Vilnius
University
Press

Contents lists available at Vilnius University Press

Teisė
2024, Vol. 130, pp. 66–76

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2024.130.6

On The Legal Limits and Criminal Procedural Implications of Applying Artificial Intelligence in Corporate Internal Investigations*

Túlio Felippe Xavier Januário

http://orcid.org/0000-0003-0400-1273
Faculty of Law of University of Coimbra
Pátio da Universidade 3004-528 Coimbra, Portugal
E-mail: tuliofxj@gmail.com

On The Legal Limits and Criminal Procedural Implications of Applying Artificial Intelligence in Corporate Internal Investigations

Túlio Felippe Xavier Januário

(University of Coimbra (Portugal))

Summary. The paper addressed the following questions: how can AI be applied in corporate internal investigations and what are the legal limits for its use? In case of effective application, how can it affect the admissibility and valuation of the information collected from these procedures in an eventual criminal lawsuit? It was demonstrated that, with the expectation of increasing the effectiveness and efficiency of compliance programs, AI has been used in real-time – and often predictive – supervision of employees, as well as in carrying out internal investigations, through, for example, lie detection systems. However, due to the limitations and risks of this technology, its employment must comply with legal parameters and restrictions. Therefore, three categories of restrictions were analyzed: with respect to (i) *legal requirements for data processing*, we noted that the processing of data to be used as input in those systems must find legal support in one of the hypotheses provided for in Articles 6 and 9(2) of the GDPR. Furthermore, the fundamental principles that substantiate the test of proportionality between the intended purpose and the intervention to be carried out, provided for in Article 5, must be observed. Regarding *(ii) possible prohibitions on the use of AI systems in the context of internal investigations*, we observed that the use of technologies to control and supervise the work environment must take into account the requirements of legality, shall not affect areas in which employees' expectations of privacy must prevail, and, lastly, must observe a second test of proportionality, aimed at assessing whether the technology in question is adequate and necessary to achieve the purpose intended with it and whether the rights possibly affected by it should not prevail. About the *(iii) limits to the admissibility and valuation of elements of information from internal investigations*, we concluded that their admission in criminal proceedings will depend on a new judgment of legality and proportionality. In addition, they may be admitted when presented by the company, in its defence, or by Public Prosecution, provided that a third test of proportionality is observed and that these elements of information are not considered sufficient to substantiate the conviction of any defendant, therefore having probative value similar to elements from state investigation acts.

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

[*] This investigation was carried out within the scope of the project entitled „Autoria e responsabilidade em crimes cometidos através de sistemas de inteligência artificial“, funded by the „Fundação para a Ciência e a Tecnologia – FCT“ (2020.08615.BD).

Received: 14/03/2024. **Accepted:** 19/03/2024

Dirbtinio intelekto taikymo įmonių vidaus tyrimuose teisinės ribos ir baudžiamieji procesiniai padariniai

Túlio Felippe Xavier Januário

(Koimbros universitetas (Portugalija))

Santrauka. Straipsnyje nagrinėjami šie klausimai: kaip dirbtinis intelektas gali būti taikomas įmonių vidaus tyrimuose ir kokios yra jo naudojimo teisinės ribos? Jei taikymas veiksmingas, kaip jis gali paveikti šių procedūrų metu surinktos informacijos priimtinumą ir vertinimą galimoje baudžiamojoje byloje? Buvo parodyta, kad, tikintis padidinti atitikties programų veiksmingumą ir efektyvumą, dirbtinis intelektas buvo naudojamas realiuoju laiku – ir dažnai prognozuojant – darbuotojų priežiūrą, taip pat atliekant vidaus tyrimus, pavyzdžiui, pasitelkiant melo nustatymo sistemas. Tačiau dėl šios technologijos apribojimų ir rizikos jos naudojimas turi atitikti teisinius parametrus ir apribojimus. Todėl buvo analizuojamos trys apribojimų kategorijos: kalbėdami apie (i) *teisinius duomenų tvarkymo reikalavimus*, pažymėjome, kad duomenų, kurie bus naudojami kaip įvesties duomenys šiose sistemose, tvarkymas turi būti teisiškai pagrįstas viena iš BDAR 6 straipsnyje ir 9 straipsnio 2 dalyje numatytų hipotezių. Be to, turi būti laikomasi pagrindinių principų, kuriais grindžiamas BDAR 5 straipsnyje numatytas siekiamo tikslo ir vykdomos intervencijos proporcingumo testas. Dėl (ii) *galimų draudimų naudoti dirbtinio intelekto sistemas atliekant vidaus tyrimus* reikia pažymėti, kad naudojant technologijas darbo aplinkai kontroliuoti ir prižiūrėti turi būti atsižvelgiama į teisėtumo reikalavimus, neturi būti daroma poveikio sritims, kuriose vyrauja darbuotojų lūkesčiai dėl privatumo, ir, galiausiai, turi būti laikomasi antrojo proporcingumo kriterijaus, kuriuo siekiama įvertinti, ar atitinkama technologija yra tinkama ir būtina, kad būtų pasiektas jos įgyvendinimo tikslas, ir ar neturėtų vyrauti teisės, kurioms ji gali turėti įtakos. Dėl (iii) *vidaus tyrimų informacijos elementų priimtinumo ir vertinimo ribų* padarėme išvadą, kad jų priėmimas baudžiamajame procese priklausys nuo naujo teisėtumo ir proporcingumo vertinimo. Be to, jie gali būti pripažįstami, kai juos pateikia bendrovė, gindamasi nuo kaltinimų, arba prokuratūra, su sąlyga, kad laikomasi trečiojo proporcingumo kriterijaus ir kad šie informacijos elementai nelaikomi pakankamais bet kurio kaltinamojo apkaltinamajam nuosprendžiui pagrįsti, todėl jų įrodomoji vertė yra panaši į valstybinio tyrimo aktų elementų įrodomąją vertę.

