in fair and have a high degree of consistency in its application to banks in different countries with a view to diminishing an existing source of competitive inequality among international banks'.[10] In order to achieve these goals, the document devoted special attention to establishing risk assessment standards. It is important to mention that the three subsequent accords aimed to respond to the intensification of financialization and to the economic crises of the 1990s and of 2008, demonstrating that financial systems were already deeply integrated.[11]

Financial systems integration had an undeniable impact on control mechanisms and on the need for their coordination coordination. Following the FATF recommendations, they can be categorized into: (a) information duties; (b) compliance duties.

---

[8] We are aware that the complexity of the distinction is higher than that briefly presented here. However, in terms of juridical and criminal consequences, it is essential to distinguish these two types of technology. This delimitation will directly reverberate in the conclusions that we will reach in this article. For a more detailed analysis of this issue, see: Eric Hilgendorf, 'Recht und autonome Maschinen – ein Problemaufriß' in Eric Hilgendorf and Sven Hötitzsch (eds), *Das Recht vor den Herausforderungen der modernen Technik* (Nomos 2015); Peixoto and Silva (n 5).

[9] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51(2) UC Davis Law Review 399, 405 <https://lawreview.law.ucdavis.edu/issues/archive.html> accessed 13 July 2021; Peixoto and Silva (n 5) 75.

[10] Basel Committee on Banking Supervision, 'International Convergence of Capital Measurement and Capital Standards (Basel Capital Accord I)' (1988) 1.

[11] Peter Went, 'Basel III Accord: Where Do We Go From Here?' (2010), 11 <https://dx.doi.org/10.2139/ssrn.1693622> accessed 13 July 2021.

As regards (a) information duties, the following is suggested: i) *national cooperation and coordination mechanisms* (Recommendation n. 2); ii) '*that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations*' (Recommendation n. 9); iii) *customer due diligence,* when certain conditions are observed and following certain procedures (Recommendation n. 10); iv) *record-keeping* (Recommendation n. 11); v) *reporting of suspicious transactions* (Recommendation n. 20) and vi) *transparency and beneficial ownership of legal arrangements* (Recommendation n. 25).[12]

Regarding b) compliance duties, it is recommended that States, when implementing an action model, assess the main sources of risk to which their institutions are subject, promoting programs that effectively curb terrorist financing and money laundering. This analysis is also required from institutions and professionals that operate in the financial system.[13]

With regard to the FIUs, the FATF reinforces the importance of their autonomy and active role, recommending a broad scope of powers and responsibilities of competent authorities (Recommendations 26-35).[14]

The imposition of the security systems resulting from these recommendations encourages regulatory models such as good governance and compliance, in addition to differentiated models of responsibility attribution, aiming at responding to the 'organizational deficits' or states of 'organized irresponsibility' from companies. In order to guarantee the stability of the economic system, collaboration duties are resorted to.[15]

In addition, in sectors that are sensitive to money laundering, some people are selected to act as *gatekeepers* against suspicious activities, preventing the commitment of crimes and reporting it to the central intelligence agency.[16] Taking this preventive potential as a premise, legislations around the world have intensely focused on creating duties for these economic agents. However, this premise is imprecise because the model promotes dependence of control agents on the information provided by *gatekeepers* and the quality

[12] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations)' (2012-2020).

[13] ibid.

[14] '29. Financial intelligence units * Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly'. Ibid.

[15] Eduardo Saad-Diniz, 'Fronteras del Normativismo: a Ejemplo de las Funciones de la Información en los Programas de Criminal Compliance' (2013) 108 Revista da Faculdade de Direito da Universidade de São Paulo 415, 423.

[16] See: John C. Coffee Jr., 'Understanding Enron: It's About the Gatekeepers, Stupid' (2002) 207 Columbia Law School Working Paper 1, 5 <https://dx.doi.org/10.2139/ssrn.325240> accessed 14 July 2021; John C. Coffee Jr, 'The Attorney as Gatekeeper: An Agenda for the SEC' (2003) 103(5) Columbia Law Review 1293, 1296ff <https://doi.org/10.2307/1123838> accessed 14 July 2021; Ana Carolina Carlos de Oliveira, *Lavagem de dinheiro: responsabilidade pela omissão de informações* (Tirant lo Blanch 2019) 30.

of this information is not consistent. Since this dependence can generate a series of problems, this 'surrender' of the supervisory body to interinstitutional cooperation is seemingly no longer adequate, requiring a new framework that can change the correlation of forces through the implementation of new mechanisms.

In any case, one of the main tasks of the FIUs is to receive the Suspicious Activity Reports (SARs) and other information related to money laundering, having access to public (and often private commercial) databases to properly perform their analysis.[17] At this point, the issue regarding the use of data analytics and data mining in these procedures gains relevance.

In Brazil[18], for example, the SARs received by the FIU are submitted to a pre-programmed electronic analysis and distributed individually to technical analysts. Both the communication and its procedure are registered in the same software, so that the database can have an increasing and constructive volume that will serve as subsidy resolutions of subsequent communications.

