Corporate Internal Investigations 4.0: on the criminal procedural aspects of applying artificial intelligence in the reactive corporate compliance[1]

Investigações internas corporativas 4.0: sobre os aspectos processuais penais da aplicação da inteligência artificial no âmbito reativo do compliance

Túlio Felippe Xavier Januário[2]

Universidade de Coimbra, Coimbra, Portugal

tuliofxj@gmail.com

http://orcid.org/0000-0003-0400-1273

Abstract: The aim of the present paper is to analyze the criminal procedural implications of applying artificial intelligence systems in the context of internal investigations. More specifically, we will seek to answer the following questions: how can AI be used in these procedures and which are its legal boundaries? In case of effective use of this technology, how can it, in a future criminal proceeding, affect the admissibility and valuation of elements of information derived from internal investigations? In order to address these questions, we will apply

---

2   PhD Candidate in Law at the University of Coimbra (Portugal), with a fellowship from the Fundação para a Ciência e a Tecnologia – FCT. M.Sc. in Law by the University of Coimbra (Portugal), with a research internship of the "ERASMUS+" Program at the Georg-August-Universität Göttingen (Germany). He had Graduate Studies in International Criminal Law at the Siracusa International Institute for Criminal Justice and Human Rights (Italy), Graduate Studies in Economic Criminal Law and Crime's Theory at the University of Castilla-La Mancha (Spain), Graduate Studies in Compliance and Criminal Law at IDPEE (Portugal) and Graduate Studies in Criminal Law – General Part at IBCCRIM/IDPEE (Brazil/Portugal). He holds a Bachelor´s Degree in Law by the Universidade Estadual Paulista – UNESP (Brazil).

the deductive methodology with a review of European and Brazilian legislation, doctrine and jurisprudence. At the end of the paper, we will demonstrate the limits to be observed for the processing of data and the use of AI in the scope of internal investigations, as well as the requirements and limits of sharing the information obtained from them with criminal proceedings.

Keywords: Corporate criminal law; compliance; internal investigations; artificial intelligence; criminal procedure.

Resumo: *O objetivo do presente trabalho é analisar as implicações processuais penais da aplicação de sistemas de inteligência artificial em investigações internas. Mais especificamente, buscaremos responder aos seguintes questionamentos: como a IA pode ser utilizada nesses procedimentos e quais são suas limitações legais? Em caso de efetivo uso dessa tecnologia, como ela pode afetar a admissibilidade e valoração de elementos de informação derivados de investigações internas, em um futuro processo penal? Para responder a estas questões, aplicaremos a metodologia dedutiva, com análise da legislação, doutrina e jurisprudência europeia e brasileira. Ao final do artigo, demonstraremos os limites a serem observados no processamento de dados e uso da IA no âmbito das investigações internas, assim como os requisitos e limites para o compartilhamento das informações obtidas a partir delas, com processos penais.*

Palavras-chave: *direito penal empresarial; compliance; investigações internas; inteligência artificial; processo penal.*

Introduction

Among the various mechanisms for preventing and tackling economic and business crimes, one of those that has become the object of greater legislative, jurisprudential and, mainly, doctrinal attention is certainly the compliance programs. More recently, these mechanisms, as well as several other sectors of society, have experienced the influxes of the so-called "*Revolution 4.0*"[3], since their most diverse activities have been

---

3   The use of the term "*revolution 4.0*", which we also refer to in the title, is attributed here to Barona Villar, who explains that scientific and technological

carried out with the aid of new technologies, among which autonomous systems and artificial intelligence (henceforth, AI)⁴.

---

advances, especially at the end of the 20th and the beginning of the 21st century, opened space for a new stage of industrialization, in which digitalization, connectivity, automation, robotization and artificial intelligence are combined. It is precisely this new stage that is known as Industry 4.0. According to the author, this expression was used for the first time by Henning Kagermann, president of Acatech, at the 2011 Hannover Messe. See: BARONA VILAR, Silvia. *Algoritmización del derecho y de la justicia:* de la inteligencia artificial a la Smart Justice. Valencia: Tirant lo Blanch, 2021. p. 58. In this sense: "The term "Industrie 4.0" was introduced in 2011 by the Communication Promoters Group of the Industry-Science Research Alliance to describe the widespread integration of information and communication technology in industrial production. The "4.0" alludes to how this trend's potentially revolutionary impact follows directly in the footsteps of the three previous industrial revolutions" (SCHUH, Günther et al (eds.). *Industrie 4.0 Maturity Index:* Managing the Digital Transformation of Companies: Update 2020. München: Acatech Study, 2020. p. 11).

[4] As explained by Matheus de Alencar e Miranda, (1*) technologies of automated decision are the genus*, of which (1.1) *systems/algorithms of autonomous pre-programmed decision* and (1.2) *artificial intelligence* are species. The distinction between the two species lies in the fact that in *artificial intelligence systems*, there is no human rule that determines how the algorithm decides. Human decisions are limited to defining the objective and form of learning. The algorithm, in turn, has the ability to understand the environment through data inputs and choose, among several possible courses of action, one that solves the posed problem. In turn, although systems of autonomous pre-programmed decisions can react to the environment without the need for human input at that moment of decision, they are unable to learn or create their own solution to that problem and to modify their codes. Their behavior, therefore, is a pre-programmed reaction to the posed problem. See in detail at: MIRANDA, Matheus de Alencar e. *Técnica, decisões automatizadas e responsabilidade penal*. 2023. Tese - (Doutorado em Direito). Rio de Janeiro: Universidade do Estado do Rio de Janeiro, 2023. p. 74-94. For an analysis of the difficulties in differentiating these concepts, see also: AGAPITO, Leonardo Simões; MIRANDA, Matheus de Alencar e; JANUÁRIO, Túlio Felippe Xavier. On the Potentialities and Limitations of Autonomous Systems in Money Laundering Control. *RIDP*, v. 92, n. 1, p. 87-108, 2021. p. 89ff.; SANTOSUOSSO, Amedeo; BOTTALICO, Barbara. Autonomous Systems and the Law: Why Intelligence Matters. In: HILGENDORF, Eric; SEIDEL, Uwe (eds.). *Robotics and the Law*: Legal Issues Arising from Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy. Baden-Baden: Nomos, 2017. p. 27-58. p. 35ff; HILGENDORF, Eric. Recht und autonome Maschinen – ein Problemaufriβ. In: HILGENDORF, Eric; HÖTITZSCH, Sven (eds.). *Das Recht vor den Herausforderungen der modernen Technik*. Baden-Baden: Nomos 2015. p. 11-40.

It is true, however, that despite their undeniable potential to make compliance activities more effective and efficient, the use of these technologies also raises some relevant doubts, especially if we consider some of their inherent limitations, such as the opacity of their operation and unpredictability of their outputs. Furthermore, their specific use in compliance programs, especially in their most repressive aspect, which is conducting corporate internal investigations (henceforth, CII), raises serious questions in terms of the rights and guarantees of those being investigated, which is even more serious if we consider that, although is not their exclusive purpose, they can investigate facts that constitute crimes and, consequently, be relevant in future criminal proceedings.

In view of this scenario, the central object of this investigation focuses precisely on the use of AI in the scope of CII and its criminal procedural repercussions. In other words, we will seek to answer the following questions: how has AI been and can be applied in CII and what are the legal limits for its use? In case of application, how can it affect the admissibility and valuation of the information collected in these investigations in any criminal proceedings?

To elucidate these questions, we will initially analyze the concept, operation and limitations of AI systems in order to understand not only their potentials, but also the risks generated by their use in the scope of CII. These procedures will also be the object of our attention in this topic. Through the analysis of their fundamental concepts in the light of doctrine, legislation and jurisprudence, we will seek to understand their relevance, functioning and possible criminally relevant implications.

Finally, we will focus on the main question of the present study, analyzing the legal guidelines for the use of AI in the scope of CII and for the sharing of information with the criminal procedures. In this context, based on a deductive methodology and with the analysis of Brazilian and European legislation, doctrine and jurisprudence, we will investigate three main aspects: the legal guidelines for processing data in CII; the limits to the use of AI systems in these procedures; and the requirements and limits for sharing the information elements derived from them, with an eventual criminal proceeding.

At the end of the investigation, we will seek to demonstrate that the processing of data for the purpose of applying AI in CII does not find obstacles

in the Brazilian General Data Protection Law (LGPD) or in the European General Data Protection Regulation (GDPR), provided that it is based on at least one of the legal hypotheses and respects the test of proportionality between the intended purpose and the means employed to achieve it. We will also demonstrate that, although based on the directive power of the employer, the use of AI systems in this scope is not unlimited either, and must observe, among other barriers, those imposed by the legality, the expectation of privacy of employees and by a second proportionality test. Finally, we will conclude that these elements of information can be shared with the criminal procedure provided that a third proportionality test is respected and that it is observed that they can never be considered sufficient to justify the conviction of any defendant, having a regime similar to that of the elements of information coming from public acts of investigation.

1. BLACK-BOXES 2.0: ARTIFICIAL INTELLIGENCE AND THE "NEW" FACE OF CORPORATE INTERNAL INVESTIGATIONS

Although recent attention has been paid to problems related to AI, driven especially by technological advances in this scope, it is important to mention that this field of study dates back to the post-World War II period, largely made possible by the work of Alan Turing focused on decoding messages during the war[5]. However, the use of this terminology is attributed to John McCarthy in the context of the text "*A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence",* of 1955. At the time, the author considered it as "the science and engineering of making intelligent machines, especially intelligent computer programs". Besides, "it is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable"[6].

---

[5] SHABBIR, Jahanzaib; ANWER, Tarique. Artificial intelligence and its role in near future. *Journal of Latex Class Files*, v. 14, n. 8, p. 1-11, Aug./2015, p. 3; PEIXOTO, Fabiano Hartmann; SILVA, Roberta Zumblick Martins. *Inteligência artificial e direito*, Curitiba: Alteridade Editora, 2019, p. 24.

[6] MCCARTHY, John. *What is Artificial Intelligence?*. Stanford: Stanford University, 2007; MCCARTHY, John et al. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine*, v.

Currently, a proposal of definition that seems more appropriate to the state of the art of the matter is presented by the *European Commission's High-Level Expert Group on Artificial Intelligence*, which proposes a subdivision into two categories: by i) *artificial intelligence as systems,* we can understand software or hardware that, given a complex goal, acts in the physical or digital world by perceiving their environment, interpreting the collected data, reasoning on this data and deciding the best action(s) to take, according to pre-defined parameters. Moreover, they can also be designed to learn to adapt their behavior by analyzing how the environment is affected by their previous actions. In turn, when considered an *ii) scientific discipline*, AI includes several approaches and techniques, such as machine learning, machine reasoning and robotics, integrating them in cyber-physical systems[7].

Scientific and technological advances in the area of AI have been accompanied by an undeniable expansion of the application of this technology in various fields of activities, such as transports, medicine and the capital market. It is no different with the scope of criminal justice, where autonomous and AI systems have been increasingly applied in activities of surveillance, investigation, judgment and sentence serving[8].

27, n. 4, p. 12-14, 2006, p. 14. See also: JANUÁRIO, Túlio Felippe Xavier. Vulnerabilidad e hiposuficiencia 4.0: la protección jurídico-penal de los consumidores en la era de la inteligencia artificial. In: FONTESTAD PORTALÉS, Leticia (dir.), PÉREZ TORTOSA, Francesc. (coord.). *La justicia en la sociedad 4.0*: nuevos retos para el siglo XXI. A Coruña: Editorial Colex, 2023. p. 187-199, p. 189.

[7] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE: *A Definition of AI: Main Capabilities and Scientific Disciplines: Definition Developed for the Purpose of the Deliverables of the High-Level Expert Group*, Brussels, 2018, p. 7. See also: See also: JANUÁRIO, Túlio Felippe Xavier. Vulnerabilidad e hiposuficiencia..., p. 189.

[8] For a broad analysis, see: AGAPITO, Leonardo Simões; MIRANDA, Matheus de Alencar e; JANUÁRIO, Túlio Felippe Xavier. Underneath the Robot Judge's Robe: demystifying the use of artificial intelligence in criminal justice through a global south perspective. In: KOSTIĆ, Jelena; BOŠKOVIĆ, Marina Matić. *Digitalizacija u kaznenom pravu i pravosudu*: Digitalization in Penal Law and Judiciary. Belgrade: IKSI, 2022. p. 271-289. p. 272ff.; QUATTROCOLO, Serena. *Artificial Intelligence, Computational Modelling and Criminal Proceedings*: A Framework for a European Legal Discussion. Cham: Springer Nature Switzerland AG, 2020. p. 37ff.; GLESS, Sabine. AI in the Courtroom:

Our object of study, however, refers to the application of AI in the most varied activities carried out within the scope of compliance programs[9]-[10], especially with regard to their reactive scope, that is, the

---

A Comparative Analysis of Machine Evidence in Criminal Trials. *Georgetown Journal of International Law,* v. 51, n. 2, p. 195-253, 2020. p. 202ff.

[9] Compliance programs can be understood as instruments of self-supervision and self-regulation inserted in the context of corporate governance, whose immediate purposes are the promotion of a culture of ethics and legal compliance in business activities and the prevention, investigation and repression of illegal practices within the corporate sphere. By its turn, their mediate aims are to maintain or recover the good reputation of the legal person, to secure the continuity of the business with potential profits and, mainly, to protect the corporation, its collaborators and representatives, from eventual liabilities in the most varied spheres, as well as from financial and reputational losses. JANUÁRIO, Túlio Felipe Xavier. *Criminal compliance e corrupção desportiva*: um estudo com base nos ordenamentos jurídicos do Brasil e de Portugal. Rio de Janeiro: Lumen Juris, 2019, p. 85-86. As Silva Sánchez explains, compliance programs cannot be exhausted in the mere adoption of self-surveillance mechanisms, but must also encompass positive training measures that seek to neutralize cultural factors and group dynamics that favor criminality. See in detail: SILVA SÁNCHEZ, Jesús María. *Fundamentos del derecho penal de la empresa.* Madrid: Edisofer, 2013. p. 193. The relationship between self-regulation and corporate governance is well approached by Cláudia Barrilari, who recalls that the latter has its origins in the UK and the US in the 1990s, configuring itself as commercial practices and rules that aim precisely to overcome the conflicts inaugurated with the split between the management of controllers, on the one hand, and ownership by the companies' shareholders, as well as the interests of creditors, on the other. Great influence on these concepts was exerted by the scandals of fraud and market manipulation that were publicized at this time, as well as the approval of the Sarbanes-Oxley Act. See with more details at: BARRILARI, Claudia Cristina. *Crime empresarial, autorregulação e compliance.* 2. ed. atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021. Ebook. N.P. Section 3.4.3. See also: LUZ, Ilana Martins. *Compliance & omissão imprópria.* 3. Reimp. Belo Horizonte: D'Plácido, 2021. p. 30ff.

[10] "Primitive" versions of compliance programs already existed in the US in the 1930s and 1940s, especially after SEC and DOJ impositions. However, it was after the disclosure of the *Watergate* scandal in the 1970s and the subsequent approval of the *US Sentencing Guidelines* of 1991, and especially with the financial scandals at the turn of the millennium (such as Enron, WorldCom and Parmalat), that these programs became a real asset in the attempt to overcome state difficulties in regulating, preventing, investigating and repressing corporate crimes. On the origins and historical evolution of compliance programs, see: NIETO MARTÍN, Adán. El cumplimiento normativo. In: NIETO MARTÍN, Adán et al. (dir.). *Manual de cumplimiento penal en*

conduction of CII[11]-[12]. As Christoph Burchard rightly points out, the

la empresa. Valencia: Tirant lo Blanch, 2015. p. 25-48. p. 27ff; SAAD-DINIZ, Eduardo. Ética negocial e _compliance:_ entre a educação executiva e a interpretação judicial. São Paulo: Thomson Reuters Brasil, 2019. p. 125ff. Regarding Brazil, even though compliance programs already existed in the 1990s, it was in the first two decades of the 21st century that they became the object of real expansion within companies and the focus of national doctrine. The reasons for this, according to Saavedra, lie in: i) the compliance duties inserted in the Brazilian legal system by Law 12,683/12, which modified the Anti-Money Laundering Law (Law 9,613/98); ii) the debate instigated by APn 470 (popularly known as "mensalão") on the criminal responsibility of compliance officers; and iii) the approval of the Anti-Corruption Law (12,846/13), which provides for express positive impacts in administrative penalties imposed on companies when adopting these programs. SAAVEDRA, Giovani Agostini. Panorama do compliance no Brasil: avanços e novidades. In: NOHARA, Irene Patrícia; PEREIRA, Flávio de Leão Bastos (coord.). _Governança, compliance e cidadania._ São Paulo: Thomson Reuters Brasil, 2018. p. 37-50. p. 37-38. See also: BOTTINI, Pierpaolo Cruz. Programas de compliance voltados à prevenção da lavagem de dinheiro. In: BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. _Lavagem de dinheiro:_ aspectos penais e processuais penais: comentários à Lei 9.613/1998, com alterações da Lei 12.683/2012. 4.ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 47-71; CARDOSO, Débora Motta. _Criminal compliance na perspectiva da lei de lavagem de dinheiro._ São Paulo: LiberArs, 2015. p. 125ff.