Pagrindiniai žodžiai: įmonių baudžiamoji teisė, atitiktis, vidaus tyrimai, dirbtinis intelektas, baudžiamasis procesas.

Introduction

Although they have undergone significant changes over the decades, the origins of compliance programs date back to the beginning of the 20th century, especially in some obligations imposed by the Securities and Exchange Commission – SEC and the Department of Justice – DOJ (Nieto Martín, 2015a, p. 27–28). However, it was decades later, with the disclosure of major financial scandals, such as Enron, WorldCom and Parmalat, that they gained real prominence, especially with the emergent idea of *enforced self-regulation* as the main response to the proven ineffectiveness of the *pure self-regulation* of financial agents to prevent illicit acts (Sarcedo, 2016, p. 24) and with state difficulties in regulating, preventing, investigating and repressing corporate crimes (Braithwaite, 1982). In other words, the private entities are called upon to participate in those activities, defining their own standards, which are then ratified by the State when in line with public legislation and interests and whose violations can be punished (Ayres, Braithwaite, 1992, p. 101–107; Coca Vila, 2013, p. 51).

Within the scope of these enforced self-regulation tools, 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 long-term aims are to maintain or recover the good reputation of the legal person, to secure the continuity of the business with the potentialisation of its profits and, mainly, to protect the corporation, its collaborators and representatives, from eventual liabilities in the most varied spheres, and from financial and reputational losses (Januário, 2019, p. 85–86).

Since compliance programs depend on the particularities of the corporation and its sector of activities, there is no single pre-defined model for their implementation (Rodrigues, 2020a, p. 102; Sieber, 2008, p. 458). A good example is the model proposed by Marc Engelhart (Engelhart, 2012, p. 711–719), who categorizes the stages of elaboration into three columns, namely: i) *the formulation* ("*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 program; ii) *the implementation* ("*communicate-promote-organise*"), which encompasses the program dissemination and personnel training phases, as well as the daily promotion of the culture of compliance; and iii) *the consolidation and improvement* ("*react – sanction – improve*"), marked by internal investigations and sanctioning procedures, as well as the evaluation mechanisms and continuous improvement of the program.

It is important to emphasise that, similarly to what happened in other sectors of society, these mechanisms have experienced the consequences of the so-called *Revolution 4.0,* since their activities have been increasingly conducted with the use of new technologies, such as autonomous systems and of artificial intelligence (henceforth, AI). However, despite their undeniable benefits, the use of these systems in compliance programs, especially in internal investigations, raises many questions, whether due to the limitations of these technologies (such as their opacity and unpredictability) or their potential to jeopardize some rights and guarantees of people involved (Januário, 2023, p. 724–726).

In view of this scenario, the aim of the present paper is to answer the following questions: how can AI be applied in corporate internal investigations and which are the legal limits for its use? In case if effective application, how can it affect the admissibility and valuation of the information collected from these procedures in an eventual criminal law suit? To address these topics, after a brief explanation of the fundamentals, procedures and purposes of internal investigations and how AI has helped in the achievement of their aims, we will analyse the legal guidelines for the use of this technology in this scope and for the sharing of information with criminal procedures. For that, based on a deductive methodology and with the analysis of the European legislation, doctrine and jurisprudence, we will investigate three main issues: the legal guidelines for processing data in internal investigations; the limits to the use of AI in these procedures; and the requirements and limits for sharing the elements of information derived from them with an eventual criminal proceeding.