This logic is the same as that applied to several AI tools: identification of patterns in the database and detection of other similar operations and new patterns. In this case, the patterns are the ones that, based on recorded financial transactions, indicate money laundering. The correlation probability between the operation and the pattern is equal to the probability vector of the money laundering risk matrix.

In the Brazilian system, following the procedure mentioned above, the 'Risk and Priority Management Center (CGRP)' scrutinizes each communication and creates a specific file for each case. The cases are ranked by the CGRP according to the degree of risk, in a procedure that already follows the logic of an autonomous system: the higher the risk assessed by the system, the greater attention will be given to the case.

To summarize, we can affirm that the contemporary model of money laundering and terrorist financing prevention (which is globally standardized) has automation at the basis of its prioritization of investigations and the Brazilian case is a good example of this kind of practice. We can observe that if, on the one hand, the procedure is currently performed by an autonomous system with some human intervention, on the other, the sector has enormous potential for AI application, given the use of large databases for the identification of patterns and subsequent detection of similar operations or new patterns of money laundering.

---

[17] Jean-Baptiste Maillart, 'Anti-Money Laundering Architectures: Between Structural Homogeneity and Functional Diversity' in Benjamin Vogel and Jean-Baptiste Maillart (eds), *National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection* (Intersentia 2020) 839ff.

[18] For a more detailed analysis of the Brazilian preventive model: COAF, *Casos & Casos: I Coletânea de Casos Brasileiros de Lavagem de Dinheiro: Edição Comemorativa pelos 10 Anos do Conselho de Controle de Atividades Financeiras* (COAF 2011) 10ff.

The consequences of the autonomy of the procedure can be seen in the continuity of the investigation and in the subsequent prosecution of money laundering. Currently, Financial Intelligence Reports can be instigated: i) spontaneously by FIUs; (ii) from exchanges of information with other regulatory agencies; iii) requested by a foreign authority. If the autonomous analysis indicates signs of money laundering, the report must be sent ahead to the competent authorities, alongside with all the evidence collected. From this moment on, the reports often serve as a subsidy for criminal investigations and evidence in criminal proceedings.

Considering international requirements and the particularities of money laundering and its perpetrators, it is evident that investigation and prevention by FIUs demand major financial, technological and personnel resources. However, practical experience demonstrates that these expectations are not fulfilled, specially taking into account the infrastructure of the FIUs in developing countries.[19]

That said, it is possible to point out an interdependence between regulation and automation in the system of money laundering prevention. In other words, it is clear that the feasibility of regulation enforcement depends on automation, given the discrepancy between the volume of SARs to be analyzed and the human resources available to carry out the enforcement. On the other hand, the automation of this system is only possible due to the database provided by the regulation. In short, without database there is no system development (autonomous or AI). Ultimately, the success of automation will always depend on the quality of the data provided by the regulation and the success of the latter will always depend on the quality of automation.

3 Challenges in Using AI to Control Money Laundering

Considering the abovementioned regulatory standards, AI systems involved in money laundering surveillance face at least three different kinds of challenges, which are: a) *inadequacy of data produced by FIUs*; b) *lack of reliability of data produced by FIUs*; c) *opacity of AI*. We will now analyze each of them in detail.

3.1 Insufficiency and inadequacy of data

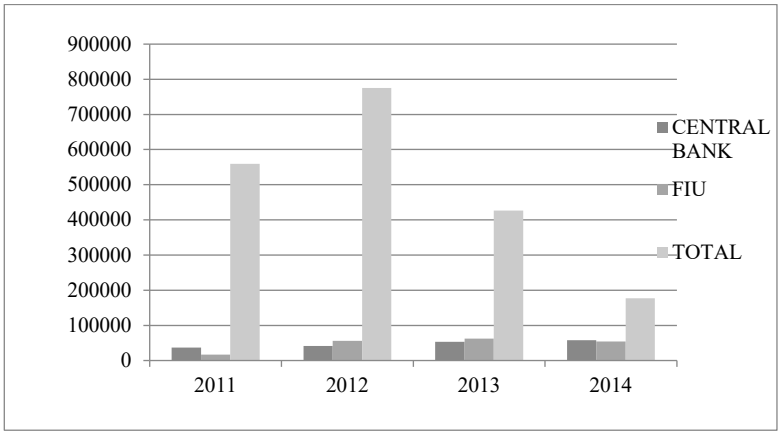
When analyzing the FIUs' reports, it remains clear that the abovementioned informational standards end up creating further issues, besides money laundering itself. As an example, it has been already demonstrated that, in the last decade, the Brazilian FIU suffered a decrease in its efficiency along the years, contrasting with the expansion of informational duties. At the beginning of its activities, there was an increase in the number of