[11] We have had the opportunity to partially address this topic on other occasions. The present paper is intended to bring a theoretical deepening in some its fundamental aspects. See also: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felipe Xavier. Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal. In: D'ÁVILA, Fábio Roberto; AMARAL, Maria Eduarda Azambuja (eds.). _Direito e Tecnologia._ Porto Alegre: Citadel, 2022. p. 363-392; JANUÁRIO, Túlio Felipe Xavier. Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales. _Estudios Penales y Criminológicos_, Santiago de Compostela, forthcoming.

[12] It is important to emphasize that there is no single pre-defined model of compliance program, since it undeniably depends on the particularities of the corporation and its sector of activity (in that sense, see: RODRIGUES, Anabela Miranda. _Direito penal económico:_ uma política criminal na era compliance. 2.ed. Coimbra: Almedina, 2020. p. 102; SIEBER, Ulrich. Compliance-Programme im Unternehmensstrafrecht: ein neues Konzept zur Kontrolle von Wirtschaftskriminalität. In: SIEBER, Ulrich et al. (Hrsg.). _Strafrecht und Wirtschaftsstrafrecht – Dogmatik, Rechtsvergleich, Rechtstatsachen_: Festschrift für Klaus Tiedemann zum 70. Geburtstag. Köln: Carl Heymanns Verlag, 2008. p. 449-484. p. 458). For illustrative purposes, we can cite the model proposed by Marc Engelhart, who classifies its stages of elaboration

time when only state agents made use of predictive systems to detect and prevent crimes is gone. On the contrary, *digital criminal compliance* (DCC) can be considered the buzzwords when it comes to employing digital systems for real-time prevention of compliance violations[13].

Depending on the complexity of the case and the companies involved and their respective scopes of activity, CII tend to be proportionally complex, with a high expenditure of time and human and financial resources of the corporation, for the purpose of properly ascertaining the facts in question. For this reason, technological instruments capable of assisting in certain tasks that demand the processing of an immense amount of data in a short time, especially with accuracy superior to that of humans, have been increasingly sought after.

When talking about the digitization of criminal compliance, it refers to the intelligent analysis of a large data set (big data), especially through AI, in order to ensure compliance with laws and prevention of

---

into three columns, namely: i) the *formulation*, characterized by the trinomial "detect-define-structure", which includes risk management, approval of a code of ethics and conducts, the implementation of a whistleblowing channel and the definition of the respective competences within the scope of the program; ii) the *implementation*, marked by the trinomial "communicate-promote-organize", which includes the program dissemination and personnel training phases, as well as the daily promotion of the culture of compliance; and iii) *consolidation and improvement*, marked by the trinomial "react – sanction – improve", and which encompasses CII and sanctioning procedures, as well as the evaluation mechanisms and continuous improvement of the program. See: ENGELHART, Marc. *Sanktionierung von Unternehmen und Compliance*: eine rechtsvergleichende Analyse des Straf- und Ordnungswidrigkeitenrechts in Deutschland und den USA. 2. ergänzte und erweiterte Auflage. Berlin: Dunker & Humblot, 2012. p. 711-719. Also based on this classification: JANUÁRIO, Túlio Felippe Xavier. *Criminal compliance e...*, p. 90ff; VERÍSSIMO, Carla. *Compliance:* incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva: 2017, p. 271ff.; GARCÍA CAVERO, Percy. *Criminal compliance.* Lima: Palestra Editores, 2014, p. 27ff; RODRIGUES, Anabela Miranda. *Direito penal económico...*, p. 102ff.

13 BURCHARD, Christoph. Das »Strafrecht« der Prädiktionsgesellschaft: ...oder wie »smarte« Algorithmen die Strafrechtspflege verändern (könnten). *Forschung Frankfurt: das Wissenschaftsmagazin: Recht und Gesetz*, n. 1, p. 27-31, Aug./2020, p. 28. See also: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 369.

crimes within companies[14]. The reasons for this option lie precisely in the pretension of greater effectiveness and efficiency of the compliance program and, consequently, greater security for the company, since more advanced computer systems are able to predict with high accuracy the actions and productive processes, as well as to prevent and detect situations that may be harmful to the corporation[15].

According to Burchard, digital criminal compliance presents the promise (not necessarily fulfilled) of being a more complete, objective, neutral and effective form of compliance. The author explains that one of the main limitations of traditional (human-based) compliance is the fact that it is often forced to operate retrospectively (ex post). This occurs precisely due to human limitations and errors and despite the prior existence (ex ante) of data on possible non-compliance. Furthermore, despite the need to contain corporate crimes, companies are always faced with the dilemma that compliance measures tend to paralyze the company. With the digitalization of the compliance structure and the ability of new technologies to analyze big data in real time, the expectation is to predict a large number of possible infractions, preventing their occurrences. Furthermore, even if they are not avoided in some cases, the data storage capacity of AI systems would certainly favor the ex post investigation of the facts[16].

In view of these ambitions, it is important to point out that some functionalities of compliance programs already experience the benefits of digitalization and some new technologies. This is the case, for example, of the digitalization of whistleblowing and guidance channels and the portals of training and clarification of doubts of the employees. Furthermore, employee training itself can be favored by technological tools, which

---

[14] BURCHARD, Christoph. Digital Criminal Compliance. In: ENGELHART, Marc et al (Hrsg.). *Digitalisierung, Globalisierung und Risikoprävention:* Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II. Berlin: Duncker & Humblot, 2021. p. 741-756. p. 742.

[15] RODRIGUES, Anabela Miranda; SOUSA, Susana Aires de. Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal. In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal,* vol. II. Coimbra: Almedina, 2022. p. 11-39. p. 13.

[16] BURCHARD, Christoph. Digital Criminal Compliance..., p. 744-747.

can be used to clarify doubts about concrete and specific situations, especially those that can be easily solved in light of the company's code of ethics[17]. With the consequent reduction in the demand for services, the competent department is able to dedicate itself to the resolution of more delicate cases, which cannot be solved by the system[18].

In addition, activities that demand the processing of a huge amount of data in a short time tend to be especially benefited. This is the case, for example, of the analysis of the legal and regulatory aspects applicable to a given situation, especially if we consider that companies have been increasingly subjected to an immensity of legislation, including international ones, due to their activities in different markets. In this sense, tools that assist in the automated processing of data and categorization of those that are relevant in the specific case tend to benefit not only the compliance sector, but the generality of the company's legal activities. Dedicating itself to the study of the applications of these technologies in the legal field, we have *legal tech* (or *law tech*), which refers precisely to the use of new technologies (from the simplest ones, such as those used

---

[17] Cornelia Inderst draws attention to the importance of training using technology when the company is large, especially with dispersed and global operations. This increases the possibility of standardizing behavior standards in all branches, as well as control over the effective implementation of training programs. See in detail at: INDERST, Cornelia. Einzelaufgaben der Compliance-Organisation. In: GÖRLING, Helmut et al. *Compliance:* Aufbau – Management – Risikobereiche. Hamburg: C.F. Müller, 2010. p. 112-122. p. 115.

[18] It is important to mention, however, that despite its possible benefits, the digitization of reporting and helping channels must also be subject to some reservations. To what extent, for example, would AI be able to more effectively ensure the confidentiality of denounces and whistleblowers? As we suggested on another occasion, if on the one hand it is a fact that the reduction of human contacts with sensitive information could open up fewer gaps for possible undue leaks and possible reprisals and embarrassment to those involved, on the other hand, we must ask ourselves about the level of security of these channels and also who would have access to data and what would be the destination given to them, after processing. Furthermore, it is questionable to what extent the reduction of human contacts is beneficial in these situations. We have doubts about whether machine assistance in these cases, which are often delicate, could not end up representing a "dehumanization" of care for victims, who may feel helpless and disrespected at these times. See more details at: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 370-371.

in data storage, security or in office administrative services, up to the most modern ones, which help or even replace lawyers in some tasks) for the simplification and enhancement of legal services[19].

Also in this sense, the identification, monitoring and analysis of risks – activities that we will include here within the scope of so-called *risk assessment* – are positively impacted by the aforementioned data processing capacity. As if that were not enough, algorithms that are capable not only of a mere risk categorization, but also effectively able of autonomously update themselves with their previous experiences and the most recent scientific knowledge, legal updates and jurisprudence, certainly add to the program's efficiency[20].

Within the scope of due diligence activities[21], there are already tools on the market that assist in the collection of information regarding third parties, merger or acquisition target companies and any other agents, which the company wishes to do business with, identifying the viability, risks and transaction values. The benefits of using AI in this scope are once again in its high data processing capacity and its high accuracy, which helps in the preparation of a very precise and informative final report[22].

These are, however, some less controversial features of AI within compliance programs. Larger issues arise from its application when

---

[19] See: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 371; CORRALES, Marcelo; FENWICK, Mark; HAAPIO, Helena. Digital Technologies, Legal Design and the Future of the Legal Profession. In: CORRALES, Marcelo; FENWICK, Mark; HAAPIO, Helena (ed.). *Legal Tech, Smart Contracts and Blockchain*. Singapore: Springer, 2019. p. 1-16.

[20] CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 372.

[21] On the difficulties of conducting due diligence procedures, especially in transnational contexts, see: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Beyond Ecocide: Extraterritorial Obligations of Due Diligence as an Alternative to Address Transnational Environmental Damages?. *RIDP*, v. 93, n. 1, p. 231-250, 2022.

[22] As an example, see the following tools already available on the market: RELATIVITY. *One platform for all your legal & compliance needs*; NEOWAY COMPLIANCE. *Diligência prévia completa e gestão de compliance para análise e prevenção de riscos*; UPLEXIS. *Atualize seu processo de tomada de decisão*. For a more detailed analysis, see: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 372.

monitoring and supervising the work environment and tools, as well as the workers themselves. Furthermore, its capabilities can also be used in the measures of CII themselves, whether merely because of the immense amount of data it can store and which may be of interest for fact-finding, or because of its potential to effectively assist in conducting interviews, analyzing data and making decisions and predictions.

In order to better understand how new technologies such as AI can be employed in CII, we first need to understand what these procedures are. CII can be considered a set of procedures conducted within a given company, with or without the help of external professionals, with the aim of investigating facts showing signs of legal, ethical or bylaw violations that come to its knowledge. They cannot be confused with day-to-day supervisory activities, or with due diligence procedures, since they have a reactive and non-day-to-day nature[23].

Even if not considered *legally obliged* to do so, companies have a *burden* of investigating[24] the facts that occurred within their scope,

---

[23] CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe X. Investigação defensiva corporativa: um estudo do Provimento 188/2018 e de sua eventual aplicação para as investigações internas de pessoas jurídicas. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 6, n. 1, p. 283-328, jan./abr. 2020, p. 294.

[24] In a different sense, Leon Alapont considers that, in light of the Spanish legal system, there is an unavoidable obligation to conduct CII when the company is aware of possible risks and compliance violations. See: LEÓN ALAPONT, José. *Canales de denuncia e investigaciones internas en el marco del compliance penal corporativo.* Valencia: Tirant lo Blanch, 2023. p. 341. We dare to disagree with this position. Although we recognize that the failure to conduct this procedure may be a considered negative aspect, in a specific case, within the scope of the judgment on the effectiveness of the compliance program for the purpose of obtaining a certain criminal procedural benefit (in this case, exemption from criminal liability of the person legal), we did not identify in Art. 31, bis, 5, 4th, of the Spanish Penal Code, an *obligation* to conduct them, precisely because it will depend on the judge, in the concrete case, to assess when the legal entity made the sufficient and necessary efforts to ascertain the facts. In some hypotheses, when the facts are evident, it will often not be necessary to conduct a CII itself, without this absence implying a failure in the compliance program. Think, for example, of cases in which a certain employee is "caught" attacking or harassing a colleague or third party, or committing some other offense that does not require further investigation. In these cases, internal measures (sanctions, dismissal) and external measures (notification of the authorities) can be taken without initiating a proper internal investigation procedure.

since not doing it may end up calling into question the adequacy and effectiveness[25] of their compliance programs and, consequently, affecting possible procedural benefits derived from them, such as non-prosecution agreements, penalty reductions or even the exclusion of corporate criminal liability[26]-[27].

---

[25] As highlighted by Adán Nieto Martín, the effectiveness of a compliance program can be assessed in two different ways, depending on its purpose. The *retrospective valuation* analyzes the effectiveness of the program in relation to the moment in which the facts were committed, in order to verify if the company had the necessary controls to avoid the unlawful occurrence. In some legal systems, such as Spanish, this assessment is important to determine whether the company should be held criminally liable and can have its sentence mitigated. In turn, the *prospective valuation* aims to analyze the entire program in relation to a certain type of crime, not being limited, however, to a specific occurrence. In the Spanish system, this evaluation is important to know the type of sanction. In some other countries, there is also the possibility of submitting the company to a kind of probation or entering into certain agreements. See: NIETO MARTÍN, Adán. Como avaliar a efetividade dos programas de cumprimento?. In: NIETO MARTÍN, Adán; SAAD-DINIZ, Eduardo (org.). *Legitimidade e efetividade dos programas de compliance.* São Paulo: Tirant lo Blanch, 2021. p. 6-26. p. 7-9.

[26] JANUÁRIO, Túlio Felipe Xavier. O sigilo profissional no âmbito das pessoas jurídicas: um estudo da particular posição dos in-house lawyers e dos advogados de compliance e de investigações internas. *Revista Brasileira de Ciências Criminais*, São Paulo, ano 27, n. 159, p. 297-339, set./2019, p. 315; JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 7, n. 2, p. 1453-1510, mai./ago. 2021, p. 1466. In a similar sense, Montiel states that any obligation to conduct internal investigations can only be identified with regard to the requirements of good governance derived from compliance, since, legally, there is no such obligation. See: MONTIEL, Juan Pablo. Sentido y alcance de las investigaciones internas en la empresa. *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, v. XL, p. 251-277, 2013. p. 262-265.

[27] On this point, we disagree with Sahan and Moosmayer, who understand that from Article 130 of the *Gesetz* über *Ordnungswidrigkeiten (OWig)* it is possible to derive an obligation to conduct CII. In our point of view, when establishing the administrator's obligation to take the necessary supervisory measures to prevent non-compliance with the obligations of the establishment or company, under penalty of administrative infraction, the Law does not specify what these measures are, making no express mention of conducting CII. Therefore, we understand that whether or not to carry out this procedure ends up being at the discretion of the administrator or person competent to

The investigative procedures tend to follow a minimally uniform rite, subject to some obvious particularities of the corporation and its scope of activities. As a rule, the company becomes aware of facts that are potentially illegal, or contrary to its internal rules, from denouncements through communication channels[28], its daily supervisory activities or

---

do so, as to what measures would be necessary in the specific case, without prejudice, of course, that these may be considered insufficient in the future and that the legal entity and its representatives suffer the consequences of this choice. We analyzed this problem in detail in: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Dos níveis de exigibilidade dos procedimentos de investigação interna. In: INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS. *Anais do CPCRIM*: IV Congresso de Pesquisas em Ciências Criminais, de 21 a 23 de outubro de 2020. São Paulo: IBCCRIM, 2020. p. 215-237. See also: SAHAN, Oliver. Investigaciones empresariales internas desde la perspectiva del abogado. In: KUHLEN, Lothar; MONTIEL, Juan Pablo; DE URBINA GIMENO, Íñigo Ortiz (eds.). *Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 245-259. p. 248-250; MOOS-MAYER, Klaus. Investigaciones internas: una introducción a sus problemas esenciales. In: ARROYO ZAPATERO, Luis; NIETO MARTÍN, Adán (dir.). *El derecho penal económico en la era compliance.* Valencia: Tirant lo Blanch, 2013. p. 137-144. p. 138.

28 As Beatríz García-Moreno explains, through the so-called *internal whistleblowing*, companies are expected, among other measures, to implement reporting channels so that their employees and other people close to the corporation can report certain irregularities internally, which will be subject to investigation and sanction by the company itself. See: GARCÍA-MORENO, Beatriz. *Del whistleblower al alertador:* la regulación europea de los canales de denuncia. Valencia: Tirant lo Blanch, 2020. p. 249. The Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law provides for the obligation of legal entities with 50 or more workers (or even fewer, in specific cases), to establish internal reporting channels. The procedure for these channels is provided for in Article 9 in the following terms: "Article 9 Procedures for internal reporting and follow-up 1. The procedures for internal reporting and for follow-up as referred to in Article 8 shall include the following: (a) channels for receiving the reports which are designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the reporting person and any third party mentioned in the report is protected, and prevents access thereto by non-authorised staff members; (b) acknowledgment of receipt of the report to the reporting person within seven days of that receipt; (c) the designation of an impartial person or department competent for following-up on the reports which may be the same person or department as the one that receives the reports and which will maintain communication with the reporting person

even externally, through the current or imminent promotion of a state investigation or criminal proceeding communicated directly to the company or reported in the media[29].

In some cases, as highlighted by Nieto Martín, depending on the origin of the complaint, it may be necessary to carry out a *preliminary investigation*, prior to the CII, in order to verify the degree of verisimilitude of the allegations, avoiding, thus, waste of the company's financial resources, as well as unnecessary interference in the scope of the rights of any persons being investigated[30].