1. AI in internal investigations

Given that compliance programs, however efficient they may be, cannot be infallible, not being able to completely cancel the risks of illicit actions within the company, it is important that they are equipped with instruments for precise action in those moments when things go wrong (Januário, 2021, p. 1462). That said, we can consider internal investigations as a set of procedures carried out within a company, with or without the help of external professionals, with the goal of investigating facts that show signs of legal, ethical or by-law violations. It is important to point out that these procedures cannot be confused with day-to-day supervisory activities or with due diligence activities, as, unlike the latter, they have a reactive and non-day-to-day nature (Canestraro, Januário, 2020, p. 294).

Despite possible variations arising from the particularities of the corporation and its sector of activity, investigative procedures tend to follow a uniform rite. The company becomes aware of the facts through its supervisory activities, complaints, or even through state investigation procedures that are communicated to it or released to the press. The decision to promote an internal investigation is then taken by the administrators or, by delegation, by the compliance officer. After defining an investigation plan, with the establishment of deadlines, competences and budget, the investigative diligences themselves begin, comprising analyses of documents, video and audio files, interviews and, depending on the case, expert exams (Nieto Martín, 2015b, p. 238; Canestraro, Januário, 2020, p. 298; Januário, 2021, p. 1470).

Upon completion of the investigations, a report is prepared with the respective conclusions, which may, depending on the case and the company's interests: i) justify the application of internal sanctions when illegal practices are identified; ii) integrate, together with the collected evidence, the company's defence in a possible law suit related to the case; iii) be shared with the competent authorities, together with the relevant documents and evidence, in order to bargain for possible procedural benefits, such as settlements, reduction in sentences or acquittals (Nieto Martin, 2015b, p. 258; Januário, 2021, p. 1471).

It is precisely from the possibility of sharing the information obtained through internal investigations with the authorities that some of the major concerns arise in terms of possible violations of the rights and guarantees of those being investigated. There is not only the risk of applying abusive and disproportionate methods in investigations, but also of attempts to direct their conclusions, trying to exempt the company and its administrators from responsibilities, attributing them to subordinate employees (Januário, 2021, p. 1472; Canestraro, Januário, 2020, p. 301). Besides that, when the investigated facts constitute criminal offences, the information obtained through internal investigations will be of interest to public authorities for the purpose of ascertaining authorship and punishing the individual who committed the crime. For this reason, the transfer of this information to a criminal proceeding, either as defensive evidence or through its collaboration with the authorities, raises several questions about the compatibility of these private procedures with some rights of those being investigated, such as the presumption of innocence, the contradictory and the right to non-self-incrimination (Januário, 2023, p. 742–744).

In our view, the relevance of these discussions has been accentuated due to the increasing use of AI in the most varied activities of compliance programs, including internal investigations. As Burchard (Burchard, 2020, p. 28) properly points out, *digital criminal compliance* can be considered the buzzword when talking about the employment of digital systems for real-time prevention of compliance violations, since the application of AI for the analysis of big data has the potential to increase the efficiency and effectiveness of the compliance program, especially if we consider that more advanced computer systems have greater ability to predict, with higher precision, the productive processes and actions, as well as to prevent and detect harmful situations (Burchard, 2021, p. 742; Rodrigues, Sousa, 2022, p. 13).

According to Burchard (2021, p. 744–747), digital criminal compliance presents the promise (not necessarily accomplished) of being a more comprehensive, objective, unbiased, and effective form of compliance. The author elucidates that a primary constraint of conventional (human-driven) compliance lies in its frequent retrospective (ex post) operation. This occurs precisely due to human limitations and errors and despite the prior availability of data on possible non-compliance. Through the digitalisation of compliance structure and the real-time data processing capabilities of emerging technologies, the expectation is to predict a large number of potential violations, preventing their occurrence. Furthermore, even if they are not avoided in certain instances, the data storage capacity of AI systems would undeniably facilitate subsequent investigation of the facts.

Among several other features that are already undergoing a certain degree of digitalisation, monitoring and supervising the work environment and conducting internal investigations, are certainly those in which the use of AI generates the most controversy. Based on the analysis of a dataset (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, all of them accessed through devices incorporated into workers' desks and offices), the *predictive surveillance of employees* is expected to determine with a high degree of precision which employees are more likely to commit acts of non-compliance, including criminal offences (Burchard, 2021, p. 747; Dearden, 2016; Moore, 2018, p. 26). Some other systems are allegedly able to identify "sensitive keywords" in communications and send an alert to the responsible department, in order to enable real-time monitoring of interlocution, besides being able of measuring the workers' productive time, distinguishing it from the time he/she deals with parallel matters (Canestraro, Januário, 2022, p. 373–374; Januário, 2023, p. 740)[1].