[19] In Brazil, for example, according to the Federal Decree n. 9.003/17, the FIU has 31 employees, 15 of them responsible for analyzing and supervising the SARs. Considering the volume of almost 1.5 million SARs, it is evident that, without automation, the FIUs would be unable to perform their duties. See: José Carlos de Oliveira, Leonardo Simões Agapito and Matheus de Alencar, 'O Modelo de "Autorregulação Regulada" e a Teoria da Captura: Obstáculos à Efetividade no Combate à Lavagem de Dinheiro no Brasil' (2017) 10 Quaestio Iuris 365, 378-381 <https://doi.org/10.12957/rqi.2017.26847> accessed 14 July 2021.

investigations, charges and convictions for money laundering.[20] Furthermore, the Central Bank of Brazil used to be effective back then in demanding and analyzing accurate information from its regulated entities before transferring it to the FIU. Nevertheless, while the number of SARs increased, the efficiency dropped. According to the FIU's statistics, in 2009, 93,270 SARs were reported by the sectors regulated by the Central Bank of Brazil, with a 57% level of efficacy (useful percentage of the information provided).[21] After the internalization of Basel III Standards in 2010 and the intensification of the FATF's demands for an anti-terrorism agenda, the number of operations reported by the Brazilian Central Bank grew to 1,289,087 in 2011; 1,587,427 in 2012; 1,286,233 in 2013; and 1,144,542 in 2014, but the efficacy level was below 30%.[22]

With regard to atypical operations, which have attracted major attention from regulatory authorities, since they present evidence of money laundering, the numbers appear to follow a downward trend: 559,992 in 2011 (37,237 from the Central Bank; 16,684 from the UIF); 775,535 in 2012 (41,819 from the Central Bank; 55,646 from the UIF); 426,153 in 2013 (53,244 from the Central Bank and 62,732 from the UIF) and 177,467 in 2014 (57,455 from the Central Bank and 53,818 from the UIF). In absolute numbers, graphically:[23]

Graph 1 – The SARs reported to the FIU in Brazil[24]



The graph shows the above-mentioned decrease in the total number of suspicious operations over time. If communications plummeted, however, the proportion of suspicious transactions among those notified also decreased, reaching the number of 177,467 atypi-

[20] Remarkably in the period from 2003 to 2006, when a massive computerization and major integration between authorities occurred (especially between the FIU and the Federal Police). See: Vanessa Alessi Manzi, *Compliance no Brasil: consolidação e perspectivas* (Saint Paul 2008) 57-59.
[21] Marcelo de Aguiar Coimbra and Vanessa Alessi Manzi, *Manual de Compliance* (Atlas 2010) 72.
[22] Oliveira, Agapito and Alencar (n 19) 378-381.
[23] ibid. 379.
[24] ibid. 379.

cal transactions compared to 1,144,542 total communications in 2014. This amount to almost one million communications not used for elaborated investigations, only stored as data.

Thus, we can observe some consequences caused by the tightening of duties: i) an initial exponential increase of communications; ii) a reduction of effectiveness of the inspections; iii) changes in procedure of regulated entities, which started to financially behave below 'atypical' standards.

It is crucial to highlight that while this reactive movement is itself capable of creating different problems for the analysis by autonomous systems (especially in terms of bias, false positives and false negatives), the high number of useless operations reveals an even major problem: the data have not been properly used for effective action.

3.2 Unreliable data

The global model of money laundering prevention is based on trust in the communications made by obligated agents. From them, a database of operations will be created, which will be the basis for the analysis and detection of suspicious operations. Therefore, it is important to verify whether these communications are providing a reliable database.

However, there are different mechanisms and opportunities for obligated entities to manipulate and to mislead the authorities. In other words, a regulated agent can take advantage of the regulatory entity's dependence and the minimum possibility of being discovered to falsify or hide essential information. At the same time, he or she can purposefully communicate various supposedly suspicious operations, which are known to be lawful, in order to overload the regulators with information and, thus, increase their dependence.[25]

In such situations, it is evident that the autonomous system of money laundering prevention is hampered by the low quality of the database. A solution to this issue is complex, since the regulatory body does not even have enough means to check all the communications provided. The verification of those that were maliciously provided is even less feasible.

On the other hand, in cases where suspicious activities are not reported, the discovery of these crimes is also unlikely – the discovery being generally dependent on criminal proceedings involving other offenses. And even when they are discovered, administrative punishment for incorrect communication from the obligated agents rarely occurs, given

[25] An exemplary case occurred in Brazil, within the scope of Criminal Action 470/MG ('Mensalão'). One of the defendants was convicted of money laundering by the Supreme Court and the decision was based, among other reasons, on the falsification of data and omission of communications to the FIU. It is important to highlight that this conduct was not detected by the regulatory agency and was only discovered in the course of the criminal action, through documents and witnesses that contradicted the content of the false communications. For more details, see: Oliveira, Agapito and Alencar (n 19) 381.

the lack of alignment between different control bodies, especially between the public prosecutors and enforcement agencies.