Subsequently, an *investigation plan* is defined. This phase is essential for previously assessing the costs and time required for the CII, as well as for defining the limits of the methods employed. Furthermore, it is at this stage that the competences within the procedure are defined, appointing a person or department responsible for the investigation and

---

and, where necessary, ask for further information from and provide feedback to that reporting person; (d) diligent follow-up by the designated person or department referred to in point (c); (e) diligent follow-up, where provided for in national law, as regards anonymous reporting; (f) a reasonable timeframe to provide feedback, not exceeding three months from the acknowledgment of receipt or, if no acknowledgement was sent to the reporting person, three months from the expiry of the seven-day period after the report was made; (g) provision of clear and easily accessible information regarding the procedures for reporting externally to competent authorities pursuant to Article 10 and, where relevant, to institutions, bodies, offices or agencies of the Union. 2. The channels provided for in point (a) of paragraph 1 shall enable reporting in writing or orally, or both. Oral reporting shall be possible by telephone or through other voice messaging systems, and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe" (EUROPEAN PARLAMENT; COUNCIL OF THE EUROPEAN UNION. *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019:* on the protection of persons who report breaches of Union law. Available on: <http://data.europa.eu/eli/dir/2019/1937/2023-05-02>. Accessed on May 29th, 2023).

29 CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe X. Investigação defensiva corporativa..., p. 298.

30 NIETO MARTÍN, Adán. Investigaciones internas. In: NIETO MARTÍN, Adán et al. (dir.) *Manual de cumplimiento penal en la empresa*. Valencia: Tirant lo Blanch, 2015. p. 231-271. p. 235-236.

also deciding whether or not to hire external professionals[31]-[32]. In any case, internal or external lawyers must be granted the respective powers of attorney and signatures in the relevant terms of confidentiality must be taken from those involved in the investigation in order to ensure the legitimacy of the measures taken, as well as to preserve the secrecy of the information collected, if so decided[33].

Once the investigations themselves have begun, interviews are conducted, documents, audio and video recordings and other digital files (such as email messages, web files and hard disks) are collected and analyzed, and these may even be from working instruments – such as corporate computers and cell phones. Depending on the case and the area of activity, technical expertise may also be required[34].

It is precisely in the execution of these investigative activities that AI proves to be most useful. Attention is drawn, for example, to the

---

[31] Ibidem, p. 240-241. It is also important to point out that it may be in the company's best interest that facts under investigation are not disclosed to a greater number of employees than is strictly necessary, as an early disclosure, even if limited to the company's internal scope, may represent severe disadvantages to it and unfair stigmatization of the investigated. See: PELZ, Christian. Offenbarungs- und Meldepflichten bei Internal Investigations. In: In: AHLBRECHT, Heiko et al (Hrsg.). *Unternehmensstrafrecht:* Festschrift für Jürgen Wessing zum 65. Geburtstag. München: C. H. Beck, 2016. p. 605-624. p. 605.

[32] As we have already analyzed in detail on other occasions, one of the main factors that can be considered by the company when deciding whether or not to hire external professionals concerns the undeniable controversy over the extent of professional secrecy to so-called in-house lawyers, with different positions on whether they would be covered by prerogatives such as the *work-product-protection* and the *attorney-client-privilege*. See in detail at: JANUÁRIO, Túlio Felippe Xavier. O sigilo profissional..., p. 316ff; JANUÁRIO, Túlio Felippe Xavier. Cadeia de custódia..., p. 1468-1470. See also: VASCONCELLOS, Vinicius Gomes de. "The Right to Counsel and the Protection of Attorney-Client Privilege in Criminal Proceedings": direito de defesa técnica e relações cliente-advogado no processo penal contemporâneo. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 29, n. 176, p. 257-272, fev./2021. p. 263-264; p. 315-320; GALEGO SOLER, José-Ignácio. Investigaciones internas corporativas: de la práctica a la teoría. In: GÓMEZ MARTÍN, Víctor et al (dir.). *Un modelo integral de Derecho penal:* Libro homenaje a la profesora Mirentxu Corcoy Bidasolo. Madrid: BOE, 2022. p. 1150-1165. p. 1154-1157.

[33] NIETO MARTÍN, Adán. Investigaciones internas..., p. 240-242.

[34] JANUÁRIO, Túlio Felippe Xavier. Cadeia de custódia..., p. 1470.

predictive surveillance of employees, through which, based on the analysis of a dataset, it is expected to determine with a high degree of precision which employees are more likely to commit acts of non-compliance, including criminal offenses[35]. This dataset may include, for instance, audio and video files of environmental and telephone recordings, monitoring of e-mails and internet browsers, information about computer keystrokes, content published on social media and information regarding facial expressions, body heat, physical gestures and voice tones, being these later accessed through devices incorporated into workers' desks and offices[36]-[37].

Some other systems already available on the market[38] are allegedly able to detect "sensitive keywords" in communications (videos, phone calls, emails, etc.) and send an alert to the responsible department, so that it can analyze the interlocution. In addition, they have the ability to measure the actual work time performed by the employee, comparing it with the time he deals with outside matters[39].

Focusing his analysis on the use of AI in lie detection systems, and its possible use in CII, Trentmann explains that the present and the future of technical lie detection involve the detection and evaluation by AI systems of verbal and non-verbal signals and patterns. During a statement,

---

[35] BURCHARD, Christoph. Digital Criminal Compliance..., p. 747.

[36] DEARDEN, Lizzie. The Telegraph Backtracks on Sensors Monitoring Whether Journalists are Sitting at Desks Amid Outrage. *The Independent*, Jan./2016; MOORE, Phoebe V. *The Threat of Physical and Psychosocial Violence and Harassment in Digitalized Work*. Geneva: International Labour Office. Bureau for Workers' Activities, 2018. p. 26; CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felipe Xavier. Inteligência artificial e..., p. 373; JANUÁRIO, Túlio Felippe Xavier. Inteligencia artificial y..., forthcoming.

[37] Burchard mentions that these technologies are already in full swing, being known as *electronic performance monitoring*. The author exemplifies them with the use of GPS data and the (in theory, voluntary) implantation of chips in employees – a practice known as chipping. See: BURCHARD, Christoph. Digital Criminal Compliance..., p. 747; JANUÁRIO, Túlio Felippe Xavier. Inteligencia artificial y..., forthcoming.

[38] These are some of the functionalities announced, for example, by the systems *Veriato* and *Veritone*. See: VERIATO. *Employee Monitoring & Insider Threat Detection Software*: see and understand exactly what your employees are doing; VERITONE. *Making the AI revolution work for you*.

[39] CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 373-374.

the system collects, through cameras and microphones, information about facial expressions, gestures, language use or the frequency of certain terms and formulations. Subsequently, it compares these data to the empirical knowledge stored by the system and assesses whether the information provided by the declarant is true or false. The author explains that AI works particularly with voice stress analysis and with facial or eye scanning, also being able, in a combined approach, to recognize patterns very quickly, even based on an almost infinite data repertoire[40].

Among the many examples of AI-based systems for the analysis of verbal, non-verbal and combined signals[41], the so-called *Eye Detect* stands out for its application also in the private sphere[42]. As Trentmann explains, this system is owned by the American company *Conversus*, having been launched in 2019, but the technology used by it was created at the University of Utah in 2003 and has been improved since then. This software's approach is based on the observation that when a person is lying, their brain has to work harder, which ends up unconsciously affecting their eyes. Therefore, through high-speed cameras (especially infrared), the system records the reactions of the declarant's eyes to certain questions or situations, including changes in pupil diameter, eye movements, blinks or fixations. Its algorithm then calculates a credibility

---

[40] TRENTMANN, Christian H. W.. *Wahrheitsdetektionssyteme mit künstlicher Intelligenz*: ein neues Legal-Tech-Modell für Internal Investigations. Baden-Baden: Tectum Verlag, 2022. p. 29-30.

[41] The author cites and explains several examples of AI systems based on verbal signals (such as *Precire*, *VeriPol* and *Online Polygraph*), non-verbal signals (such as *Silent Talker*, *Facesoft*, *iBorderCtrl* and the aforementioned *Eye Detect*) and on combined analysis (such as *Real-life-Trial-Data-Analysis*, *DARE* and *AVATAR*). As the author points out, while a person can distinguish a true statement from a false one in 54% of cases (56% when prosecutors, judges and policemen), AI-based lie detection systems have an average hit rate of 79.17% when based on verbal signals, 87.75% when based on non-verbal signals and 82.67% when based on a combined analysis. See in detail at: TRENTMANN, Christian H. W. Op. Cit., p. 30ff.

[42] It is estimated that there are around 500 users of this technology, in 42 different countries. In Spain, for example, an automotive repair corporation uses the system to find out if its mechanics are making unnecessary repairs to customer vehicles. See: HELLER, Piotr. Lügendetektoren: Kann dieses Auge lügen?. *Frankfurter Allgemeinen Zeitung*, 12.10.2019. p. 2.

value between 0 and 100, with any value below 50 indicating that the claim is a lie[43].

We, therefore, observe that there is great potential for using AI in CII and compliance programs as a whole. However, even though we recognize that this technology can in fact make these activities more efficient and effective, the risks derived from it are equally relevant, and hence reflections on its legal bases are fundamental, especially if we consider its possible implications in criminal proceedings.

When the investigations are completed, a final report will be prepared with their respective conclusions[44]. The destination that will be given to the information obtained will be decided according to the specific interests of the company[45]. If signs of practices that are illegal or contrary to the company's internal regulations are found, the corporation may choose to: i) apply internal sanctions, such as warnings, suspensions or dismissals; ii) safeguard the information for the preparation of the company's defense in future state liability procedures, including in court, presenting the evidence it deems appropriate in those respective moments; or iii) share with the competent authorities the information and evidence collected that it deems appropriate and relevant, requesting their incorporation in official investigations and bargaining for eventual procedural benefits, such as settlements, reductions in sentences or acquittals, if applicable[46].

It is precisely from the hypothesis of sharing the results of CII with the authorities that some of the most relevant controversies arise in this scope, not only due to susceptibilities to "risk shifting" or violation

---

[43] TRENTMANN, Christian H. W.. Op. Cit., p. 43ff.

[44] NIETO MARTÍN, Adán. Investigaciones internas..., p. 258.

[45] In the same sense, emphasizing that internal responsible persons may decide, on their own initiative, whether to investigate and subsequently report to the authorities: SAHAN, Oliver. Op. cit., p. 246.

[46] CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felipe X. Investigação defensiva corporativa..., p. 299; JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., p. 1471.

of rights and guarantees of those involved[47]-[48]. Since in these procedures possible criminal offenses are generally investigated, the information collected in CII will often not be limited to the defensive purposes of the legal entity[49], and may be of interest to public authorities for the

---

[47] JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., p. 1472; CANES-TRARO, Anna Carolina; JANUÁRIO, Túlio Felipe X. Investigação defensiva corporativa..., p. 301. On the risk of risk shifting, that is, the behavior of administrators trying to transfer criminal responsibilities to occupants of lower positions or even to the legal entity, see: BALCARCE, Fabián I.; BERRUEZO, Rafael. *Criminal compliance y personas jurídicas.* Buenos Aires: Editorial B de F, 2016. p. 163-164; LAUFER, William S. Corporate Liability, Risk Shifting, and the Paradox of Compliance. *Vanderbilt Law Review*, v. 52, n. 5, p. 1343-1420, out./1999. p. 1368 e ss. Neira Pena also highlights this concern, noting that the neutrality of the investigator may be at stake, especially in cases where the company's directors are investigated. According to the author, in some legal systems, this problem is faced by imputing the crime of *obstruction of justice* to those who hinder the proper conduct of CII. The option, however, is controversial, especially if we think of the legal entity as having the *right against self-incrimination*. See in detail at: NEIRA PENA, Ana María. *La instrucción de los procesos penales frente a las personas jurídicas.* Valencia: Tirant lo Blanch, 2017. p. 344-347.

[48] The concern about the rights of whistleblowers can be observed, for example, in the Directive (EU) 2019/1937, which provides for measures to protect and support these agents. See: EUROPEAN PARLAMENT; COUNCIL OF THE EUROPEAN UNION. *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019:* on the protection of persons who report breaches of Union law. Available on: <http://data.europa.eu/eli/dir/2019/1937/2023-05-02>. Accessed on May 29th, 2023. See also, as examples, the Laws that transposed the Directive to the internal legal systems of Portugal and Spain, in: PORTUGAL. *Lei n. º 93/2021, de 20 de dezembro:* Regime Geral de Proteção de Denunciantes de Infrações. Available on: <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=&nid=3544&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo>. Accessed on May 29th, 2023; ESPAÑA. *Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.* Available on: <https://www.boe.es/eli/es/l/2023/02/20/2/con>. Accessed on May 29th, 2023.

[49] On the relevance of compliance programs in the attribution of criminal responsibility to legal entities, see: SOUSA, Susana Aires de. *Questões fundamentais de direito penal da empresa.* 2. ed. Coimbra: Almedina, 2023. p. 150ff; JANUÁRIO, Túlio Felipe Xavier. O ônus da prova da existência e eficácia dos programas de compliance no âmbito do processo penal das pessoas jurídicas: um estudo com base no ordenamento jurídico espanhol. *Revista Brasileira de Ciências Criminais*, São Paulo, ano 27, n. 160, p. 219-257, out./ 2019. p. 230ff.

purpose of ascertaining authorship and punishing the individual who committed the crime. For this reason, the transfer of this information to the criminal trial, either as defensive evidence from company, or through its collaboration with the authorities, raises numerous questions, starting with the compatibility of these private procedures with the rights and guarantees of those being investigated, such as the presumption of innocence, the contradictory and the right to non-self-incrimination[50]. In addition, since the collection of evidence in this scope is carried out by private entities, generally dissociated from public authorities, there are doubts regarding the possible means of ensuring the reliability of the evidence collected in CII and how to fully certify the procedure that was carried out in the collection, transport and storage of these information, including the subjects who intervened in each phase of the process[51-52].

The relevance of all these discussions enhances, in our view, if we consider the possible application of AI in CII, which is why it is fundamental to address the topic of possible legal frameworks for its employment and its possible criminal procedural implications.

---

[50] The issue becomes even more problematic if we observe that, in practice, those affected by CII tend to give up their most basic rights, such as the non-self-incrimination. This is due not only to the pressure (expressed or tacit, with the risk of dismissal) that is exerted on them, but also to the lack of understanding about the possibility that the information they offer may be passed on to public authorities in the future. See in detail: MOMSEN, Carsten. Internal Investigations zwischen arbeitsrechtlicher Mitwirkungspflicht und strafprozessualer Selbstbelastungsfreiheit. *Zeitschrift* für *Internationale Strafrechtsdogmatik*, n. 6, p. 508-516, 2011. p. 512.

[51] It is for this reason that we believe that the documentation of the chain of custody is also of paramount importance in the context of internal investigations. For a comprehensive study of this topic and its criminal procedural implications, see: JANUÁRIO, Túlio Felippe Xavier. Cadeia de custódia..., passim.

[52] In this scope, the concern with the preservation of digital evidence deserves special attention, since, as with most white-collar crimes, CII also depend heavily on the analysis of computer systems. As Basar explains, also in this corporate context, the future use of collected evidence depends, in addition to other conditions, on whether the originality of the digital data is not in question. In this sense, see: BASAR, Eren. Anforderungen an die digitale Beweissicherung im Strafprozessrecht und in internen Untersuchungen. In: AHLBRECHT, Heiko et al (Hrsg.). *Unternehmensstrafrecht:* Festschrift für Jürgen Wessing zum 65. Geburtstag. München: C. H. Beck, 2016. p. 635-647. p. 635; 642.

2. LEGAL GUIDELINES FOR APPLYING ARTIFICIAL INTELLIGENCE IN INTERNAL INVESTIGATIONS AND THE POSSIBLE ADMISSIBILITY OF INFORMATION IN SUBSEQUENT CRIMINAL PROCEDURES

2.1. LEGAL REQUIREMENTS FOR DATA PROCESSING

When referring to the use of AI within the scope of CII, we must bear in mind that this technology inescapably depends on data that feed its system. For this reason, the first question to be answered is about the eventual legal permissibility and the possible limits for data processing in this scope.

As Victor Valente points out, the protection of personal data is a fundamental and extremely personal, autonomous right, being effectively a result of the functionalization of privacy. Personal data are, above all, components of personality or legal capacity, conferring rights to their holder and legal obligations regarding informational self-determination[53]. In Brazil, the Federal Constitution provides in its Article 5th, X, the protection of the inviolability of private life, in addition to ensuring, in its item LXXIX, the right to the protection of personal data, including in digital media. In Europe, Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone is entitled to protection of personal data concerning them.

If we take the Brazilian legal system as a basis, we will see that the General Data Protection Law (LGPD) excludes from its regime, among others, data regarding public safety and criminal proceedings[54]. Likewise, the General Data Protection Regulation (GDPR) is also not applicable, within Europe, to data processed by authorities for the purposes of

---

[53] VALENTE, Victor Augusto Estevam. *A proteção de dados pessoais no direito penal:* uma análise crítica da criminalização nas perspectivas constitucional e de política criminal. Belo Horizonte: D'Plácido, 2022. p. 46-49.