Regarding the application of AI in lie detection systems, Trentmann (2022, p. 29–30) explains that the present and future of these technologies involve the evaluation by AI systems of verbal and non-verbal signals and patterns. Through cameras and microphones, the system gathers data about facial expressions, gestures, linguistic patterns and the prevalence of specific terms and phrases during a statement. Subsequently, it compares this information with the empirical knowledge stored by the system and evaluates the veracity of the information provided by the speaker. The author clarifies that AI primarily works with voice stress analysis and facial or ocular scanning, and it is able to recognise patterns very quickly, based on an almost infinite repository of data.

With regard specifically to their application in the private sphere, the so-called *Eye Detect* stands out[2]. Based on the observation that, when lying, a person's brain has to work harder, the system identifies reactions of the declarant's eyes to certain questions or situations, including eye movements, blinks, fixations and changes in pupil diameter. With these data, it calculates a credibility value between 0 and 100, with any value below 50 indicating that the person is lying (Trentmann, 2022, p. 43ff).

2. Legal limitations and requirements

When we analyse the legal frameworks for the application of AI in internal investigations, we must keep in mind that these systems are inexorably dependent on data. For this reason, the first category to be considered is the i) *legal requirements for data processing.*

Data processing for the purposes of public security and criminal investigations must comply with two fundamental principles: a) the *necessary reserve of law* and b) the *prohibition of excess* (in the sense that the proportionality of interventions must be observed) (Gleizer *et al*., 2021, p. 40). Even though the purposes of internal investigations are not restricted to those mentioned above, we believe that these precepts can guide these private diligences, since facts of criminal relevance may be investigated and the evidence collected in this context could be of interest to public authorities (Januário, 2023, p. 746).

With regard to the *reserve of Law,* based on the General Data Protection Regulation (GDPR), the main legal bases that authorise the processing of data within the scope of investigation are, in descending order of relevance, i) compliance with a legal obligation; ii) exercise or defence of legal claims; iii) the pursuit of legitimate interests by the controller; and iv) the consent of data subject. Data processing is a fundamental measure for the fulfillment of legal obligations, wherefore, in our view, it is the main legal basis. It prevails over the exercise or defence of legal claims, not only because this hypothesis is provided solely for the "special categories of personal data" (Article 9(2)), but also due to the fact that internal investigations will not always depend on the existence or imminence of a parallel suit. In

[1] These are some of the functionalities announced, for example, by the systems Veriato (2023) and Veritone (2023).

[2] In Spain, for example, an automotive repair corporation uses the system to find out if its mechanics are making unnecessary repairs to customer vehicles (Heller, 2019, p. 2).

turn, invoking the legitimate interests of the controller for the processing of personal data included in this "special category" is not allowed, which is why we do not consider it the most appropriate basis in the case of internal investigations. Finally, with regard to consent, the possibility of its revocation at any time (Art. 7(3) GDPR) turns it into a "subsidiary ground", albeit an important one. Furthermore, we have doubts about whether we can speak of an effective freedom of consent in labour relations, in which there are evident fears of dismissals or non-hiring (European Parliament, Council of the European Union, 2016b; Januário, 2023, p. 747–750; Palhares *et al*., 2021; Article 29 Working Party, 2018).

It is important to point out that the GDPR expressly prohibits the processing of data related to criminal convictions or offences, unless conducted under the control of an official authority or authorised by the law of a Member State, which also ensures rights and guarantees of the data subjects (Article 10) (European Parliament, Council of the European Union, 2016b). In our point of view, due to this limitation, the use of data related to possible criminal records as input to AI systems depends on the knowledge and supervision of the state authority or the authorisation of the Member State's Law. If the occurrence of the crime is verified after the beginning of the investigation, its continuance will depend on the legal authorisation and/or supervision of the authority (Januário, 2023, p. 746–747).

The *prohibition of excess* represents the balance to be made between the means applied by the controller and the purposes sought with it. It materialises itself through some principles provided for by the GDPR and the Directive (EU) 2016/680, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability (European Parliament, Council of the European Union, 2016a; European Parliament, Council of the European Union, 2016b; Gleizer *et al*., 2021, p. 59).

In addition, however, to the limitations and requirements for data processing, it is also important to assess, more broadly, what would be ii) *the limits for the application of AI systems in internal investigations.* First, it must be considered whether the requirement of legality is fulfilled, that is, the adoption of the system must find legal support. In a work environment, it is generally considered that the supervision and control tools adopted by the employer are supported by his/her directive power, which attributes to him/her the burdens and powers to control the work environment, the company's assets and its employees. These powers, however, are not unlimited, having their limits precisely in laws, collective agreements and, above all, in the Constitution (Januário, 2023, p. 752–753).