Finally, regulated institutions have also developed their own autonomous systems to manage risks and guide enterprises through new opportunities. However, these systems are hardly comprehended even by their developers. In Brazil, for example, the new regulation on stock markets demands a complex report on risk assessment programs, including on numbers of operations detected and notifications.[26] These numbers are consistently useless to guarantee effectiveness but will be utterly understood under a qualitative verification. It is necessary to create a new framework to validate the employment of AI in money laundering risk management programs.

3.3 Limitations of AI

In addition to the aforementioned difficulties encountered in the prevention and prosecution of money laundering, we cannot disregard the fact that autonomous systems and AI have also serious limitations, which certainly reverberate when applied in this field.

Firstly, since these technologies depend on mass processing of data, the concern about the security, reliability and lawfulness of these data is crucial.[27] More specifically, it is important to ensure that they were not obtained by violating rights of their holders. In any case, there is an undeniable risk that these data may be biased, as they may end up reflecting their developers' prejudices and discriminations.[28]

Furthermore, there are undeniable difficulties in understanding, controlling and, consequently, refuting the conclusions reached by the AI and its algorithms. For this reason, AI is considered opaque, since there are no concrete conditions for measuring 'how' and 'why' the outputs are produced, and even the input is often unknown. That is why these algorithms are commonly equated to 'black boxes'.[29]

---

[26] Comissão de Valores Mobiliários, 'Instrução CVM n.617, de 5 de dezembro de 2019' <http://conteudo.cvm.gov.br/legislacao/instrucoes/inst617.html> accessed 13 July 2021.

[27] Caitlin Mulholland and Isabella Z. Frajhof, 'Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: Breves Anotações Sobre o Direito à Explicação Perante a Tomada de Decisões por Meio de Machine Learning' in Ana Frazão and Caitlin Mulholland (eds), *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade* (Thomson Reuters Brasil 2019).

[28] See: Adrienne Yapo and Joseph Weiss, 'Ethical Implications of Bias in Machine Learning' [2018] *Proceedings of the 51st Hawaii International Conference on System Sciences* 5365, 5366; Peixoto and Silva (n 5) 34-35; Túlio Felippe Xavier Januário, 'Considerações Preambulares Acerca das Reverberações da Inteligência Artificial no Direito Penal' in Murilo Siqueira Comério and Tainá Aguiar Junquilho (eds), *Direito e Tecnologia: um debate multidisciplinar* (Lumen Juris 2021).

[29] See: Jenna Burrell, 'How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data & Society 1, 1 <https://doi.org/10.1177/2053951715622512> accessed 23 January 2020; William Nicholson Price II, 'Artificial Intelligence in Health Care: Applications and Legal Issues' (2017) 599 U of Michigan Public Law Research Paper 1, 2 <https://ssrn.com/abstract=3078704> accessed 23 January 2020; Miriam Wimmer, 'Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios' in Ana Paula M. Canto de Lima, Carmina Bezerra Hissa and Paloma Mendes Saldanha (eds), *Direito Digital: Debates Contemporâneos* (Thomson Reuters Brasil 2019); Anabela Miranda

Without disregarding the undeniable benefits of AI, it is certain that its limitations imply difficulties to be faced in the most diverse sectors in which this technology is applied.[30] When it refers to usage that directly or indirectly impacts on the criminal justice system, these difficulties are even more accentuated, given the importance of the interests in question.

Far beyond the relevant reverberations in evidentiary matters and the countless controversies that they raise,[31] the progressive usage of autonomous systems and AI in decision-making in several phases of intelligence, investigation and judicial instruction procedures sparks endless debates regarding AI's feasibility and limits.[32]

In the scope of money laundering prevention, similar questions must be considered. What kind of public and private data can be used by autonomous systems? How people directly affected by these systems could understand the reasons and contest eventual

Rodrigues, 'Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020) 25.

[30] For an exemplary study of these potentialities and difficulties in the sectors of autonomous vehicles, medicine and stock market, see: Túlio Xavier Januário, 'Veículos Autónomos e Imputação de Responsabilidades Criminais por Acidentes' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020) 95ff; Túlio Felippe Xavier Januário, 'Inteligência Artificial e Responsabilidade Penal no Setor da Medicina' (2021) 17(34) Lex Medicinae: Revista Portuguesa de Direito da Saúde 37 <https://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas> accessed 15 July 2021; Túlio Felippe Xavier Januário, 'Inteligência Artificial e Manipulação do Mercado de Capitais: uma Análise das Negociações Algorítmicas de Alta Frequência (High-Frequency Trading – HFT) à Luz do Ordenamento Jurídico Brasileiro' (2021) 29(186) Revista Brasileira de Ciências Criminais (forthcoming).