[54] See Article 4th, in: BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*: Lei Geral de Proteção de Dados Pessoais. Available on: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Accessed on February 27th, 2023. About this, see: GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública.* Rio de Janeiro: Marcial Pons, 2021. p. 20.

"prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"[55]. However, in our opinion, these rules are not directly an impediment for data processing in CII. As we have already mentioned, not only the primary purposes of these procedures are neither strictly the public safety nor the investigation of crimes, but also there is a clear economic purpose when these activities are carried out.

This understanding also seems not to make CII incompatible with the provisions of Article 4th, §2nd, of the LGPD. It is a fact that this provision prohibits the processing of personal data by private persons for the sole purpose of investigation and criminal prosecution. However, as we have already pointed out, although these CII procedures can identify facts that fall under crimes, this is not their exclusive purpose. A contrary understanding, in our view, would make it impossible not only CII, but also compliance programs as a whole, hindering legal entities from fulfilling duties imposed to them by Law.

A point to be noted, however, is that, under the GDPR, the processing of data related to criminal convictions or offenses is not permitted, unless conducted under the control of an official authority or authorized by the law of a Member State of the Union, which also ensures rights and guarantees of the data subjects[56]. The interpretation to be made of this article, in our view, is that the use of data related to possible criminal records as input to AI systems can only occur if the

---

[55] See Article 2 (2) (d), in: EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available on: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Accessed on March 09th, 2023.

[56] See Article 10, in: EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available on: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Accessed on March 09th, 2023.

investigation takes place with the knowledge and supervision of the state authority in question or if the law of the Member State authorizes it. Furthermore, when the occurrence of a criminal offense is verified during the investigation, the processing of data may continue to take place for the purposes of better ascertaining the facts only in cases where the law authorizes the company to investigate (eg, anti-money laundering laws) or with the knowledge of the authority.

The LGPD presents different requirements for their processing in the case of *personal data* or *sensitive personal data*[57]-[58]. In a very similar way, the GDPR admits the processing of data in the cases provided for in Article 6, while Article 9(2) provides for the exceptional situations in which the processing of "special categories of personal data"[59] will be admitted.

In light of these legislation, we can consider that the main legal bases that authorize the processing of data within the scope of CII are, in descending order of relevance, i) *compliance with a legal or regulatory obligation*, by the company; ii) *the regular exercise of rights in judicial,*

---

[57] For the purposes of this Law, "personal data" is considered to be information related to an identified or identifiable natural person, and "sensitive personal data", those about "racial or ethnic origin, religious conviction, political opinion, union affiliation or organization of a religious, philosophical or political nature, data referring to health or sexual life, genetic or biometric data, when linked to a natural person" [free translation]. See Article 5th, in: BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*: Lei Geral de Proteção de Dados Pessoais. Available on: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Accessed on February 27th, 2023.

[58] See Article 7th and 11, in: BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*: Lei Geral de Proteção de Dados Pessoais. Available on: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Accessed on February 27th, 2023.

[59] Are thus considered: "1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited". EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available on: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Accessed on March 09th, 2023

administrative or arbitration proceedings; iii) the *pursuit of legitimate interests by the company*; iv) the *consent of the holder*[60].

In order to justify this order, we must point out that in cases where compliance obligations are imposed on the legal entity by law, decrees or regulations[61], they justify the processing of personal data as an indispensable measure for the fulfillment of these obligations. In our view, this legal basis overlaps with the hypothesis of regular exercise of rights in proceedings (expressly provided for only in the LGPD and not in the GDPR, except for sensitive data), because, although the legal entity has the legitimate right to defend itself, in some situations there would not be ongoing, or on the verge of being initiated, judicial, administrative or arbitration proceedings. Although the admissibility of this basis can

---

[60] Highlighting that the legal bases of the LGPD most commonly invoked by data controllers, regarding compliance and CII activities, are "legitimate interest" and "compliance with legal obligations": PALHARES, Felipe; PRADO, Fernando; VIDIGAL, Paulo. Compliance Digital e LGPD. In: NOHARA, Irene Patrícia Diom; ALMEIDA, Luís Eduardo de (coord.). *Coleção compliance, v. 5*. São Paulo: Thomson Reuters Brasil, 2021. Ebook. N. P. Section 5.3.14. We did not list here the "public interest" provided for by the GDPR, because even though the invocation of this legal basis can be ventilated, the delimitation between CII that in fact pursue this objective (for example, the investigation of a crime that occurred in its environment) and those who seek to investigate facts that are only of their private interest seems to us to be very casuistic. The same can be said with regard to the provision, in both legislations, of the possibility for the purpose of fulfilling contractual obligations, as it would depend on an analysis of the provisions set forth in the concrete employment contract.

[61] In the Brazilian Anti-Corruption Law (Law 12.846/13), for example, there is express recognition of compliance programs as relevant to the dosimetry of the sanction. In this regard, see in detail at: SILVEIRA, Renato de Mello Jorge. Autorregulação, responsabilidade empresarial e criminal compliance. In: SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. *Compliance, direito penal e lei anticorrupção.* São Paulo: Saraiva, 2015. p. 25-239. p. 190ff; FERNANDES, Fernando Andrade. Brasil. In: RODRÍGUEZ-GARCÍA, Nicolás (dir.); ONTIVEROS ALONSO, Miguel; ORSI, Omar Gabriel; RODRÍGUEZ-LÓPEZ, Fernando (coord.). *Tratado angloiberoamericano sobre compliance penal.* Valencia: Tirant lo Blanch, 2021. p. 155-241. p. 208ff. Regarding compliance duties in the scope of Anti-Money Laundering, specially in Portugal, see: CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felipe Xavier. Programas de compliance e branqueamento de capitais: implicações da lei nº 83/2017, de 31 de agosto, no regime jurídico de Portugal. *Revista Científica do CPJM*, v. 1, n. 3, p. 65-98, 2022.

be ventilated considering future hypothetical processes, the use of this legal basis is more appropriate when the company is actually defending itself, especially when sharing data with public authorities (a hypothesis that we will discuss in detail later).

The pursuit of the company's legitimate interest, although quite appropriate to the context of CII, is in third place on this list because, as can be seen from the aforementioned Article 11 of the LGPD and Article 9(2) GDPR, it is a hypothesis that does not support the processing of sensitive personal data, which will be of particular relevance (especially the biometric ones) if we consider the use of some AI systems in compliance programs and CII.

Finally, even though we consider the subject's free, informed and unequivocal consent necessary for each specific purpose of processing his/her data (including for subsequent purpose changes, such as eventual sharing with authorities), we understand that this should be the subsidiary legal basis in the case of CII and compliance programs. Firstly, because, pursuant to Article 8th, §5th, LGPD and Article 7(3) GDPR, consent may be revoked at any time, upon express manifestation by the holder. Also, because we have serious doubts about whether we can effectively talk about freedom of consent in labor relations. In other words, the fear of not being hired or, as the case may be, being fired, can hinder subordinate employees from exercising effectively, with freedom, their agreement or not with the processing of their data[62].

However, in light of the GDPR, we understand that the consent of the data subject is essential, even if this is not the legal basis invoked by the controller, when it comes to data processing for the purposes of using autonomous systems and AI. This is because Article 21 provides that the subject may object, at any time, to the processing of their data based on the public interest or the legitimate interest of the controller (hypotheses (e) and (f) of Article 6(1) GDPR), for e.g. profiling purposes, unless the

---

[62] Precisely in this sense: ARTICLE 29 WORKING PARTY. *Guidelines on consent under Regulation 2016/679:* Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2018. Available on: <https://ec.europa.eu/newsroom/article29/items/623051>. Accessed on March 10th, 2023; PALHARES, Felipe; PRADO, Fernando; VIDIGAL, Paulo. Op. cit., N. P. Section 5.3.7.2.2.

controller demonstrates that there are "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims". Furthermore, in accordance with Article 22, the data subject has the right not to be subject to any decision based on automated data processing, which may produce legal effects or affect him or her in any way, unless, among other hypotheses, if authorized by the legal system in question or based on the explicit consent of the data subject[63]. For this reason, regardless of the legal basis used, we maintain that there must also be the explicit consent of the data subject, including which data will be processed, for what purposes, and even which technological systems will be employed in the processing of this data.

Despite this order listed above, we maintain that, provided that the respective requirements are met, any of these legal bases can be invoked to substantiate the processing of data within the scope of compliance programs and CII. Legal authorization, however, although imperative, is not enough. The guiding principles of data processing must also be observed.

In a monograph on the subject, Gleizer, Montenegro and Viana maintain that the processing of data for purposes of public security and criminal investigations must comply with two fundamental principles: the *necessary reserve of law* (in the sense that all data processing presupposes authorization by law) and the *prohibition of excess* (in the sense that the proportionality of interventions must be observed)[64]. Although the purpose of CII is not strictly the investigation of crimes, we understand that these two principles can also guide the processing of data in this private sphere, not only because they are not incompatible with the LGPD and GDPR (quite the contrary), but, also, precisely because is possible that,

---

[63] See Articles 21 and 22 in: EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available on: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Accessed on March 09th, 2023.

[64] In this sense: GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. Op. Cit., p. 40.

within the scope of these CII, facts of criminal relevance are investigated and may be of interest to state investigations and proceedings.

Legal authorization refers precisely to the cases mentioned above, in which data processing is authorized. With regard to the test of proportionality, it refers to the balance that must be made between the means used by the data controller and the purposes sought by the processing. The criteria that must be observed in this proportionality test are, according to the authors: i) the legitimacy of the purpose, that is, that the purpose pursued must actually correspond to interests related to the common good; ii) adequacy, in the sense that the means chosen must be able to promote the purpose in question; iii) the necessity, in the sense that there should not be less onerous and equally efficient means to achieve the purpose in question; and iv) proportionality in the strict sense, in the sense that the severity of the intervention and the common interests pursued must be pondered[65].

According to the authors, this proportionality test is precisely materialized through the list of principles that is brought by Articles 6th of the LGPD and similar articles in the GDPR and DPD[66]. In short, they are: *good faith*; i) *purpose* (legitimate, specific, explicit, and informed purposes to the holder); ii) *adequacy* (processing according to the purposes informed to the data subject and the context of the treatment); iii) *necessity* (processing limited to the minimum necessary to achieve the purposes); iv) *free access* (facilitated and free consultation by the holders, of the form, duration and completeness of the data); v) *data quality* (accuracy, clarity, relevance and up-to-date data); vi) *transparency* (clear, precise and accessible information); vii) *security* (protection against unauthorized access, destruction, loss, alteration, communication or diffusion); viii) *prevention* (measures to avoid harm); ix) *non-discrimination* (prohibition of treatment for unlawful or abusive discriminatory purposes) and x) *responsibility and accountability* (clear demonstration of personal data protection measures and their effectiveness)[67].

---

[65] Ibidem, p. 58.

[66] Ibidem, p. 59.

[67] See Article 6th, in: BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*: Lei Geral de Proteção de Dados Pessoais. Available on: <https://www.planalto.gov.

Responding, therefore, to the question raised at the beginning of the topic, we understand that the processing of data for the purpose of applying AI in the scope of CII does not find obstacles, either in the LGPD or in the GDPR, being admitted, provided that it is supported by at least one of the legal hypotheses and respects the proportionality between the legitimate purpose sought and the means applied.

2.2. (In)Admissibility of AI systems in corporate internal investigations

A different question is to know which AI instruments would be admissible in the field of CII. Since they are very efficient in collecting, processing and storing data, as well as in predictions and decision-making, they open the door for the company to obtain a multitude of data and information from its employees, in addition to, in cases with more advanced systems, performing real-time monitoring and enabling automatic decision-making. However, even if there are eventually no problems in data processing, it is certain that the company will not be able to apply any and all AI systems without considering some rights and guarantees of those involved. Concerns about the level of intrusion into workers' privacy, secrecy of communications[68] and even physical integrity are evident[69].

A first limit to be observed is that of *legality*, that is, the adoption of these instruments must find legal support. As a rule, employer supervision

---

br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Accessed on February 27th, 2023. For a detailed analysis, see also: VALENTE, Victor Augusto Estevam. *A proteção de...,* p. 64ff; PALHARES, Felipe; PRADO, Fernando; VIDIGAL, Paulo. Op. cit., N. P. Section 5.2.

[68] According to Adán Nieto Martín, the difference between the two lies in the moment when the intervention takes place. When access to the content of a communication is given "live", at the time it occurs and affecting the channel in which it develops, the restricted right is that of *secrecy of communications*, which enjoys jurisdictional guarantee and requires a court order. On the contrary, when control takes place *a posteriori*, through access to the content of the communication, the affected right is privacy. See: NIETO MARTÍN, Adán. Investigaciones internas..., p. 250.

[69] CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 376.

and control measures are based on the *employer's directive power*[70], which attributes to him/her the burdens and powers related to the control of the work environment, the company's assets and employees. However, it is certain that these powers are not unlimited, encountering barriers precisely in the constitution, in the laws and eventually in collective agreements.

In Spain, for example, the Workers' Statute is clear in its Articles 20.3 and 18, that the employer can adopt the measures he/she deems opportune for the surveillance and control of the worker's labor obligations and duties, as well as for the protection of the business assets[71]. According to Gómez Martín, within the scope of this company's right to inspect its workers, there are two very distinct groups of cases: i) the right to register the worker, his locker and his personal objects; and ii) the right to supervise the work instruments that the employer makes available to the employee. In the first case, it is a very exceptional measure to be taken only in the working environment and hours, and must also respect, to the maximum, the worker's dignity and privacy. In turn, the second group encompasses the installation of cameras, microphones and other technological forms of communication control, especially those carried out in the computers and cell phones provided by the company. It is important to point out that, although based on the rights and duties assumed in the employment contract, especially the employers' right to supervise and control their means of production, properties and employees, this control cannot be unlimited either. Even if provided for work purposes, work tools (such as cell phones and corporate computers) may be used

---

[70] DELGADO, Maurício Godinho. *Curso de direito do trabalho*. 11. ed. São Paulo: LTr, 2012. p. 662; BARROS, Alice Monteiro. *Curso de direito do trabalho*. 7. ed. São Paulo: LTr, 2011, p. 462; CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 373; JANUÁRIO, Túlio Felippe Xavier. Inteligencia artificial y..., forthcoming.

[71] See: ESPAÑA. *Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.* Available on: <https://www.boe.es/eli/es/rdlg/2015/10/23/2/con>. Accessed on March 03th, 2023. See also: LEÓN ALAPONT, José. Medios de tecnovigilancia e investigaciones internas en el ámbito empresarial: algunas consideraciones sobre la tutela penal y procesal del secreto de las comunicaciones la intimidad (¿derechos negociables?). In: ROPERO CARRASCO, Julia (coord.). *Aspectos jurídicos de actualidad en el ámbito del derecho digital.* Valencia: Tirant lo Blanch, 2023. p. 114-141. p. 127.

in some specific cases for personal purposes, especially outside working hours or during rest periods[72].

In Brazil, the legislation is not clear and much less extensive in this matter. Initially, it is understood that the directive power of the employer is based on Article 2nd CLT, when considered as the person who directs the personal provision of service. This is a power derived from the labor contract itself and whose content can be divided into *organizational*, *control* and *disciplinary powers*[73]. Concrete provisions, however, about which control measures are permitted or prohibited are scarce[74]. Article 74 allows, in a general way, the control of working hours, which may be manual, mechanical or electronic. Furthermore, Article 373-A, item VI, prohibits intimal searches of female employees[75].

One could question, for example, in light of the lack of legal authorization and mainly in view of the reserve of jurisdiction in the matter, whether the employer would be authorized to intercept (including with technological systems, perhaps with AI) employees' communications. Gustavo Garcia, considers it inadmissible, since telegraphic, data and telephone communications are inviolable, except, in the latter case, with a court order for the purposes of investigation and criminal proceedings. Although the constitutionally foreseen inviolability is unquestionable, we understand, however, that a possible obstacle would not be based on this

---

72 GÓMEZ MARTÍN, Victor. Compliance y derecho de los trabajadores. In: KUHLEN, Lothar; MONTIEL, Juan Pablo; DE URBINA GIMENO, Íñigo Ortiz (eds.). *Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 125-146. p. 132-135.

73 See: GARCIA, Gustavo Filipe Barbosa. *Curso de direito do trabalho.* 8. ed. Rio de Janeiro: Forense, 2014. Ebook. N.P. Section 11.5.

74 Amauri Mascaro and Sônia Mascaro draw attention, for example, to the fact that the personal search arose from usages and customs, and just cannot be abusive. For the authors, the new technological control mechanisms, among which those that make use of images or sensors, must obey the same principles, balancing in the specific case, the dignity and privacy of the employee and the requirements of security and organization. See: NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro. *Curso de direito do trabalho.* São Paulo: Saraiva, 2014. 29. ed. Ebook. N.P. Chapter 43. Section 11.