It is quite controversial, for example, the admissibility or not of interceptions (inclusive those with new technologies, such as AI), by the employer, of the employees' communications. Some authors consider it inadmissible, especially due to the inviolability of telegraphic, data and telephone communications, with the exception of, in the latter case, the existence of a court order for the purposes of investigations and criminal proceedings (Garcia, 2014). On the other hand, some doctrine understands that the freedom of communications and intimacy would not be affected if interlocutors have previous knowledge of the recording (Badaró, 2020, p. 592). Based on this position, we understand that the employment of AI systems that monitor communications does not constitute a violation of the freedom of communication and intimacy, 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 (Januário, 2023, p. 755).

Another important limit to be observed is the *expectations of privacy*. It is usual that, although provided exclusively for work purposes, some tools (such as corporate e-mails, computers and mobile phones) end up being used also for some personal communications. For this reason, it is quite consolidated the understanding that, in order for these tools to be inspected and monitored, prior, express and detailed knowledge must be given to the employee that those objects can only be used for work purposes, that they may be subject to specific forms of inspection and what information may be collected from them (Copland v. the United Kingdom*,* 2007; Bărbulescu v. Romania, 2007; Gómez Martín, 2022, p. 1174ff; Canestraro, Januário, 2022, p. 376–377).

However, the legitimacy of the employer's intervention depends not only on respect for the employee's expectation of privacy, but must also be proportionate. In our view, it is necessary to assess, in the specific case: i) whether the restriction of the worker's right is likely to achieve the desired purpose (*adequacy* judgment); ii) if there are no other equally effective forms that restrict the worker's right less (*necessity* judgment); iii) whether the concrete restriction of the worker's right is more beneficial for the common good than its preservation to the detriment of the purpose sought (*proportionality in the strict sense*) (Alcácer Guirao, 2022, p. 997–998; Gómez Martín, 2013, p. 133; Maschmann, 2013, p. 151ff; Estrada I Cuadras, Llobet Anglí, 2013, 205; Januário, 2023, p. 757).

Finally, it is important to consider that, although the purpose of internal investigations is not restricted to them, facts that constitute criminal offences may be investigated. For this reason, despite being procedures conducted in a private environment, often dissociated from state investigations, they become a problem of criminal procedural relevance, from the moment the company decides to share the information and documents obtained with the public authorities, either to obtain procedural benefits or to defend themselves in criminal lawsuits.

The importance of this discussion is accentuated, in our opinion, when we consider the possibility of using AI in internal investigations. Despite its potential to make these activities more efficient and effective, we cannot ignore that this technology still has some limitations, such as its opacity. By this, we mean that, due to its technical complexity, the human comprehension of its internal processes and the foundations of its decisions is difficult (Burrell, 2016, p. 1; Wimmer, 2019; Rodrigues, 2020b, p. 25). Furthermore, due to their ability to learn from previous experiences and autonomously adapt their own algorithms, the most advanced AI systems can prove to be unpredictable even for their developers and programmers (Sousa, 2020, p. 64). Finally, there are risks related to the data used as input, whether with regard to the legality of their collection or their quality (Miró Lliñares, 2018, p. 114ff; De Hoyos Sancho, 2020, p. 16ff; Mulholland, Frajhof, 2019; Peixoto, Silva, 2019, p. 34–35).

For these reasons, it is essential to analyse what would be iii) *the limits for sharing with a criminal procedure information and documents obtained in internal investigations*, when AI systems are used.

The first point to be considered is that, depending on the situation, sharing data processed within the scope of an internal investigation can configure a change of purpose and, consequently, a new intervention. That is, if the legal basis invoked was other than the defence of the company in legal proceedings, a new judgment of legality and proportionality will be necessary (Januário, 2023, p. 763–764). Considering that sharing data involves two distinct interventions and applying the so-called *two-door model,* the formal legality can be ascertained through a law that authorises the entity that first collected and stored the data (primary controller) to give access to the information and another one that authorises the entity that will receive the data (secondary controller) (Gleizer *et al*., 2021, p. 138–140).

With regard to the admissibility of this sharing with the criminal procedure, we understand that some situations must be differentiated. In principle, the elements of information will be admissible when the company presents them in the context and for the purposes of its defence. A contrary understanding, in our view, would violate its rights of defence and to present evidence and would even be a factor that discourages the adoption of compliance programs and the conduction of internal investigations (Januário, 2021, p. 1483–1484; Januário, 2023, p. 766ff).