[31] For a broad analysis of possible evidentiary issues arising from artificial intelligence, see: Serena Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a - European Legal Discussion* (Springer 2020) 37ff; Sabine Gless, 'AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials' (2020) 51(2) Georgetown Journal of International Law 195, 202ff <https://ssrn.com/abstract=3602038> accessed 15 July 2021; Sónia Fidalgo, 'A Utilização de Inteligência Artificial no Âmbito da Prova Digital – Direitos Fundamentais (Ainda Mais) Desprotegidos' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020) 129ff. For a specific analysis on the digital chain of custody, see: Túlio Felippe Xavier Januário, 'Cadeia de Custódia da Prova e Investigações Internas Empresariais: Possibilidades, Exigibilidade e Consequências Processuais Penais de sua Violação' (2021) 7(2) Revista Brasileira de Direito Processual Penal 1453 <https://doi.org/10.22197/rbdpp.v7i2.453> accessed 12 October 2021.

[32] See: Danielle Kehl, Priscilla Guo, and Samuel Kessler, 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing' (2017) *Responsive Communities Initiative* <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041> accessed 15 July 2021; Vicent Chiao, 'Fairness, Accountability and Transparency: Notes on Algorithmic Decision-Making in Criminal Justice' (2019) 15 International Journal of Law in Context 126 <https://doi.org/10.1017/S1744552319000077> accessed 15 July 2021; Anabela Miranda Rodrigues, 'A Questão da Pena e a Decisão do Juiz – entre a Dogmática e o Algoritmo' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020) 230ff; Luís Greco, *Poder de Julgar sem Responsabilidade de Julgador: a Impossibilidade Jurídica do Juiz-Robô* (Marcial Pons 2020) 17ff.

outputs that may be prejudicial to them? And most importantly, is the output from these technologies really trustworthy?

4 Building a New Framework: Surpassing Data Bias and AI Ambiguities

4.1 Controlling information overload and false positives by autonomous decisions

Even in a country such as Brazil, where the banking sector is underexplored, there is an immense quantity of SARs to be audited. An operational example of this problem is presented by Jun Tang and Lishan Ai in China,[33] where a bank failed to comply with information duties until it was punished for the lack of reports.[34] On the very next 30 days, 1,700 SARs were reported. It seems that compliance programs end up being designed by banks to transfer or avoid responsibility, but not to effectively collaborate. The first mistake is to consider that the ineffectiveness of compliance programs in bank sectors is only their fault, even when they are complying with regulation.

To avoid an overly large number of false positives, information patterns must mature data before the report, which means that banks should check those transactions in a more complex system of conditions and characteristics. A great example was proposed by Zengan Gao and Mao Ye, who indicate that regulators should explore the decision tree and Bayesian inference systems, mixing different criteria to demonstrate how unusual, abnormal, or illegal a specific suspicious transaction might be.[35] Those data would be easily cross-checked by AI programs, which are already used to prevent credit frauds.

As previously presented in another paper, money laundering cannot be recognized by an isolated transaction.[36] It is important to take a step back and look at the big picture, just as in any other organized crime investigation. On banking reports, it is important to assess not only transactions but also people involved, economic activities informed, different groups linked and public profiles. To 'follow the money' is to investigate a complex chain of exchanges, not a simple line of transfers. In this sense, Zengan Gao and Mao Ye propose: a) to identify central members, subgroups and 'money laundering networks'; b) a case-based system of information (which can be elaborated with machine learning

[33] For a comprehensive study on money laundering control in China, see: Jing Lin, *Compliance and Money Laundering Control in China: Self Control, Administrative Control and Penal Control* (Duncker & Humblot 2016) 18ff.

[34] Jun Tang and Lishan Ai, 'The System Integration of Anti-Money Laundering Data Reporting and Customer Relationship Management in Commercial Banks' (2013) 16(3) Journal of Money Laundering Control 231, 232 <https://doi.org/10.1108/JMLC-04-2013-0010> accessed 13 July 2021.

[35] Zengan Gao and Mao Ye, 'A Framework for Data Mining-Based Anti-Money Laundering Research' (2007) 10(2) Journal of Money Laundering Control 170, 171 <http://www.emeraldinsight.com/1368-5201.htm> accessed 13 July 2021.

[36] Matheus de Alencar e Miranda and Leonardo Simões Agapito, 'Critérios de Validade e Eficiência de Compliance e Impactos na Interpretação da Lavagem de Dinheiro' in Eduardo Saad-Diniz, Luís Augusto Brodt, Henrique Abi-Ackel Torres and Luciano Santos Lopes (eds), *Direito Penal Econômico nas Ciências Criminais* (Vorto 2019) 241ff.

programs); c) a data mining technique that could sum 'customer, account, product, geography, and time' information by vectors analysis.[37]

As reported by Jun Tang and Lishan Ai, different mechanisms of data mining have been already applied by financial institutions to comprehend their clients, which are classified and evaluated for commercial and risk assessment proposes. Even home banking behaviors and smartphone apps and cookies are collected as market strategy. Banks knows their clients much more than what has been asked and profiles created should be better explored by the FIUs.[38]

However, that also means that national and international authorities of personal data protection would play a central role in the banking sector, whose institutions must be obliged to present their data mining programs without anonymization. At this point, a more collaborative framework between different authorities of personal data protection and companies (regulator-regulator and regulator-bank) becomes as important as the FIUs' reports.