75 BRASIL. *Decreto-Lei nº 5.452, de 1º de maio de 1943*: Aprova a Consolidação das Leis do Trabalho. Available on: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Accessed on March 03th, 2023.

issue. If, on the one hand, terminologically speaking, the recording of a conversation between two agents by a third party would fit the concept of a *telephone interception* or an *environmental interception*, on the other, it would not affect the freedom of communications and intimacy, if (and only if) interlocutors have previous knowledge of the recording[76]. By this we mean that the eventual use of AI systems that monitor telephone, telematic or environmental communications does not violate Art. 5th, XII, CF, provided that there is knowledge on the part of the interlocutors. This does not mean, of course, that this employment is *proportional*, a criterion that we will discuss later.

Directly related to the abovementioned issue, we can also identify as one of the main limits that must be observed (not only when applying new technologies, such as AI, but in CII as a whole) those spaces in which there are *expectations of privacy* on the part of those investigated. Even if provided for work purposes, it is commonplace, in practice, for employees to use some work tools, such as cell phones, computers and corporate e-mail, also to deal with personal matters. This is an undeniable result of today's fluidity of boundaries between the work and home environment, accentuated by phenomena such as the digitalization of work and the home office[77]. For this reason, there are precedents and it is well recognized in the doctrine that there is an *expectation of privacy*

---

[76] According to the classification presented by Badaró, *telephone interception* is configured when there is telephone communication, with third-party interference, without the interlocutors' knowledge; *wiretapping,* when there is telephone communication, with the interference of a third party, with the knowledge of one of the interlocutors*; clandestine telephone recording*, when the telephone communication is recorded by one of the interlocutors; *environmental interception*, when a third party records a conversation between those present, without the knowledge of any of them; and *clandestine environmental recording*, when one of those present records a conversation, without the knowledge of the other. For the author, situations in which there is environmental or telephone recording, by one of the interlocutors or by a third party, with everyone's knowledge, do not enjoy legal relevance in terms of freedom of communications or protection of privacy. See with details and references at: BADARÓ, Gustavo Henrique. *Processo penal*. 8.ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. p. 592.

[77] OIT. *Trabalho em tempos de COVID*: Relatório do diretor-geral, Conferência Internacional do Trabalho, 109ª sessão, Genebra, 2021. p. 14.

and consequent limits to the inspection and monitoring of information stored in cell phones, computers, e-mail and other work instruments[78].

This expectation, however, may be excluded, in the specific case, when the employer gives the employee *prior and explicit notice* that the objects and tools are to be used exclusively for work purposes, defining the limits of permissibility for their use and making it clear that they can be inspected and what the concrete information that can be collected from them will be[79].

---

[78] See: ECHR. *Case of Copland v. The United Kingdom.* Application n.º 62617/00. Strasbourg, 03/04/2007. Available on: <https://www.juridice.ro/wp-content/uploads/2016/07/1531450.pdf>. Accessed on June 10th, 2021; BRASIL. TRT-9. *TRT-PR-02822-2001-660-09-00-8 (RO-05568-2002) – Acórdão -06845-2003.* Rel. Juíza Janete do Amarante. Diário da Justiça Paraná, XLIX, Edição digitalizada n. 6343. Curitiba, 6ª feira, 04 de abril de 2003. p. 397. Available on: <https://www.tjpr.jus.br/diario-da-justica>. Accessed on June 10th, 2021; ESPAÑA. TS. SALA DE LO PENAL. *STS 1486/2021 - ECLI:ES:TS:2021:1486:* Sentencia núm. 328/2021. Ponente: Manuel Marchena Gómez. 22.04.2021. Available on: <https://www.poderjudicial.es/search/AN/openCDocument/cac2ec927df2ac24eb9f320e282b0b4267378998e-9c61ee7>. Accessed on March 10th, 2023; CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 376-377. For a detailed analysis of the Spanish judgment 328/2021, see: GÓMEZ MARTÍN, Víctor. ¿Un nuevo golpe de gracia a las investigaciones internas corporativas? Reflexiones en voz alta sobre la sentencia de tribunal supremo 328/2021, de 22 de marzo. In: GÓMEZ MARTÍN, Víctor et al (dir.). *Un modelo integral de Derecho penal:* Libro homenaje a la profesora Mirentxu Corcoy Bidasolo. Madrid: BOE, 2022. p. 1167-1178. p. 1174ff. On the contrary, rejecting this expectation of privacy: ESPAÑA. TS. SALA DE LO SOCIAL. *STS, 6 de Octubre de 2011.* Ponente: Jesus Souto Prieto. Available on: <https://vlex.es/vid/-347104538>. Accessed on March 10th, 2023.

[79] See: BRASIL. TST. *RR - 61300-23.2000.5.10.0013.* 1ª. Turma. Rel. Ministro João Oreste Dalazen. Data de Julgamento: 18/05/2005. Data de Publicação: DJ 10/06/2005. Available on: <http://www.tst.jus.br/>. Accessed on June 10th, 2021; ECHR. *Case of Bărbulescu v. Romania.* Application n.º 61496/08. Strasbourg, 05/09/2007. Available on: <http://www.marinacastellaneta.it/blog/wp-con-tent/uploads/2017/09/CASE-OF-BARBULESCU-v.-ROMA-NIA.pdf>. Accessed on June 10th, 2020; PORTUGAL. STJ. *Processo 07S043. N.º Convencional JSTJ000. N.º do Documento SJ200707050000434.* Rel. Mário Pereira. Data do Acórdão: 05/07/2007. Available on: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/54d3c9f0041a33d-58025735900331cc3?Open-Document&Highlight=0,07S043>. Accessed on June 10th, 2021; CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 377; GÓMEZ MARTÍN, Victor.

It is also important to mention, as Montiel does, that there are certain areas in which the *expectation of privacy is unchangeable*, as an eventual breach would affect an intangible core of intimacy, referring to the most private and personal sphere of workers. This would be the case, for example, of digital files from recordings made in locker rooms and bathrooms, genetic tests and compulsory intimate searches[80].

But attending the employee's expectation of privacy is not enough to attest to the legitimacy of the employer's intervention. In our view, it is necessary to balance the interests based on the *proportionality test*[81], assessing whether, in the specific case, i) the measure restricting the worker's right is likely to achieve the desired purpose (*adequacy* judgment); ii) if there are no other equally effective measures that restrict to a lesser degree the worker's right (*necessity* judgment); iii) whether the concrete restriction of the worker's right results in more benefits for the common good than its preservation to the detriment of the purpose sought (*proportionality in the strict sense*)[82]. Gómez Martín understands as

---

Compliance y derecho..., p. 134-135; ECHR. *Case of Copland v. The United Kingdom.* Application n.º 62617/00. Strasbourg, 03/04/2007. Available on: <https://www.juridice.ro/wp-content/uploads/2016/07/1531450.pdf>. Accessed on June 10th, 2021.

[80] For the author, postal or electronic correspondence of a personal nature, as well as lockers and offices assigned for personal use, also fall under this category. See: MONTIEL, Juan Pablo. Autolimpieza empresarial: compliance programs, investigaciones internas y neutralización de riesgos penales. In: KUHLEN, Lothar; MONTIEL, Juan Pablo; DE URBINA GIMENO, Íñigo Ortiz (eds.). *Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 221-243. p. 234-235.

[81] In the same opinion: ALCÁCER GUIRAO, Rafael. Investigaciones internas: prolegómenos constitucionales y cuestiones abiertas. In: GÓMEZ MARTÍN, Víctor et al (dir.). *Un modelo integral de Derecho penal:* Libro homenaje a la profesora Mirentxu Corcoy Bidasolo. Madrid: BOE, 2022. p. 989-1000. p. 997-998; GÓMEZ MARTÍN, Victor. Compliance y derecho..., p. 133. Also highlighting the rule of proportionality, plus the employee's consent, as pillars of authorization of compliance programs, especially in light of Article 32 of the BDSG, see: MASCHMANN, Frank. Compliance y derechos del trabajador. In: *KUHLEN, Lothar et al. (eds.). Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 147-167. p. 151ff.

[82] ESTRADA I CUADRAS, Albert; LLOBET ANGLÍ, Mariona. Derechos de los trabajadores y deberes del empresario: conflicto en las investigaciones empresariales internas. In: SILVA SÁNCHEZ, Jesús-María (dir.); MONTANER

disproportionate, for example, using technological instruments to carry out constant and indiscriminate surveillance of everything that appears on the worker's computer screen, without distinction between what is personal and what is related to work[83].

In the light of what has been exposed so far, we can observe that this judgment made between the interests at stake in the specific case, based on the proportionality test, is perhaps the most fundamental criterion in assessing the admissibility or not of AI systems in CII. As we have explained, the criterion of legality ends up being fulfilled not only by the norms that authorize the necessary measures to implement the employer's directive power, but also by those that encourage the adoption of specific supervision and control measures within the scope of compliance programs. Therefore, with the exception of some occasional express prohibitions, AI systems in this field are not illegal.

Likewise, it has been demonstrated that there are spaces in which the employee's expectation of privacy must be respected, and in some cases it cannot even be waived under any circumstances. However, fulfilling this criterion does not impose severe practical difficulties either, since it demands mere prior and detailed information to the employee about the limits of use and the possibility and means of surveillance. In addition, we cannot forget the undeniable position of vulnerability in which workers find themselves, which is why we believe that, even if notified, they will often not be in full conditions to truly understand the implications of the situation they are facing, or not interested in extend the discussions regarding it, precisely due to the fear of being fired or not being hired.

The proportionality test, in turn, ensures the analysis, in the specific case, of what technology is being used, which rights are being restricted, what the expected benefit of this use, the level of suspicion and the severity of the facts are, in addition to other important for the analysis of the admissibility, or not, of using the system. We understand that an absolute answer, either in the sense of full admissibility or in the sense of an absolute ban on AI in CII, would not be satisfactory.

FERNÁNDEZ, Raquel (coord.). *Criminalidad de empresa y compliance: prevención y reacciones corporativas.* Barcelona: Atelier, 2013. p. 197-228. p. 205.

[83] GÓMEZ MARTÍN, Victor. Compliance y derecho..., p. 135.

It is evident that companies are currently in an uncomfortable position of complying with an immensity of duties imposed by law and regulations, whose non-compliance can bring severe reputational and financial consequences and especially in terms of liability, including criminal responsibility. And it is also true that emerging technologies, in which we include AI, are fundamental for compliance, aggregating in terms of efficiency and effectiveness.

However, if even within the scope of criminal investigations and prosecutions, not any and all measures based solely on efficiency are admissible, much less will they be in this environment of *privatization of criminal procedure*[84], in which there is often no suspicion of an illegal act, since many instruments are used for day-to-day supervision and monitoring purposes.

Based on what has been said, we consider unacceptable, for example, any kind of polygraph, such as those exposed in the first topic[85]. At stake, in our view, is the constitutional guarantee that no one will be subjected to torture or inhuman or degrading treatment, provided for in Brazil in Art. 5th, II, CF[86]. Despite its alleged efficiency for detecting lies, which would make it *adequate* for achieving its purposes, we understand that there are less harmful means to the rights of those being investigated, which would mean that it would not pass the criterion of *necessity*. It could be argued that it is more effective than other means. However, even if that is the case, the investigation of relevant facts for the company[87]

---

[84] On this "privatization", see: ANTUNES, Maria João. Privatização das investigações e compliance criminal. *Revista Portuguesa de Ciência Criminal*, Coimbra, ano 28, n. 1, p. 119-128, jan./abr. 2018. p. 121-122.

[85] On the contrary, admitting it solely for the purpose of exculpation and when the initiative for its use came from the employee himself: TRENTMANN, Christian H. W.. Op. Cit..

[86] In this sense: LOPES JR., Aury. *Direito processual penal*. 19. ed. São Paulo: SaraivaJur, 2022. p. 513.

[87] We understand that the facts discovered in interviews have their relevance restricted to the business environment, because, as we will explain later, we sustain, following Canestraro, that interview reports cannot be transferred to criminal procedures. See: CANESTRARO, Anna Carolina. *As investigações internas no âmbito do criminal compliance e os direitos dos trabalhadores*: considerações sobre a possibilidade de investigar e a transferência de informações para o processo penal. São Paulo: IBCCRIM, 2020. p. 93-94.

certainly does not prevail over the protection of human dignity, object of protection of the guarantee in question.

2.3. Legal boundaries on the transmission to criminal proceedings of information obtained in internal investigations with the assistance of AI

Although the investigation of crimes is not necessarily the purpose of CII, it is true that the facts ascertained within their scope may correspond to criminal offenses. That said, even though conducted in a private environment, by entities dissociated from public authorities, CII become a relevant problem in criminal procedural terms from the moment that the company, upon completing the investigation, decides to share the established information with the public authorities for the purpose of obtaining the appropriate benefits (possible mitigation or exemption of penalties, conclusion of agreements, etc.) or even present them in the context of their defense in judicial or administrative proceedings that are brought against them.

However, it is evident that the conclusions of the investigation will not always be limited to demonstrating, if that is the case, the correctness of the organization, controls and business procedures, but will often indicate who the people who circumvented the compliance program and committed the crimes were. This raises a number of questions, especially with regard to the admissibility and probative value of the conclusions of CII and the documents collected in them, in future criminal proceedings.

On the one hand, it is true that the debates on how to guarantee the reliability of the elements of information collected in CII and whether and how to make these procedures compatible with criminal procedural guarantees such as non-self-incrimination, the contradictory and the presumption of innocence, have already existed even before the massive use of AI in these activities[88]. However, the progressive use of these

---

[88] As Neira Pena points out, even though at first glance they may seem unrelated to CII, some rights and guarantees of those being investigated, such as the presumption of innocence, the right to remain silent, not to incriminate oneself and to have a private lawyer, must, in fact, be observed, otherwise, the use of this information in a future investigation or criminal proceeding may be rejected. See: NEIRA PENA, Ana María. *La instrucción de...*, p. 361-362. On

technologies tends to accentuate the relevance of these discussions, especially if we consider that, in addition to their indisputable benefits, they have serious limitations and risks[89].

A first limitation, already widely pointed out by the doctrine, is the *opacity* of AI systems. This means that, due to its technical complexity, this technology imposes severe difficulties on the human understanding of its internal procedures, the decisions that underlie decision-making and even the data that are used as input, to reach of a given output. That is, even though we have access to the concrete decision taken by the system, understanding its "hows" and "whys", when possible, is very difficult[90]-[91].

---

this topic, especially on the impossibility of waiving the right to non-self-incrimination in the employment contract, see: SILVA, Douglas Rodrigues da. *Investigações corporativas e processo penal:* uma análise sobre os limites da licitude da prova. Londrina: Thoth, 2021. Ebook. N.P. Section 4.3.3.

[89] See: JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e responsabilidade penal no setor da medicina. *Lex Medicinae*: Revista Portuguesa de Direito da Saúde, ano 17, n. 34, p. 37-63, jul./dez. 2020, p. 44ff; JANUÁRIO, Túlio Xavier. Inteligência artificial e direito penal da medicina. In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal, volume II*. Coimbra: Almedina, 2022. p. 125-174, p. 135ff.

[90] See: BURRELL, Jenna. How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. *Big Data & Society,* v. 3, n. 1, p. 1-12, jan./jun. 2016, p. 1; WIMMER, Miriam. Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios. In: LIMA, Ana Paula Canto de; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes (eds), *Direito Digital:* Debates Contemporâneos, São Paulo: Thomson Reuters Brasil, 2019; Ebook. N. P. Chapter 1. Section 3.; RODRIGUES, Anabela Miranda. Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização. In: RODRIGUES, Anabela Miranda (coord.). *A Inteligência Artificial no Direito Penal, vol. 1.* Coimbra: Almedina, 2020, p. 11-58. p. 25; DE HOYOS SANCHO, Montserrat. El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea. *Revista General de Derecho Procesal*, n. 55, p. 1-29, 2021, p. 4; JANUÁRIO, Túlio Felippe Xavier. 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. *Revista Brasileira de Ciências Criminais*, ano 29, n. 186, p. 127-173, Dec./2021, p. 159. Nieva Fenoll also highlights the difficulties imposed by intellectual property issues. See at: NIEVA FENOLL, Jordi. *Inteligencia artificial y proceso judicial.* Madrid: Marcial Pons, 2018. p. 143.

[91] This opacity is increased if we consider that the companies responsible for the development of this technology are generally protected by trade secrets

This opacity also has, as one of its consequences, doubts related to the data used as input, either with regard to the legality of their obtaining or their own quality. In this sense, as Miró Lliñares points out, today's data collection differs from that carried out in the past, which always depended on minimally conscious and active conduct by their holders. Currently, data are shared on a massive scale, causing well-founded fears of disproportionate violations of people's privacy. Furthermore, poor data quality can be caused by poor qualification by the programmer, collection over a very short period of time, or the simple fact that the data in question are not representative. In either case, the invalidity or inaccuracy of the data will increase the chances of inaccurate outputs and, consequently, of errors[92].

Finally, we must also not forget that, due to their ability to "learn" from their past experiences and autonomously adapt their own algorithms,

---

and intellectual property rights, having no interest in making public some aspects of their production. See: GÓMEZ COLOMER, Juan-Luis. Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión. In: CALAZA LÓPEZ, Sonia; LLORENTE SÁNCHEZ-ARJONA, Mercedes (dir.). *Inteligencia artificial legal y administración de justicia*. Cizur Menor: Aranzadi, 2022. p. 257-287. p. 262-263.