In turn, when presented by the Public Prosecution or even by the company's defence, but in detriment of another defendant (e.g., an employee), there is a conflict between the rights to defence of both defendants, as well as the guarantees to the contradictory and due process of the subject affected by the evidence. Therefore, we understand that the solution for these cases should be guided by the following directives: i) the elements of information will be admissible when presented by the defendant in its defence and will be fully valued for these purposes; ii) these elements of information, whether presented by the defence or by the Public Prosecution, cannot be considered sufficient to support a conviction. They will have a regime similar to state investigation acts, being sufficient only to substantiate the *opinio delicti* of the Prosecution (Canestraro, 2020, p. 95ff); iii) finally, since the elements of information presented by the company cannot be valued for the purposes of substantiating the conviction of another defendant, it may be necessary to separate the lawsuits[3], as provided for by several legal systems (Januário, 2021, p. 1483ff; Januário, 2023, p. 766ff).

It is evident that the admission of these elements of information in no way exempts the necessary judgment to be made about their credibility. Among other aspects, it is fundamental to verify the integrity, identity, and authenticity of digital evidence obtained with the intervention of AI systems, even if they come from internal investigations (Januário, 2021).

Conclusions

1. As demonstrated throughout the investigation, AI has been progressively applied in compliance programs and internal investigations, aiming to increase the efficiency and effectiveness of these procedures. However, due to the limitations and risks of this technology, its employment must comply with legal parameters and restrictions.
2. First, the processing of data to be used as input in these systems must find legal support in one of the hypotheses provided for in Articles 6 and 9(2) of the GDPR. Furthermore, the fundamental principles that substantiate the test of proportionality between the intended purpose and the intervention to be carried out, provided for in Article 5, must be observed.
3. In addition, it is important to analyse the limitations and requirements for the application of the concrete AI system. As noted, for the purposes of complying with legality, the use of technologies to control and supervise the work environment generally finds support in the rules related to the directive power of the employer, even if this is not unlimited. Besides that, it is crucial that they do not affect areas in which employees' expectations of privacy must prevail. Finally, a second test of proportionality must be observed, assessing whether the technology in question is adequate and necessary to achieve the purpose intended with it and whether the rights possibly affected by it should not prevail.
4. With regard to criminal procedural aspects, it is crucial to analyse the admissibility and valuation of elements of information from internal investigations when AI systems have been applied. Since sharing can configure, depending on the case, misuse of purpose and, consequently, a new intervention, a new judgment of legality and proportionality may be necessary for sharing and receiving these data. In addition, the elements of information may be admitted in criminal proceedings when

[3] A different solution is proposed, for example, by Dominik Brodowski (2014, p. 219–221) and Maria João Antunes (2018, p. 126–127). According to them, although legal entities enjoy some criminal procedural guarantees, if they come into conflict with the rights and guarantees of natural persons, these latter must prevail. Some of the foundations for this understanding would reside in the fact that, due to the nature assumed by legal entities, their rights would admit some relativizations. Furthermore, some procedural rights are linked not only to the parity of arms in criminal proceedings, but also to the dignity of the human person, which does not extend to companies. Besides, in crimes committed by corporations, there is no risk of imprisonment, thus not affecting the hard core of criminal law.

presented by the company, in its defence, or by Public Prosecution, provided that a third test of proportionality is observed and that these elements are not considered sufficient to substantiate the conviction of any defendant, therefore having probative value similar to elements from state investigation acts. Bearing in mind the probable conflict between the procedural rights and guarantees of the individuals and companies prosecuted, it may prove necessary to separate the lawsuits.

Bibliography

Legal acts

European Parliament, Council of the European Union. (2016a). *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* [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680 [Accessed 14 August 2023)].

European Parliament, Council of the European Union. (2016b). *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)* [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed 09 March 2023].

Special literature

Alcácer Guirao, R. (2022). Investigaciones internas: prolegómenos constitucionales y cuestiones abiertas. In: Gómez Martín, V. *et al*. (ed.). *Un modelo integral de Derecho penal: Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*. Madrid: BOE, 989–1000.

Antunes, M. J. (2018). Privatização das investigações e compliance criminal. *Revista Portuguesa de Ciência Criminal*, 28(1), 119–128.

Ayres, I., Braithwaite, J. (1992). *Responsive regulation: transcending the deregulation debate*. Oxford: Oxford University Press.

Badaró, G. H. (2020). *Processo penal*. 8.ed. São Paulo: Thomson Reuters Brasil.

Braithwaite, J. (1982). Enforced self-regulation: a new strategy for corporate crime control. *Michigan Law Review*, 80(7), 1466–1507, https://doi.org/10.2307/1288556

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

Burchard, C. (2020). Das »Strafrecht« der Prädiktionsgesellschaft: …oder wie »smarte« Algorithmen die Strafrechtspflege verändern (könnten), *Forschung Frankfurt: das Wissenschaftsmagazin: Recht und Gesetz*, (1), 27–31.