4.2 Information bias: improving data analyses by human intervention

Changing informational standards might be very ineffective if the reports are not reliable. As demonstrated before, informational standards have been enforced and redesigned, creating new duties that were only able to change information volumes without impact on administrative or penal procedures. To improve data analysis, at least four measures are required, considering the need of a relationship of trust between *gatekeepers* and public auditors.

Taking Brazil as an example once again, the absence of instruments for whistleblowing protection is an important issue for a more collaborative regulatory framework. In this scenario, even the Personal Data Protection Law (13.709/18) failed to define a Data Protection Officer, whose duties accumulated in the same agents (controllers) responsible for creating and controlling those systems. It became the best scheme for private auditors and commerce of certifications by big companies. There is no need of an external auditor if a legal protection for *gatekeepers* exists and if developers and operators of data mining programs demonstrate good performance.

Besides that, international regulatory standards on money laundering prevention rely on an agency model, which has its function compromised by big companies' complexity and a lack of attention from consumers. Public interest is also captured by market's interests. To build a new regulatory framework, third parties' representatives, unions and NGOs should be better listened to. Popular participation is essential for accountability, a balance between regulators and *gatekeepers* and for a plural perspective of data efficiency. It also strengthens the informal social control, which can be aligned with formal

[37] Gao and Ye (n 35) 171.
[38] Tang and Ai (n 34) 232.

social control to counter undesired behavior more effectively. In this case, the undesired behavior is AI manipulation.

Database bias may also be intentionally designed in a way that things that are not informed (false negatives) might be audited by a more proactive performance of regulators. The simplest mechanism of verification is the inspection *in loco*, observed when a public agent has open access to corporate computers, physical files, and workers. The inspection might create some positive effects, such as the institutional 'materialization' and employees' collaboration. When a public agent visits a company, it is an opportunity to solve many questions regarding legal standards and official reports. Agent's reports may also reveal companies' innovations and red flags, creating a better perspective of companies changes through the years. Inspections *in loco* may also create a safe space for employees that intent to collaborate but feel insecure about official channels.

However, institutional 'materialization' also creates opportunities for illegal favors and can also be easily deflected by a reactive attitude and trained behaviors. In this scenario, those inspections could become expensive, with low effectiveness. A remote inspection (by digital platforms) could be cheaper and faster but might also be easily deflected by cosmetic compliance programs.

A second model of verification might occur through a sandbox experiment. Regulatory sandboxes are already used by monetary authorities and reserve banks to develop new ideas and to test business models.[39] A sandbox experiment allows companies to implement an idea for a limited period with special normative conditions. The project must be well demonstrated before its implementation and all the data produced are collected by agencies to understand its potentials, vulnerabilities and opportunities. Thus, it would be possible for FIUs to create sandboxes to validate (or not) institutional systems of surveillance, data mining, and even autonomous reports. This option is much cheaper than inspections and it provides more reliable information, since corporations would have a lot of interest in collaborating and receiving a FIU's certification.

If the present enforcement model works well, it is also possible that the data bias problem is eased, creating the best scenario for using AI. With good data (or avoiding data bias), many of the AI problems (as pointed in 3.3) may be solved. Other problems are usually addressed through upgrades in transparency, by making the AI's objectives public, by development documentation (with making business rules transparent and clear to users) and, eventually, the coding itself.

[39]As an example: Banco Central do Brasil, 'Sandbox Regulatório' <https://www.bcb.gov.br/estabilidade financeira/sandbox> accessed 13 July 2021. On the topic of regulatory sandboxes and their importance in the scope of new technologies, see: Susana Aires de Sousa, '"Não Fui Eu, Foi a Máquina": Teoria do Crime, Responsabilidade e Inteligência Artificial' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020) 86ff.

5 Conclusion

As demonstrated, the main issue of autonomous decisions in money-laundering surveillance is data bias created by an empty and insufficient regulatory framework. In addition to that, financial integration promoted by Basel Accords and FATF (top-down regulation) is responsible for similar regulatory struggles in different local economic realities, which means that those regulatory standards might have to be reviewed from FIUs' experiences (bottom-up regulation). These developments might emerge from institutional changes on FIUs, but also from new regulatory experiments.

However, the greatest challenge on autonomous decisions is still related to the question about how to promote the disclosure of autonomous decisions steps. The overcoming of data bias might guarantee a more reliable AI system, but not a more legitimate one. At this point, understanding that autonomous decisions have limitations and might demand human verification in this scope may be necessary. Satisfactory investigations and valid sanctions may never be conducted exclusively by autonomous systems. However, complex algorithms are able to assist human surveillance and to ensure security and anonymity of the data (both useful and useless). That being said, a well-developed system might legitimate itself through its efficiency results during previous tests and permanent monitoring.