[92] MIRÓ LLINARES, Fernando. Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología,* 3. época, n. 20, p. 87-130, Jul./2018, p. 114ff. On the issue of data security and quality and their possible impacts, see: DE HOYOS SAN-CHO, Montserrat. El Libro Blanco sobre Inteligencia Artificial de la Comis-ión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo". *Revista Española de Derecho Europeo,* n. 76, p. 9-44, Oct./Dec. 2020, p. 16ff; JANUÁRIO, Túlio Felipe Xavier. Considerações preambulares acerca das reverberações da inteligência artificial no direito penal. In: COMÉRIO, Murilo Siqueira; JUNQUILHO, Tainá Aguiar (orgs.). *Direito e tecnologia*: um debate multidisciplinar. Rio de Janeiro: Lumen Ju-ris, 2021. p. 295-314; MIRANDA, Matheus de Alencar e; JANUÁRIO, Túlio Felipe Xavier. Novas tecnologias e justiça criminal: a tutela de direitos humanos e fundamentais no âmbito do direito penal e processual penal. In: MOREIRA, Vital et. al. (orgs.). *Temas de Direitos Humanos do VI CIDH Coimbra 2021*. Campinas/Jundiaí: Brasílica/ Edições Brasil, 2021, p. 284-298, p. 286ff.

more advanced AI systems can end up proving to be unpredictable at a certain point, even for their programmers[93]-[94].

In our opinion, these limitations have the potential to further increase the risk of violating the rights and guarantees of those investigated in CII. The opacity of AI systems and the algorithms used by them tend to limit the concrete possibilities of those involved to understand and contest the decisions eventually taken against them. Likewise, the analysis of which dataset was taken into account for a given decision and, consequently, whether they were obtained in a lawful manner and operated in a non-imprecise or even non-discriminatory manner is quite an obstacle.

This framework reinforces what we have already argued on other occasions[95], in the sense that the transfer of information and documents from CII to the criminal process must be subject to rigorous analysis, and one cannot speak of unrestricted transmission of the integrality of the fruits of these procedures.

Initially, it is important to point out that sharing data processed within the scope of CII can configure, depending on the case, a change of purpose and, consequently, a new intervention. By this we mean that, if the legal basis used to authorize the processing of data has been other than the exercise of defense in judicial, administrative or arbitration proceedings,

---

[93] Precisely as Susana Aires de Sousa explains, one of the main specificities of autonomous systems lies in their ability to achieve *outputs* without human interference, based solely on information and experience acquired by them. As a result, *outputs* (even illegal ones) that were not even imagined by the programmers can be achieved. See: SOUSA, Susana Aires de. "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial". In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal*. Coimbra: 2020. p. 59-94. p. 64. See also: JANUÁRIO, Túlio Xavier. Veículos autónomos e imputação de responsabilidades criminais por acidentes. In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal*. Coimbra: Almedina, 2020. p. 95-128, p. 118ff; VALENTE, Victor Augusto Estevam. *Inteligência artificial e o direito penal:* a propósito da responsabilidade criminal em decorrência de sistemas tecnológicos altamente complexos nas empresas. Belo Horizonte: D'Plácido, 2023. p. 28.

[94] We addressed these aforementioned limitations also in: JANUÁRIO, Túlio Felippe Xavier. Inteligencia artificial y..., forthcoming.

[95] JANUÁRIO, Túlio Felippe Xavier. Inteligencia artificial y..., forthcoming; CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., passim.

sharing them for these areas will require a new legal authorization and judgment of proportionality in a broad sense. Consider, for example, the hypothesis that data processing initially took place only to fulfill compliance obligations (Art. 7th, II, LGPD). The use of these data for the exercise of defense in legal proceedings, even if to demonstrate the existence and effectiveness of the compliance program, constitutes a deviation from the original purpose, which does not necessarily prohibit their sharing, but demands a new analysis on the fulfillment of the requirements for this purpose.

The misuse of purpose configured by data sharing is observed even in the field of public entities. Citing the *principle of informational separation*, whose constitutional status in Germany had even been recognized by the BVerfG, Gleizer, Montenegro and Viana draw attention to the fact that data transfer between bodies of criminal prosecution, public security and intelligence, must be exceptional, and all exceptions must be clearly regulated and delimited by law, in authorization rules. According to the authors, any form of sharing implies an autonomous intervention in informational rights, as they represent a breach in the finalistic linkage[96].

As the authors argue, we can consider *data sharing* when two entities (even if carrying out activities of the same nature) or two departments within the same entity, exchange information, regardless of how they do it. For the authors, the *formal legality* of this sharing could be solved through the so-called *two-door model*, in the sense that is necessary a rule to authorize the entity that first collected and stored the data (primary controller) to give access to the information and another rule that authorizes the entity that will receive the data (secondary controller). The foundation of this proposition relies in the fact that data sharing involves two distinct interventions, each of which demands its own legal basis. The first would consist of changing the purpose that had determined the collection of data, with legal authorization specifying the extent of shared data and the new purposes for which sharing is acceptable. The second refers to the storage and use of data by the secondary controller, and the legal authorization must specify the conditions for processing

---

[96] GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. Op. Cit., p. 56-57.

the data and the standards of protection, including the duties of control and elimination[97].

The authors also support a second criterion, which is obligatory to observe in the context of sharing, which would refer to the *material principle of differentiation according to the proximity between the purposes of the collection and the new purpose sought with sharing*. This means that the greater the distance between these purposes, the more onerous the intervention and the higher the requirements to be observed for sharing. German doctrine, by the way, usually applies the so-called *hypothetical intervention doctrine*, which supports the possibility of sharing between entities only if the secondary controller has similar authorization for a hypothetical collection, under the same terms as the primary controller, including the one regarding gravity of the means employed by the latter[98].

Applying these considerations to the scope of CII, sharing the data collected in these procedures with the state investigation and prosecution authorities would require, in the first place, specific and clear legal authorization to change the purpose of data processing, that is, for sharing with the authority. In Brazilian law, this authorization is found in Arts. 7th, VI and 11, II, d, LGPD. Once this requirement has been met, it would be necessary legal authorization for the authority in question to receive data from CII. In the persistent lack of data protection legislation in the field of criminal justice in Brazil[99], the precise regulation of this matter is unfortunately still missing, and this analysis is only possible

---

[97]   Ibidem, p. 135-138.

[98]   Ibidem, p. 138-140.

[99]   In Europe, data processing for the purposes of "prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties" is regulated by Directive (EU) 2016/680. See: EUROPEAN UNION. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016:* on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Available on: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&-from=EN>. Accessed on March 10th, 2023. In Brazil, although it is in the legislative process, we still do not have a data protection law in the field of criminal justice and public security.

in light of the rules on sharing information in specific areas (e.g., anti-money laundering; anti-corruption; state-owned companies, etc.) and, in the case of the criminal procedures, the rules of admissibility and valuation of evidence. The *material legality* does not seem to present major difficulties, since, despite the difficulties to do so, public investigation and criminal prosecution authorities have the means to request this information themselves.

It is also important to mention that if the legal basis used as fundament for processing data in CII has been the *consent of the holder* (Art. 7th, I; Art. 11, I, LGPD), it must contain, from the first moment, explicit information on its purpose to the holder, under penalty of a new legal basis or a new consent form being necessary[100].

As regards admissibility of documents collected within the scope of CII in criminal proceedings, we understand that some situations should be differentiated. In principle, these elements of information will be admissible in criminal proceedings when the company presents them in the context of its defense, precisely as a realization of its right of defense and right to present evidence. A contrary understanding, in our opinion, would represent not only an unacceptable violation of these rights, but also a factor that discourages the adoption of compliance programs and the conduction of CII[101].

The issue is much more complex when it comes to the admissibility of elements of information from an CII, presented by the Public Prosecution, to the detriment of another defendant (an employee, for example), or even presented by the company's defense, in detriment

---

[100] As Gleizer, Montenegro and Viana point out, the fundamental rights that protect the conditions for the free development of the personality guarantee the predictability, on the part of the individual, about the use that will be made of his/her data. This means, in other words, that the purpose of the intervention must be determined in advance, at the time of data collection (*principle of finalistic linkage*), and that any subsequent change in this purpose must be justified, that is, any treatment with a purpose different from the one on which the collection was based, will configure an autonomous intervention act that will demand a new and autonomous legal authorization. See: GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. Op. cit., p. 50-51.

[101] JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., p. 1483-1484; JANUÁRIO, Túlio Felipe Xavier. Inteligencia artificial y..., forthcoming.

to another defendant. In these cases, as noted, there is a conflict between the rights to contradictory and due process of the subject affected by the evidence and the right of defense of the defendants, especially of the company that conducted the CII[102].

For these situations, we propose the following solutions: i) the elements of information will be admissible in criminal proceedings when presented by the defendant in his defense and will be fully valued for these purposes, except, of course, when obtained illegally[103].

ii) although admissible, the aforementioned elements of information, whether presented by the Public Prosecution, or presented by one defendant against another, can never be considered sufficient to substantiate a conviction. This is an intermediate proposal between full valuation and total non-admission[104], which aims to meet the functionality

---

[102] JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., p. 1483-1484; JANUÁRIO, Túlio Felipe Xavier. Inteligencia artificial y..., forthcoming.

[103] JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., p. 1483-1484; JANUÁRIO, Túlio Felipe Xavier. Inteligencia artificial y..., forthcoming.

[104] Greco and Caracas, for example, understand that there is a *prohibition of admitting evidence* (*Beweisverwendungsverbot*) whenever it is identified that the start of the CII was encouraged by the criminal prosecution bodies or if they postpone the start of state investigation procedures, for the purpose of taking advantage of the evidentiary material produced in private proceedings. See: GRECO, Luís; CARACAS, Christian. Internal investigations e o princípio da não auto-incriminação. In: LOBATO, José Danilo Tavares et al (orgs.). *Comentários ao direito penal econômico brasileiro.* Belo Horizonte: D'Plácido, 2018. p. 787-820. p. 807ff. Although it is a well-founded solution and seems to solve the problem presented here, we have doubts about its practical usefulness, mainly due to the fact that the authors consider as an incentive any influence of the prosecution bodies on the formation of the company's will that results (from the perspective of adequate causality) in the initiation of the CII. As Engelhart points out, there are several levels of state incentives for these procedures, ranging from i) *pure self-regulation* (level 1), in which there is no public incentive, with the adoption of these programs being a mere option marked by market interests, up to a possible vi) *general obligation to implement compliance programs* (level 6). However, at intermediate levels, there are still very relevant incentives, which are certainly considered by corporations when deciding whether or not to promote a compliance program and an internal investigation. In addition to ii) *public informal support* (level 2), with the promotion of courses and training programs, Engelhart identifies: iii) *rewards for compliance*, through non-prosecution agreements and penalty reductions, for example (level 3); iv) *punishment for failures or lack of*

of compliance programs (especially in their aspect of collaboration with the state), without disregarding the rights to due process and contradictory of the affected subjects[105]-[106]. Proposing this solution, Anna Carolina

---

compliance, through the aggravation of penalties or even the judicial determination of the implementation or correction of a compliance program (level 4); and v) *exclusion of corporate criminal liability for the adoption of effective compliance programs* (level 5). See: ENGELHART, Marc. *The Nature and Basic Problems of Compliance Regimes*. Freiburg im Breisgau: Max-Planck-Institut für ausländisches und internationales Strafrecht, 2018. p. 21-30. In practice, therefore, cases in which there will be no incentive for these procedures will be very rare, if not non-existent, which would result, therefore, that any and all elements of information arising from these investigations would be inadmissible.

[105] JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., p. 1483-1484; JANUÁRIO, Túlio Felipe Xavier. Inteligencia artificial y..., forthcoming.

[106] A different solution is proposed by Hernandez Colomer. The author classifies CII as *preventive investigations* (daily supervision of the company and of the compliance program); *confirmatory investigations* (to prove or clarify facts identified in the scope of preventive investigations) and *defensive investigations* (carried out after the beginning of the state procedures, for the purpose of defending the legal entity). For the author, preventive investigations, carried out based on the directive power of the employer, admit greater violations of fundamental rights of the employee, but the elements of information obtained from them should not be admitted in criminal proceedings. On the other hand, the elements of information obtained through confirmatory or defensive investigations, have much narrower limits of violation of employee rights. However, in case of violation of these rights, they cannot be accepted either, as there is a link between the business activity of investigation and the state's interest on investigating the facts. See in detail at: COLOMER HERNÁNDEZ, Ignacio. Derechos fundamentales y valor probatorio en el proceso penal de las evidencias obtenidas en investigaciones internas en un sistema de compliance. In: GÓMEZ COLOMER, Juan-Luis (dir.); MADRID-BOQUÍN, Christa M. (coord.). *Tratado sobre compliance penal:* responsabilidad penal de las personas jurídicas y modelos de organización y gestión. Valencia: Tirant lo Blanch, 2019. p. 609-652. Although this is a very interesting and well-founded option, we disagree on some points. Initially, we understand that the day-to-day supervision of the company cannot be considered an investigation itself. However, our main question regarding this position concerns its practical consequences related to the evidentiary admissibility in criminal proceedings. Although we agree with the premise that there are different limits to be observed when dealing with daily supervision activities or CII, we understand that any inadmissibility of any and all information arising from what the author calls "preventive investigations" would be easily circumvented in practice, by, for example, subpoenaing the compliance officer as a witness in court, or requesting expert examination

---

Canestraro explains that the sharing of information from CII with the criminal procedure must be subject to a new judgment of legality and proportionality, which is usually positive (with the exception of interview reports)[107]. However, since they have not been produced under contradictory, these elements themselves cannot justify a conviction, being sufficient only to form the *opinio delicti* of the Public Prosecution, in a regime similar to that of state investigation acts[108].

iii) finally, as a result of the two premises mentioned above, we maintain that the elements of information presented and admitted as defensive evidence of the company cannot be valued for the purpose of substantiating the conviction of another defendant. The solution to this impasse, in our view, lies between two alternatives: i) the first of them, supported by the majority doctrine[109], would be to consider that, even though natural and legal persons enjoy the right of defense and procedural guarantees related to it, they would not necessarily have the same "weight" for both. That is, in case of conflict between the rights of defense of natural and legal persons, the ones of natural persons

---

on digital files of the company. Once public and private investigators already know what exactly to look for, it is very simple to collect other elements of information that prove the fact.

[107] The author understands that the repetition in court of the hearing of the people interviewed in the scope of CII would not result in any loss in terms of effectiveness of the verification of the facts, in addition to ensuring the rights of the interviewee in a more incisive way. Therefore, she understands that, within the scope of the proportionality test, sharing the interview report with the criminal procedure does not meet the requirement of *necessity*, and is, therefore, not admissible. See: CANESTRARO, Anna Carolina. *As investigações internas...*, p. 93-94. See also: ROXIN, Imme. Problemas e estratégias da consultoria de compliance em empresas. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 23, n. 114, p. 321-339, mai./jun. 2015. p. 334.

[108] CANESTRARO, Anna Carolina. *As investigações internas...*, p. 95ff; CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e..., p. 384.

[109] In this sense: BRODOWSKI, Dominik. Minimum Procedural Rights for Corporations in Corporate Criminal Procedure. In: BRODOWSKI, Dominik et. al. (eds.). *Regulating Corporate Criminal Liability.* Cham: Springer, 2014. p. 211-225. p. 219-221; ANTUNES, Maria João. Privatização das investigações..., p. 126-127. For a detailed analysis of the legal person's procedural rights and guarantees, see: ANTUNES, Maria João. *Processo penal e pessoa coletiva arguida.* Coimbra: Almedina, 2020. p. 45ff.

would have primacy. The foundations for this position would be: due to the nature of legal persons, their fundamental rights would admit some relativizations; some procedural rights are linked not only to the guarantees directly related to equality of arms in criminal proceedings, but also to the dignity of the human person, which does not extend to legal persons[110]. II) The second possibility, which in our opinion would be the most appropriate, would be the use of the faculty provided for by some legal systems, that is, the separation of processes. This is the case, for example, of the Brazilian legal system, which allows the judge, in Art. 80 CPP[111], the separation of processes when deemed convenient for a relevant reason[112].

It is clear that, assuming the admission of these elements of information in the criminal procedure, in no way hinders the imperious judgments about their credibility within the scope of their valuation. Even because, as we have already pointed out throughout the paper, AI systems pose some challenges in terms of transparency and, consequently, contestability of their decisions. If we think of their application in the most varied functions of CII, we tend to have an environment of even greater difficulties for the exercise of the defense of those affected by these elements of information, even if a contradictory *a posteriori* is assured.

As we have already argued on other occasions[113], due to the questions that are raised around the integrity, identity and authenticity of digital evidence[114] obtained with some form of AI intervention, it is essential, also within the scope of CII, to document the chain of custody,

---

[110] On this distinction, see: NEIRA PENA, Ana María. *La instrucción de...*, p. 235ff.