Burchard, C. (2021). Digital Criminal Compliance. In: Engelhart, M. *et al*. (ed.) *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag: Teilband II*. Berlin: Duncker & Humblot, 741–756.

Burrell, J. (2016). How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. *Big Data & Society*, 3(1), 1–12, https://doi.org/10.1177/2053951715622512

Canestraro, A. C. (2020). *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 [online]. Available at: https://ibccrim.org.br/publicacoes/exibir/58/as-investigacoes-internas-no-ambito-do-criminal-compliance-e-os-direitos-dos-trabalhadores [Accessed 16 August 2023].

Canestraro, A. C., Januário, T. F. X. (2020). 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*, 6(1), 283–328, https://doi.org/10.22197/rbdpp.v6i1.324

Canestraro, A. C., Januário, T. F. X. (2022). Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal. In: D'Ávila, F. R. *et al*. (ed.) *Direito e Tecnologia*. Porto Alegre: Citadel, 363–392.

Coca Vila, I. (2013). ¿Programas de cumplimiento como forma de autorregulación regulada? In: Silva Sánchez, J. M. *et al*. (ed.). *Criminalidad de empresa y compliance: prevención y reacciones corporativas*. Barcelona: Atelier, 43–76.

De Hoyos Sancho, M. (2020). 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*, (76), 9–44, https://doi.org/10.37417/rede/num76_2020_534

Engelhart, M. (2012). *Sanktionierung von Unternehmen und Compliance: eine rechtsvergleichende Analyse des Straf- und Ordnungswidrigkeitenrechts in Deutschland und den USA*. 2. ed. Berlin: Dunker & Humblot.

Estrada i Cuadras, A., Llobet Anglí, M. (2013). Derechos de los trabajadores y deberes del empresario: conflicto en las investigaciones empresariales internas'. In: Silva Sánchez, J. M. *et al*. (ed.). *Criminalidad de empresa y compliance: prevención y reacciones corporativas.* Barcelona: Atelier, 197–228.

Garcia, G. F. B. (2014). *Curso de direito do trabalho*. 8. ed. Rio de Janeiro: Forense.

Gleizer, O. *et al*. (2021). *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons.

Gómez Martín, V. (2013). Compliance y derecho de los trabajadores. In: Kuhlen, L. *et al*. (ed.). *Compliance y teoría del derecho penal*. Madrid: Marcial Pons, 125–146.

Gómez Martín, V. (2022). ¿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, V. *et al*. (ed.) *Un modelo integral de Derecho penal: Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*. Madrid: BOE, 1167–1178.

Januário, T. F. X. (2019). *Criminal compliance e corrupção desportiva: um estudo com base nos ordenamentos jurídicos do Brasil e de Portugal*. Rio de Janeiro: Lumen Juris.

Januário, T. F. X. (2021). Cadeia de custódia da prova e investigações internas empresariais: possibilidades, exigibilidade e consequências processuais penais de sua violação. *Revista Brasileira de Direito Processual Penal*, 7(2), 1453–1510, https://doi.org/10.22197/rbdpp.v7i2.453

Januário, T. F. X. (2023). Corporate Internal Investigations 4.0: on the criminal procedural aspects of applying artificial intelligence in the reactive corporate compliance. *Revista Brasileira de Direito Processual Penal*, 9(2), 723–785, https://doi.org/10.22197/rbdpp.v9i2.837

Maschmann, F. (2013). Compliance y derechos del trabajador. In: Kuhlen, L. *et al*. (ed.). *Compliance y teoría del derecho penal*. Madrid: Marcial Pons, 147–167.

Miró Llinares, F. (2018). Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, 3(20), 87–130, https://doi.org/10.5944/rdpc.20.2018.26446

Moore, P. V. (2018). *The Threat of Physical and Psychosocial Violence and Harassment in Digitalized Work*. Geneva: International Labour Office.

Mulholland, C., Frajhof, I. Z. (2019). Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: Frazão, A. *et al*. (ed.). *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade*. São Paulo: Thomson Reuters Brasil.

Nieto Martín, A. (2015a). El cumplimiento normativo. In: Nieto Martín, A. *et al*. (ed.) *Manual de cumplimiento penal en la empresa.* Valencia: Tirant lo Blanch, 25–48.

Nieto Martín, A. (2015b). Investigaciones internas. In: Nieto Martín, A. et al. (ed.) *Manual de cumplimiento penal en la empresa*. Valencia: Tirant lo Blanch, 231–271.

Palhares, F. *et al*. (2021). Compliance Digital e LGPD. In: Nohara, I. P. D. *et al*. (ed.). *Coleção compliance, v. 5*. São Paulo: Thomson Reuters Brasil.