References

Abel Souto M, 'Blanqueo, Innovaciones Tecnológicas, Amnistía Fiscal de 2012 y Reforma Penal' (2012) 14 Revista Electrónica de Ciencia Penal y Criminología 1 <http://criminet.ugr.es/recpc/14/recpc14-14.pdf> accessed 14 July 2021

Banco Central do Brasil, 'Sandbox Regulatório' <https://www.bcb.gov.br/estabilidadefinanceira/sandbox> accessed 13 July 2021

Basel Committee on Banking Supervision, 'International Convergence of Capital Measurement and Capital Standards (Basel Capital Accord I)' (1988)

Blanco Cordero I, El Delito de Blanqueo de Capitales (2nd edn, Aranzadi 2002)

Bottini PC, 'Aspectos Conceituais da Lavagem de Dinheiro' in Gustavo Henrique Badaró and Pierpaolo Cruz Bottini (eds), Lavagem de Dinheiro: Aspectos Penais e Processuais Penais: Comentários à Lei 9.613/98, com alterações da Lei 12.683/12 (4th edn, Thomson Reuters Brasil 2019)

Brandão N, Branqueamento de Capitais: O Sistema Comunitário de Prevenção (Coimbra Editora 2002)

Burrell J, 'How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data & Society 1 <https://doi.org/10.1177/2053951715622512> accessed 23 January 2020

Calo R, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51(2) UC Davis Law Review 399 <https://lawreview.law.ucdavis.edu/issues/archive.html> accessed 13 July 2021

Canestraro AC, 'Compartilhamento de Dados e Persecução do Crime de Branqueamento de Capitais no Âmbito dos Paraísos Financeiros' (2018) 22(35) Revista de Estudos Jurídicos Unesp 135 <https://doi.org/10.22171/rej.v22i35.2197> accessed 12 July 2021

—— 'Cooperação Internacional em Matéria de Lavagem de Dinheiro: da Importância do Auxílio Direto, dos Tratados Internacionais e os Mecanismos de Prevenção' (2019) 5(2) Revista Brasileira de Direito Processual Penal 623 <https://doi.org/10.22197/rbdpp.v5i2.234> accessed 12 July 2021

Chiao V, 'Fairness, Accountability and Transparency: Notes on Algorithmic Decision-Making in Criminal Justice' (2019) 15 International Journal of Law in Context 126 <https://doi.org/10.1017/S1744552319000077> accessed 15 July 2021

COAF, *Casos & Casos: I Coletânea de Casos Brasileiros de Lavagem de Dinheiro: Edição Comemorativa pelos 10 Anos do Conselho de Controle de Atividades Financeiras* (COAF 2011)

Comissão de Valores Mobiliários, 'Instrução CVM n.617, de 5 de dezembro de 2019' <http://conteudo.cvm.gov.br/legislacao/instrucoes/inst617.html> accessed 13 July 2021

Coffee Jr JC., 'Understanding Enron: It's About the Gatekeepers, Stupid' (2002) 207 Columbia Law School Working Paper 1 <https://dx.doi.org/10.2139/ssrn.325240> accessed 14 July 2021

—— 'The Attorney as Gatekeeper: An Agenda for the SEC' (2003) 103(5) Columbia Law Review 1293 <https://doi.org/10.2307/1123838> accessed 14 July 2021

Coimbra MA and Manzi VA, *Manual de Compliance* (Atlas 2010)

European Commission, 'Communication From the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions (Artificial Intelligence for Europe)' COM(2018) 237 final

Fidalgo S, 'A Utilização de Inteligência Artificial no Âmbito da Prova Digital – Direitos Fundamentais (Ainda Mais) Desprotegidos' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020)

Gao Z and Ye M, 'A Framework For Data Mining-Based Anti-Money Laudering Research' (2007) 10(2) Journal of Money Laundering Control 170 <http://www.emerald insight.com/1368-5201.htm> accessed 13 July 2021

Gless S, 'AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials' (2020) 51(2) Georgetown Journal of International Law 195 <https://ssrn.com/abstract=3602038> accessed 15 July 2021

Greco L, *Poder de Julgar sem Responsabilidade de Julgador: a Impossibilidade Jurídica do Juiz-Robô* (Marcial Pons 2020)

Hilgendorf E, 'Recht und autonome Maschinen – ein Problemaufriβ' in Eric Hilgendorf and Sven Hötitzsch (eds), *Das Recht vor den Herausforderungen der modernen Technik* (Nomos 2015)

Januário TFX, 'Veículos Autónomos e Imputação de Responsabilidades Criminais por Acidentes' in Anabela Miranda Rodrigues (ed*), A Inteligência Artificial no Direito Penal* (Almedina 2020)

—— 'Inteligência Artificial e Responsabilidade Penal no Setor da Medicina' (2021) 17(34) Lex Medicinae: Revista Portuguesa de Direito da Saúde 37 <https://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas> accessed 15 July 2021