[111] BRASIL. *Decreto-Lei nº 3.689, de 3 de outubro de 1941*: Código de Processo Penal. Available on: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Accessed on March 07th, 2023.

[112] JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., p. 1483-1484; JANUÁRIO, Túlio Felipe Xavier. Inteligencia artificial y..., forthcoming.

[113] JANUÁRIO, Túlio Felipe Xavier. Cadeia de custódia..., passim; JANUÁRIO, Túlio Felipe Xavier. Inteligencia artificial y..., forthcoming.

[114] On the topic of the chain of custody of digital evidence, see: BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, ano 29, n. 343, p. 7-9, jun./2021; PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. 2.ed. São Paulo: Marcial Pons, 2021. p. 173ff.

as it can prove to be the only way to attest to the legitimacy and legality of the elements collected in CII, preventing them from being excluded from the process. It is true, however, that despite the models and procedures proposed by international certification institutes[115], for the purpose of documenting the chain of custody of digital evidence, further investigations are still pending on the extent to which these models will be suitable for evidence related to AI[116].

CONCLUSION

As demonstrated, CII emerge, along with compliance programs, not only as one of the possible tools for tackling corporate crimes, but also as an important mechanism of legal entities' defense, when subject to criminal prosecution. In order to achieve these purposes and effectively and efficiently perform the tasks included therein, new technologies such as AI have been progressively employed, and it is expected that their use will help in the best and most accurate verification of facts in a shorter time and with less expenditure of companies' financial and human resources. However, in view of their limitations and especially the risks derived from them, it is essential to observe legal limits, not only in the use of these technologies, but also in the sharing with criminal procedures, of information obtained with them in the scope of CII.

In light of these considerations, we demonstrated that the processing of data as input for AI systems applied in CII must find legal support in one of the hypotheses provided for by legislation. The ones that are generally selected are those provided for by Article 7th, items I, II, VII or IX and Article 11, items I and II, "a" and "d" of the LGPD

---

[115] See, for example: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. *Guide to Integrating Forensic Techniques into Incident Response*: Recommendations of the National Institute of Standards and Technology. 2006.

[116] JANUÁRIO, Túlio Felippe Xavier. Inteligencia artificial y..., forthcoming. On evidentiary difficulties in the field of AI, see: FIDALGO, Sónia. A utilização da inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo. In: RODRIGUES, Anabela Miranda. *Inteligência artificial no direito penal*. Coimbra: Almedina, 2020. p. 129-162.

or, when applicable the GDPR, those provided for by Article 6, items (a), (c), (e) or (f) and Article 9(2), items (a) and (f). In addition, the fundamental principles for data processing and the test of proportionality between the intended purpose and the intervention that is carried out must be observed.

Even if the issue of data processing is overcome, the actual use of AI systems in CII must also observe limits. Although, in terms of *legality*, these systems usually find support in the norms that underlie the employer's directive power, it is also imperative that their application does not affect areas in which there are (and which have not been withdrawn) expectations of privacy by the employee and, once more, it must be observed a test of proportionality between the intended purpose and the technology concretely employed and the rights affected by it.

In criminal procedural terms, however, remains the tormenting question of knowing to what extent the use of AI in CII affects the admissibility and valuation of evidence in criminal proceedings. In our view, the sharing in question may represent a misuse of purpose for which the data were originally collected. If that is the case, and therefore there is a new intervention, sharing will depend, in order to comply with the requirement of *legality*, on legal authorization for sharing with the public authority in question and on legal authorization for this authority to receive these data. Furthermore, this sharing will only be admissible if the authority in question has powers to, hypothetically, collect these information under the same terms in which it was collected by the company, including with regard to the gravity of the means employed.

With regard to the admissibility in criminal proceedings of elements of information collected in CII, we maintain that they can be presented by the company, in its defense, and by the Prosecution itself, when there has been a prior sharing, provided that a new proportionality test has been overcome. However, these elements of information cannot be considered sufficient for the conviction of the company, nor for proof of guilt of other co-defendants, having probative value similar to that of the elements of information arising from acts of state investigation, such as police investigations. In addition, if the company and individual persons investigated in the scope of the CII are co-defendants, it may be beneficial to separate the procedures in order to better protect both

the right of defense of the legal entity and the procedural guarantees of the individual.

We agree that this is a complex proposal and that it tends to impose some practical difficulties in the investigation and processing of legal entities. However, we believe it is an imperative solution in view of the interests at stake, which tend to be even at higher risk when related to interventions by AI systems.

REFERENCES

AGAPITO, Leonardo Simões; MIRANDA, Matheus de Alencar e; JANUÁRIO, Túlio Felippe Xavier. On the Potentialities and Limitations of Autonomous Systems in Money Laundering Control. *RIDP*, v. 92, n. 1, p. 87-108, 2021.

AGAPITO, Leonardo Simões; MIRANDA, Matheus de Alencar e; JANUÁRIO, Túlio Felippe Xavier. Underneath the Robot Judge's Robe: demystifying the use of artificial intelligence in criminal justice through a global south perspective. In: KOSTIĆ, Jelena; BOŠKOVIĆ, Marina Matić. *Digitalizacija u kaznenom pravu i pravosudu*: Digitalization in Penal Law and Judiciary. Belgrade: IKSI, 2022. p. 271-289. https://doi.org/10.56461/ZR_22.DUKPP.20.

ALCÁCER GUIRAO, Rafael. Investigaciones internas: prolegómenos constitucionales y cuestiones abiertas. In: GÓMEZ MARTÍN, Víctor et al (dir.). *Un modelo integral de Derecho penal:* Libro homenaje a la profesora Mirentxu Corcoy Bidasolo. Madrid: BOE, 2022. p. 989-1000. Available on: <https://www.boe.es/biblioteca_juridica/publicacion.php?id=PUB-DP-2022-246>. Accessed on March 25th, 2023.

ANTUNES, Maria João. Privatização das investigações e compliance criminal. *Revista Portuguesa de Ciência Criminal*, Coimbra, ano 28, n. 1, p. 119-128, jan./abr. 2018.

ANTUNES, Maria João. *Processo penal e pessoa coletiva arguida.* Coimbra: Almedina, 2020.

ARTICLE 29 WORKING PARTY. *Guidelines on consent under Regulation 2016/679:* Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2018. Available on: <https://ec.europa.eu/newsroom/article29/items/623051>. Accessed on March 10th, 2023.

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, ano 29, n. 343, p. 7-9, jun./2021.

BADARÓ, Gustavo Henrique. *Processo penal.* 8.ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020.

BALCARCE, Fabián I.; BERRUEZO, Rafael. *Criminal compliance y personas jurídicas.* Buenos Aires: Editorial B de F, 2016.

BARONA VILAR, Silvia. *Algoritmización del derecho y de la justicia:* de la inteligencia artificial a la Smart Justice. Valencia: Tirant lo Blanch, 2021.

BARRILARI, Claudia Cristina. *Crime empresarial, autorregulação e compliance.* 2. ed. atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021. Ebook.

BARROS, Alice Monteiro. *Curso de direito do trabalho.* 7. ed. São Paulo: LTr, 2011.

BASAR, Eren. Anforderungen an die digitale Beweissicherung im Strafprozessrecht und in internen Untersuchungen. In: AHLBRECHT, Heiko et al (Hrsg.). *Unternehmensstrafrecht:* Festschrift für Jürgen Wessing zum 65. Geburtstag. München: C. H. Beck, 2016. p. 635-647.

BOTTINI, Pierpaolo Cruz. Programas de compliance voltados à prevenção da lavagem de dinheiro. In: BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. *Lavagem de dinheiro:* aspectos penais e processuais penais: comentários à Lei 9.613/1998, com alterações da Lei 12.683/2012. 4.ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. p. 47-71.

BRODOWSKI, Dominik. Minimum Procedural Rights for Corporations in Corporate Criminal Procedure. In: BRODOWSKI, Dominik et. al. (eds.). *Regulating Corporate Criminal Liability.* Cham: Springer, 2014. p. 211-225. https://doi.org/10.1007/978-3-319-05993-8_17.

BURCHARD, Christoph. Das »Strafrecht« der Prädiktionsgesellschaft: ...oder wie »smarte« Algorithmen die Strafrechtspflege verändern (könnten). *Forschung Frankfurt: das Wissenschaftsmagazin: Recht und Gesetz*, n. 1, p. 27-31, Aug./2020. Available on: <https://publikationen.ub.uni-frankfurt.de/frontdoor/index/index/year/2020/docId/55171>. Accessed on March 25th, 2023.

BURCHARD, Christoph. Digital Criminal Compliance. In: ENGELHART, Marc et al (Hrsg.). *Digitalisierung, Globalisierung und Risikoprävention:* Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II. Berlin: Duncker & Humblot, 2021. p. 741-756.

BURRELL, Jenna. How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. *Big Data & Society,* v. 3, n. 1, p. 1-12, jan./jun. 2016. https://doi.org/10.1177/20539517156225.

CANESTRARO, Anna Carolina. *As investigações internas no âmbito do criminal compliance e os direitos dos trabalhadores*: considerações sobre a possibilidade de investigar e a transferência de informações para o processo penal. São Paulo:

IBCCRIM, 2020. Available on: <https://ibccrim.org.br/publicacoes/exibir/58/as-investigacoes-internas-no-ambito-do-criminal-compliance-e-os-direitos-dos-trabalhadores>. Accessed on March 25th, 2023.

CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Beyond Ecocide: Extraterritorial Obligations of Due Diligence as an Alternative to Address Transnational Environmental Damages?. *RIDP*, v. 93, n. 1, p. 231-250, 2022.

CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Dos níveis de exigibilidade dos procedimentos de investigação interna. In: INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS. *Anais do CPCRIM*: IV Congresso de Pesquisas em Ciências Criminais, de 21 a 23 de outubro de 2020. São Paulo: IBCCRIM, 2020. p. 215-237. Available on: <https://ibccrim.org.br/publicacoes/exibir/734>. Accessed on May 27th, 2023.

CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal. In: D'ÁVILA, Fábio Roberto; AMARAL, Maria Eduarda Azambuja (eds.). *Direito e Tecnologia*. Porto Alegre: Citadel, 2022. p. 363-392.

CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe X. Investigação defensiva corporativa: um estudo do Provimento 188/2018 e de sua eventual aplicação para as investigações internas de pessoas jurídicas. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 6, n. 1, p. 283-328, jan./abr. 2020. https://doi.org/10.22197/rbdpp.v6i1.324.

CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felippe Xavier. Programas de compliance e branqueamento de capitais: implicações da lei nº 83/2017, de 31 de agosto, no regime jurídico de Portugal. *Revista Científica do CPJM*, v. 1, n. 3, p. 65-98, 2022. Available on: <https://rcpjm.cpjm.uerj.br/revista/article/view/61>. Accessed on May 27th, 2023.

CARDOSO, Débora Motta. *Criminal compliance na perspectiva da lei de lavagem de dinheiro*. São Paulo: LiberArs, 2015.

COLOMER HERNÁNDEZ, Ignacio. Derechos fundamentales y valor probatorio en el proceso penal de las evidencias obtenidas en investigaciones internas en un sistema de compliance. In: GÓMEZ COLOMER, Juan-Luis (dir.); MADRID-BOQUÍN, Christa M. (coord.). *Tratado sobre compliance penal:* responsabilidad penal de las personas jurídicas y modelos de organización y gestión. Valencia: Tirant lo Blanch, 2019. p. 609-652.

CORRALES, Marcelo; FENWICK, Mark; HAAPIO, Helena. Digital Technologies, Legal Design and the Future of the Legal Profession. In: CORRALES, Marcelo;

FENWICK, Mark; HAAPIO, Helena (ed.). *Legal Tech, Smart Contracts and Blockchain.* Singapore: Springer, 2019. https://doi.org/10.1007/978-981-13-6086-2.

DEARDEN, Lizzie. The Telegraph Backtracks on Sensors Monitoring Whether Journalists are Sitting at Desks Amid Outrage. *The Independent*, Jan./2016. Available on: <https://www.independent.co.uk/news/ media/the-telegraph-backtracks-on-sensors-monitoring-whether-journalists-are-sitting-at-desks-amidoutrage-a6807336.html>. Accessed on June 21st, 2021.

DE HOYOS SANCHO, Montserrat. El Libro Blanco sobre Inteligencia Artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como "sector de riesgo". *Revista Española de Derecho Europeo,* n. 76, p. 9-44, Oct./Dec. 2020. https://doi.org/10.37417/REDE/num76_2020_534.

DE HOYOS SANCHO, Montserrat. El uso jurisdiccional de los sistemas de inteligencia artificial y la necesidad de su armonización en el contexto de la Unión Europea. *Revista General de Derecho Procesal*, n. 55, p. 1-29, 2021. Available on: < https://www.uv.es/medarb/publicacions/2021/2021-rgdp.pdf>. Accessed on March 25th, 2023.

DELGADO, Maurício Godinho. *Curso de direito do trabalho*. 11. ed. São Paulo: LTr, 2012.

ENGELHART, Marc. *Sanktionierung von Unternehmen und Compliance*: eine rechtsvergleichende Analyse des Straf- und Ordnungswidrigkeitenrechts in Deutschland und den USA. 2. ergänzte und erweiterte Auflage. Berlin: Dunker & Humblot, 2012.

ENGELHART, Marc. *The Nature and Basic Problems of Compliance Regimes*. Freiburg im Breisgau: Max-Planck-Institut für ausländisches und internationales Strafrecht, 2018. https://doi.org/10.30709/archis-2018-3

ESTRADA I CUADRAS, Albert; LLOBET ANGLÍ, Mariona. Derechos de los trabajadores y deberes del empresario: conflicto en las investigaciones empresariales internas. In: SILVA SÁNCHEZ, Jesús-María (dir.); MONTANER FERNÁNDEZ, Raquel (coord.). *Criminalidad de empresa y compliance: prevención y reacciones corporativas.* Barcelona: Atelier, 2013. p. 197-228.

FERNANDES, Fernando Andrade. Brasil. In: RODRÍGUEZ-GARCÍA, Nicolás (dir.); ONTIVEROS ALONSO, Miguel; ORSI, Omar Gabriel; RODRÍGUEZ-LÓPEZ, Fernando (coord.). *Tratado angloiberoamericano sobre compliance penal.* Valencia: Tirant lo Blanch, 2021. p. 155-241.

FIDALGO, Sónia. A utilização da inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo. In: RODRIGUES, Anabela Miranda. *Inteligência artificial no direito penal*. Coimbra: Almedina, 2020. p. 129-162.

GALEGO SOLER, José-Ignácio. Investigaciones internas corporativas: de la práctica a la teoría. In: GÓMEZ MARTÍN, Víctor et al (dir.). *Un modelo integral de Derecho penal:* Libro homenaje a la profesora Mirentxu Corcoy Bidasolo. Madrid: BOE, 2022. p. 1150-1165. Available on: <https://www.boe.es/biblioteca_juridica/publicacion.php?id=PUB-DP-2022-246>. Accessed on March 25th, 2023.

GARCÍA CAVERO, Percy. *Criminal compliance.* Lima: Palestra Editores, 2014.

GARCÍA-MORENO, Beatriz. *Del whistleblower al alertador*: la regulación europea de los canales de denuncia. Valencia: Tirant lo Blanch, 2020

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública.* Rio de Janeiro: Marcial Pons, 2021.

GLESS, Sabine. AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials. *Georgetown Journal of International Law,* v. 51, n. 2, p. 195-253, 2020. Available on: <https://ssrn.com/abstract=3602038>. Accessed on June 15th, 2021.

GÓMEZ COLOMER, Juan-Luis. Derechos fundamentales, proceso e Inteligencia Artificial: una reflexión. In: CALAZA LÓPEZ, Sonia; LLORENTE SÁNCHEZ-ARJONA, Mercedes (dir.). *Inteligencia artificial legal y administración de justicia*. Cizur Menor: Aranzadi, 2022. p. 257-287.

GÓMEZ MARTÍN, Victor. Compliance y derecho de los trabajadores. In: KUHLEN, Lothar; MONTIEL, Juan Pablo; DE URBINA GIMENO, Íñigo Ortiz (eds.). *Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 125-146.

GÓMEZ MARTÍN, Víctor. ¿Un nuevo golpe de gracia a las investigaciones internas corporativas? Reflexiones en voz alta sobre la sentencia de tribunal supremo 328/2021, de 22 de marzo. In: GÓMEZ MARTÍN, Víctor et al (dir.). *Un modelo integral de Derecho penal*: Libro homenaje a la profesora Mirentxu Corcoy Bidasolo. Madrid: BOE, 2022. p. 1167-1178.

GRECO, Luís; CARACAS, Christian. Internal investigations e o princípio da não auto-incriminação. In: LOBATO, José Danilo Tavares et al (orgs.). *Comentários ao direito penal econômico brasileiro.* Belo Horizonte: D'Plácido, 2018. p. 787-820.

HILGENDORF, Eric. Recht und autonome Maschinen – ein Problemaufriβ. In: HILGENDORF, Eric; HÖTITZSCH, Sven (eds.). *Das Recht vor den Herausforderungen der modernen Technik.* Baden-Baden: Nomos 2015. p. 11-40.