—— 'Cadeia de Custódia da Prova e Investigações Internas Empresariais: Possibilidades, Exigibilidade e Consequências Processuais Penais de sua Violação' (2021) 7(2) Revista Brasileira de Direito Processual Penal 1453 <https://doi.org/10.22197/rbdpp.v7i2.453> accessed 12 October 2021

—— 'Considerações Preambulares Acerca das Reverberações da Inteligência Artificial no Direito Penal' in Murilo Siqueira Comério and Tainá Aguiar Junquilho (eds), *Direito e Tecnologia: um debate multidisciplinar* (Lumen Juris 2021)

—— 'Inteligência Artificial e Manipulação do Mercado de Capitais: uma Análise das Negociações Algorítmicas de Alta Frequência (High-Frequency Trading – HFT) à Luz do Ordenamento Jurídico Brasileiro' (2021) 29(186) Revista Brasileira de Ciências Criminais (forthcoming)

Kehl D, Guo P and Kessler S, 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing' (2017) *Responsive Communities Initiative* <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041> accessed 15 July 2021

Lin J, *Compliance and Money Laundering Control in China: Self Control, Administrative Control and Penal Control* (Duncker & Humblot 2016)

Maillart JB, 'Anti-Money Laundering Architectures: Between Structural Homogeneity and Functional Diversity' in Benjamin Vogel and Jean-Baptiste Maillart (eds), *National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection* (Intersentia 2020)

Manzi VA, *Compliance no Brasil: consolidação e perspectivas* (Saint Paul 2008)

Miranda MA and Agapito LS, 'Critérios de Validade e Eficiência de Compliance e Impactos na Interpretação da Lavagem de Dinheiro' in Eduardo Saad-Diniz, Luís Augusto Brodt, Henrique Abi-Ackel Torres and Luciano Santos Lopes (eds), *Direito Penal Econômico nas Ciências Criminais* (Vorto 2019)

Mulholland C and Frajhof IZ, 'Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: Breves Anotações Sobre o Direito à Explicação Perante a Tomada de Decisões por Meio de Machine Learning' in Ana Frazão and Caitlin Mulholland (eds), *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade* (Thomson Reuters Brasil 2019)

Oliveira ACC, *Lavagem de dinheiro: responsabilidade pela omissão de informações* (Tirant lo Blanch 2019)

Oliveira JC, Agapito LS and Alencar M, 'O Modelo de "Autorregulação Regulada" e a Teoria da Captura: Obstáculos à Efetividade no Combate à Lavagem de Dinheiro no Brasil' (2017) 10 Quaestio Iuris 365 <https://doi.org/10.12957/rqi.2017.26847> accessed 14 July 2021

Peixoto FH and Silva RZM, *Inteligência Artificial e Direito* (Alteridade Editora 2019)

Price II WN, 'Artificial Intelligence in Health Care: Applications and Legal Issues' (2017) 599 U of Michigan Public Law Research Paper 1 <https://ssrn.com/abstract=3078704> accessed 23 January 2020

Quattrocolo S, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion* (Springer 2020)

Rodrigues AM, 'A Questão da Pena e a Decisão do Juiz – entre a Dogmática e o Algoritmo' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020)

—— 'Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020)

Saad-Diniz E, 'Fronteras del Normativismo: a Ejemplo de las Funciones de la Información en los Programas de Criminal Compliance' (2013) 108 Revista da Faculdade de Direito da Universidade de São Paulo 415

Santosuosso A and Bottalico B, 'Autonomous Systems and the Law: Why Intelligence Matters' in Eric Hilgendorf and Uwe Seidel (eds) *Robotics and the Law: Legal Issues Arising from Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy* (Nomos 2017)

Sousa SA, '"Não Fui Eu, Foi a Máquina": Teoria do Crime, Responsabilidade e Inteligência Artificial' in Anabela Miranda Rodrigues (ed), *A Inteligência Artificial no Direito Penal* (Almedina 2020)

Tang J and Ai L, 'The System Integration of Anti-Money Laundering Data Reporting and Customer Relationship Management in Commercial Banks' (2013) 16(3) Journal of Money Laundering Control 231 <https://doi.org/10.1108/JMLC-04-2013-0010> accessed 13 July 2021

Vogel B, 'Introduction' in Benjamin Vogel and Jean-Baptiste Maillart (eds), National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulation and Data Protection (Intersentia 2020)

Went P, 'Basel III Accord: Where Do We Go From Here?' (2010) <https://dx.doi.org/10.2139/ssrn.1693622> accessed 13 July 2021

Wimmer M, 'Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios' in Ana Paula M. Canto de Lima, Carmina Bezerra Hissa and Paloma Mendes Saldanha (eds), *Direito Digital: Debates Contemporâneos* (Thomson Reuters Brasil 2019)

Yapo A and Weiss J, 'Ethical Implications of Bias in Machine Learning' [2018] Proceedings of the 51st Hawaii International Conference on System Sciences 5365