INDERST, Cornelia. Einzelaufgaben der Compliance-Organisation. In: GÖRLING, Helmut et al. *Compliance:* Aufbau – Management – Risikobereiche. Hamburg: C.F. Müller, 2010. p. 112-122.

JANUÁRIO, Túlio Felippe Xavier. Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 7, n. 2, p. 1453-1510, mai./ago. 2021. https://doi.org/10.22197/rbdpp.v7i2.453.

JANUÁRIO, Túlio Felippe Xavier. Considerações preambulares acerca das reverberações da inteligência artificial no direito penal. In: COMÉRIO, Murilo Siqueira; JUNQUILHO, Tainá Aguiar (orgs.). *Direito e tecnologia:* um debate multidisciplinar. Rio de Janeiro: Lumen Juris, 2021. p. 295-314.

JANUÁRIO, Túlio Felippe Xavier. *Criminal compliance e corrupção desportiva*: um estudo com base nos ordenamentos jurídicos do Brasil e de Portugal. Rio de Janeiro: Lumen Juris, 2019.

JANUÁRIO, Túlio Felippe Xavier. 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. *Revista Brasileira de Ciências Criminais,* ano 29, n. 186, p. 127-173, Dec./2021.

JANUÁRIO, Túlio Felippe Xavier. Inteligência artificial e responsabilidade penal no setor da medicina. *Lex Medicinae:* Revista Portuguesa de Direito da Saúde, ano 17, n. 34, p. 37-63, jul./dez. 2020. Available on: <http://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas>. Accessed on May 27th, 2023.

JANUÁRIO, Túlio Felippe Xavier. Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales. *Estudios Penales y Criminológicos,* Santiago de Compostela, forthcoming.

JANUÁRIO, Túlio Felippe Xavier. O ônus da prova da existência e eficácia dos programas de compliance no âmbito do processo penal das pessoas jurídicas: um estudo com base no ordenamento jurídico espanhol. *Revista Brasileira de Ciências Criminais*, São Paulo, ano 27, n. 160, p. 219-257, out./ 2019.

JANUÁRIO, Túlio Felippe Xavier. O sigilo profissional no âmbito das pessoas jurídicas: um estudo da particular posição dos in-house lawyers e dos advogados de compliance e de investigações internas. *Revista Brasileira de Ciências Criminais*, São Paulo, ano 27, n. 159, p. 297-339, set./2019.

JANUÁRIO, Túlio Felippe Xavier. Vulnerabilidad e hiposuficiencia 4.0: la protección jurídico-penal de los consumidores en la era de la inteligencia artificial. In: FONTESTAD PORTALÉS, Leticia (dir.), PÉREZ TORTOSA, Francesc. (coord.). *La justicia en la sociedad 4.0:* nuevos retos para el siglo XXI. A Coruña: Editorial Colex, 2023. p. 187-199. Available on: <https://www.colexopenaccess.com/libros/justicia-sociedad-4-0-nuevos-retos-siglo-xxi-3669>. Accessed on May 27th, 2023.

JANUÁRIO, Túlio Xavier. Inteligência artificial e direito penal da medicina. In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal*, volume II. Coimbra: Almedina, 2022. p. 125-174.

JANUÁRIO, Túlio Xavier. Veículos autónomos e imputação de responsabilidades criminais por acidentes. In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal.* Coimbra: Almedina, 2020. p. 95-128.

LAUFER, William S. Corporate Liability, Risk Shifting, and the Paradox of Compliance. *Vanderbilt Law Review*, v. 52, n. 5, p. 1343-1420, out./1999. Available on: <https://scholarship.law.vanderbilt.edu/vlr/vol52/iss5/9>. Accessed on June 29th, 2020.

LEÓN ALAPONT, José. *Canales de denuncia e investigaciones internas en el marco del compliance penal corporativo.* Valencia: Tirant lo Blanch, 2023.

LEÓN ALAPONT, José. Medios de tecnovigilancia e investigaciones internas en el ámbito empresarial: algunas consideraciones sobre la tutela penal y procesal del secreto de las comunicaciones la intimidad (¿derechos negociables?). In: ROPERO CARRASCO, Julia (coord.). *Aspectos jurídicos de actualidad en el ámbito del derecho digital.* Valencia: Tirant lo Blanch, 2023. p. 114-141.

LOPES JR., Aury. *Direito processual penal.* 19. ed. São Paulo: SaraivaJur, 2022.

LUZ, Ilana Martins. *Compliance & omissão imprópria*. 3. Reimp. Belo Horizonte: D'Plácido, 2021.

MASCHMANN, Frank. Compliance y derechos del trabajador. In: KUHLEN, Lothar et al. (eds.). *Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 147-167.

MCCARTHY, John et al. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine*, v. 27, n. 4, p. 12-14, 2006. https://doi.org/10.1609/aimag.v27i4.1904.

MCCARTHY, John. *What is Artificial Intelligence?.* Stanford: Stanford University, 2007. Available on: <http://jmc.stanford.edu/artificial-intelligence/index.html>. Accessed on July 20th, 2020.

MIRANDA, Matheus de Alencar e; JANUÁRIO, Túlio Felippe Xavier. Novas tecnologias e justiça criminal: a tutela de direitos humanos e fundamentais no âmbito do direito penal e processual penal. In: MOREIRA, Vital et. al. (orgs.). *Temas de Direitos Humanos do VI CIDH Coimbra 2021*. Campinas/Jundiaí: Brasílica/Edições Brasil, 2021, p. 284-298. Available on: <https://www.cidhcoimbra.com/anais>. Accessed on May 27th, 2023.

MIRANDA, Matheus de Alencar e. *Técnica, decisões automatizadas e responsabilidade penal.* 2023. Tese - (Doutorado em Direito). Rio de Janeiro: Universidade do Estado do Rio de Janeiro, 2023.

MIRÓ LLINARES, Fernando. Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología,* 3. época, n. 20, p. 87-130, Jul./2018. https://doi.org/10.5944/rdpc.20.2018.26446.

MOMSEN, Carsten. Internal Investigations zwischen arbeitsrechtlicher Mitwirkungspflicht und strafprozessualer Selbstbelastungsfreiheit. *Zeitschrift für Internationale Strafrechtsdogmatik*, n. 6, p. 508-516, 2011. Available on: <https://www.zis-online.com/dat/artikel/2011_6_586.pdf>. Accessed on March 25th, 2023.

MONTIEL, Juan Pablo. Autolimpieza empresarial: compliance programs, investigaciones internas y neutralización de riesgos penales. In: KUHLEN, Lothar; MONTIEL, Juan Pablo; DE URBINA GIMENO, Íñigo Ortiz (eds.). *Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 221-243.

MONTIEL, Juan Pablo. Sentido y alcance de las investigaciones internas en la empresa. *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, v. XL, p. 251-277, 2013. http://dx.doi.org/10.4067/S0718-68512013000100008.

MOORE, Phoebe V.. *The Threat of Physical and Psychosocial Violence and Harassment in Digitalized Wor*k. Geneva: International Labour Office. Bureau for Workers' Activities, 2018. Available on: <https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---actrav/documents/publication/wcms_617062.pdf>. Accessed on June 24th, 2021.

MOOSMAYER, Klaus. Investigaciones internas: una introducción a sus problemas esenciales. In: ARROYO ZAPATERO, Luis; NIETO MARTÍN, Adán (dir.). *El derecho penal económico en la era compliance.* Valencia: Tirant lo Blanch, 2013. p. 137-144.

NASCIMENTO, Amauri Mascaro; NASCIMENTO, Sônia Mascaro. *Curso de direito do trabalho.* São Paulo: Saraiva, 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. *Guide to Integrating Forensic Techniques into Incident Response*: Recommendations of the National Institute of Standards and Technology. 2006. Available on: <https://csrc.nist.gov/publications/detail/sp/800-86/final>. Accessed on June 27th, 2020.

NEIRA PENA, Ana María. *La instrucción de los procesos penales frente a las personas jurídicas.* Valencia: Tirant lo Blanch, 2017.

NIETO MARTÍN, Adán. Como avaliar a efetividade dos programas de cumprimento?. In: NIETO MARTÍN, Adán; SAAD-DINIZ, Eduardo (org.). *Legitimidade e efetividade dos programas de compliance.* São Paulo: Tirant lo Blanch, 2021. p. 6-26.

NIETO MARTÍN, Adán. El cumplimiento normativo. In: NIETO MARTÍN, Adán et al. (dir.). *Manual de cumplimiento penal en la empresa.* Valencia: Tirant lo Blanch, 2015. p. 25-48.

NIETO MARTÍN, Adán. Investigaciones internas. In: NIETO MARTÍN, Adán et al. (dir.). *Manual de cumplimiento penal en la empresa.* Valencia: Tirant lo Blanch, 2015. p. 231-271.

NIEVA FENOLL, Jordi. *Inteligencia artificial y proceso judicial.* Madrid: Marcial Pons, 2018.

OIT. *Trabalho em tempos de COVID*: Relatório do diretor-geral, Conferência Internacional do Trabalho, 109ª sessão, Genebra, 2021.

PALHARES, Felipe; PRADO, Fernando; VIDIGAL, Paulo. Compliance Digital e LGPD. In: NOHARA, Irene Patrícia Diom; ALMEIDA, Luís Eduardo de (coord.). *Coleção compliance, v. 5.* São Paulo: Thomson Reuters Brasil, 2021. Ebook.

PEIXOTO, Fabiano Hartmann; SILVA, Roberta Zumblick Martins. *Inteligência artificial e direito*, Curitiba: Alteridade Editora, 2019.

PELZ, Christian. Offenbarungs- und Meldepflichten bei Internal Investigations. In: AHLBRECHT, Heiko et al (Hrsg.). *Unternehmensstrafrecht:* Festschrift für Jürgen Wessing zum 65. Geburtstag. München: C. H. Beck, 2016. p. 605-624.

PRADO, Geraldo. *A cadeia de custódia da prova no processo penal.* 2.ed. São Paulo: Marcial Pons, 2021.

QUATTROCOLO, Serena. *Artificial Intelligence, Computational Modelling and Criminal Proceedings*: A Framework for a European Legal Discussion. Cham: Springer Nature Switzerland AG, 2020. https://doi.org/10.1007/978-3-030-52470-8.

RODRIGUES, Anabela Miranda. *Direito penal económico:* uma política criminal na era compliance. 2.ed. Coimbra: Almedina, 2020.

RODRIGUES, Anabela Miranda. Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização. In: RODRIGUES, Anabela Miranda (coord.). *A Inteligência Artificial no Direito Penal, vol. 1.* Coimbra: Almedina, 2020, p. 11-58.

RODRIGUES, Anabela Miranda; SOUSA, Susana Aires de. Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal. In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal,* vol. II. Coimbra: Almedina, 2022. p. 11-39.

ROXIN, Imme. Problemas e estratégias da consultoria de compliance em empresas. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 23, n. 114, p. 321-339, mai./jun. 2015.

SAAD-DINIZ, Eduardo. Ética negocial e *compliance*: entre a educação executiva e a interpretação judicial. São Paulo: Thomson Reuters Brasil, 2019.

SAAVEDRA, Giovani Agostini. Panorama do compliance no Brasil: avanços e novidades. In: NOHARA, Irene Patrícia; PEREIRA, Flávio de Leão Bastos (coord.). *Governança, compliance e cidadania.* São Paulo: Thomson Reuters Brasil, 2018. p. 37-50.

SAHAN, Oliver. Investigaciones empresariales internas desde la perspectiva del abogado. In: KUHLEN, Lothar; MONTIEL, Juan Pablo; DE URBINA GIMENO, Íñigo Ortiz (eds.). *Compliance y teoría del derecho penal.* Madrid: Marcial Pons, 2013. p. 245-259.

SANTOSUOSSO, Amedeo; BOTTALICO, Barbara. Autonomous Systems and the Law: Why Intelligence Matters. In: HILGENDORF, Eric; SEIDEL, Uwe (eds.). *Robotics and the Law*: Legal Issues Arising from Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy. Baden-Baden: Nomos, 2017. p. 27-58.

SCHUH, Günther et al (eds.). *Industrie 4.0 Maturity Index:* Managing the Digital Transformation of Companies: Update 2020. München: Acatech Study, 2020. Available on: <http://www.acatech.de/publikationen>. Accessed on May 27th, 2023.

SHABBIR, Jahanzaib; ANWER, Tarique. Artificial intelligence and its role in near future. *Journal of Latex Class Files*, v. 14, n. 8, p. 1-11, Aug./2015. https://doi.org/10.48550/arXiv.1804.01396.

SIEBER, Ulrich. Compliance-Programme im Unternehmensstrafrecht: ein neues Konzept zur Kontrolle von Wirtschaftskriminalität. In: SIEBER, Ulrich et al. (Hrsg.). *Strafrecht und Wirtschaftsstrafrecht – Dogmatik, Rechtsvergleich, Rechtstatsachen*: Festschrift für Klaus Tiedemann zum 70. Geburtstag. Köln: Carl Heymanns Verlag, 2008. p. 449-484.

SILVA, Douglas Rodrigues da. *Investigações corporativas e processo penal:* uma análise sobre os limites da licitude da prova. Londrina: Thoth, 2021. Ebook. N.P.

SILVA SÁNCHEZ, Jesús María. *Fundamentos del derecho penal de la empresa*. Madrid: Edisofer, 2013

SILVEIRA, Renato de Mello Jorge. Autorregulação, responsabilidade empresarial e criminal compliance. In: SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. *Compliance, direito penal e lei anticorrupção*. São Paulo: Saraiva, 2015. p. 25-239.

SOUSA, Susana Aires de. "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial". In: RODRIGUES, Anabela Miranda (coord.). *A inteligência artificial no direito penal*. Coimbra: 2020. p. 59-94.

SOUSA, Susana Aires de. *Questões fundamentais de direito penal da empresa.* 2. ed. Coimbra: Almedina, 2023.

THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE: *A Definition of AI: Main Capabilities and Scientific Disciplines: Definition Developed for the Purpose of the Deliverables of the High-Level Expert Group*, Brussels, 2018.

TRENTMANN, Christian H. W.. *Wahrheitsdetektionssyteme mit künstlicher Intelligenz:* ein neues Legal-Tech-Modell für Internal Investigations. Baden-Baden: Tectum Verlag, 2022.

VALENTE, Victor Augusto Estevam. *A proteção de dados pessoais no direito penal:* uma análise crítica da criminalização nas perspectivas constitucional e de política criminal. Belo Horizonte: D'Plácido, 2022.

VALENTE, Victor Augusto Estevam. *Inteligência artificial e o direito penal*: a propósito da responsabilidade criminal em decorrência de sistemas tecnológicos altamente complexos nas empresas. Belo Horizonte: D'Plácido, 2023.

VASCONCELLOS, Vinicius Gomes de. "The Right to Counsel and the Protection of Attorney-Client Privilege in Criminal Proceedings": direito de defesa técnica e relações cliente-advogado no processo penal contemporâneo. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 29, n. 176, p. 257-272, fev./2021.

VERIATO. *Employee Monitoring & Insider Threat Detection Software*: see and understand exactly what your employees are doing. Available on: <https://www.veriato.com/>. Accessed on June 22nd, 2021.

VERÍSSIMO, Carla. *Compliance*: incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva: 2017.

VERITONE. *Making the AI revolution work for you.* Available on: <https://www.veritone.com/>. Accessed on June 22nd, 2021.

WIMMER, Miriam. Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios. In: LIMA, Ana Paula Canto de; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes (eds), *Direito Digital:* Debates Contemporâneos, São Paulo: Thomson Reuters Brasil, 2019. Ebook. N. P. Chapter 1.

Authorship information

Túlio Felipe Xavier Januário. PhD Candidate in Law at the University of Coimbra (Portugal), with a fellowship from the Fundação para a Ciência e a Tecnologia – FCT. M.Sc. in Law by the University of Coimbra (Portugal), with a research internship of the "ERASMUS+" Program at the Georg-August-Universität Göttingen (Germany). He had Graduate Studies in International Criminal Law at the Siracusa International Institute for Criminal Justice and Human Rights (Italy), Graduate Studies in Economic Criminal Law and Crime's Theory at the University of Castilla-La Mancha (Spain), Graduate Studies in Compliance and Criminal Law at IDPEE (Portugal) and Graduate Studies in Criminal Law – General Part at IBCCRIM/IDPEE (Brazil/Portugal). He holds a Bachelor´s Degree in Law by the Universidade Estadual Paulista – UNESP (Brazil). tuliofxj@gmail.com

Additional information and author's declarations
(scientific integrity)

Conflict of interest declaration: the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

Declaration of originality: the author assured that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; he also attests that there is no third party plagiarism or self-plagiarism.

Editorial process dates
(https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 30/03/2023
- Desk review and plagiarism check: 02/04/2023
- Review 1: 18/04/2023
- Review 2: 30/04/2023
- Review 3: 30/04/2023
- Preliminary editorial decision: 25/05/2023
- Correction round return: 03/06/2023
- Final editorial decision: 16/06/2023

Editorial team

- Editor-in-chief: 1 (VGV)
- Associated-editor: 1 (AMNP)
- Reviewers: 3