Peixoto, F. H., Silva, R. Z. M. (2019). *Inteligência artificial e direito*. Curitiba: Alteridade Editora.

Rodrigues, A. M. (2020a). *Direito penal económico: uma política criminal na era compliance*. 2.ed. Coimbra: Almedina.

Rodrigues, A. M. (2020b). Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização. In: Rodrigues, A. M. (ed.). *A Inteligência Artificial no Direito Penal, vol. 1.* Coimbra: Almedina, 11–58.

Rodrigues, A. M., Sousa, S. A. (2022). Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal. In: Rodrigues, A. M. (ed.). *A inteligência artificial no direito penal, vol. II*. Coimbra: Almedina, 11–39.

Sarcedo, L. (2016). *Compliance e responsabilidade penal da pessoa jurídica: construção de um novo modelo de imputação baseado na culpabilidade corporativa*. São Paulo: LiberArs.

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

Sousa, S. A. (2020). "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial". In: Rodrigues, A. M. (ed.). *A inteligência artificial no direito penal*, *vol. 1*. Coimbra: Almedina, 59–94.

Trentmann, C. H. W. (2022). *Wahrheitsdetektionssyteme mit künstlicher Intelligenz: ein neues Legal-Tech-Modell für Internal Investigations*. Baden-Baden: Tectum Verlag.

Wimmer, M. (2019). Inteligência Artificial, Algoritmos e o Direito: Um Panorama dos Principais Desafios. In: Lima, A. P. C. *et al*. (ed.). *Direito Digital: Debates Contemporâneos*. São Paulo: Thomson Reuters Brasil.

Case law

Bărbulescu v. Romania (2017). ECHR, Application no. 61496/08 [online]. Available at: https://hudoc.echr.coe.int/?i=001-177082 [Accessed 15 August 2023].

Copland v. the United Kingdom (2007). ECHR, Application no. 62617/00 [online]. Available at: https://hudoc.echr.coe.int/?i=001-79996 [Accessed 15 August 2023].

Other sources

Article 29 Working Party. (2018). *Guidelines on consent under Regulation 2016/679: Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2018* [online]. Available at: https://ec.europa.eu/newsroom/article29/items/623051 [Accessed 10 March 2023].

Dearden, L. (2016). The Telegraph Backtracks on Sensors Monitoring Whether Journalists are Sitting at Desks Amid Outrage, *The Independent*, 12 January [online]. Available at: https://www.independent.co.uk/news/media/the-telegraph-backtracks-on-sensors-monitoring-whether-journalists-are-sitting-at-desks-amidoutrage-a6807336.html. [Accessed: 10 August 2023].

Heller, P. (2019). Lügendetektoren: Kann dieses Auge lügen? *Frankfurter Allgemeinen Zeitung*, 12 October [online]. Available at: https://www.faz.net/-gwz-9romr [Accessed 25 February 2023].

Veriato (2023). *Employee Monitoring & Insider Risk Management: Workforce Behavior Analytics for the Work from Anywhere World: Gain complete visibility into your remote or hybrid workforce activity to boost productivity and keep sensitive data secure* [online]. Available at: https://www.veriato.com/ [Accessed 10 August 2023].

Veritone (2023). *Impossible is outdated* [online]. Available at: https://www.veritone.com/ [Accessed 10 August 2023].

Túlio Felippe Xavier Januário is a PhD Candidate in Law at the University of Coimbra, with a fellowship from the Fundação para a Ciência e a Tecnologia – FCT. He holds a LLM from the University of Coimbra, with a research internship of the "ERASMUS+" Program at the Georg-August-Universität Göttingen. He had graduate studies in International Criminal Law at the Siracusa International Institute for Criminal Justice and Human Rights, graduate studies in Economic Criminal Law and CrimeTheory at the University of Castilla-La Mancha, graduate studies in Compliance and Criminal Law at IDPEE, and graduate studies in Criminal Law – General Part at IBCCRIM/IDPEE. He holds a LLB from the Universidade Estadual Paulista – UNESP.

Túlio Felippe Xavier Januário yra Koimbros universiteto teisės mokslų kandidatas, gavęs Fundação para a Ciência e a Tecnologia (FCT) stipendiją. Koimbros universitete įgijo teisės magistro laipsnį, stažavosi pagal „ERASMUS+" programą Getingeno universitete (Georg-August-Universität, Göttingen). Jis baigė Tarptautinės baudžiamosios teisės magistrantūros studijas Sirakuzos tarptautiniame baudžiamosios justicijos ir žmogaus teisių institute, Ekonominės baudžiamosios teisės ir nusikalstamumo teorijos magistrantūros studijas Kastilijos-La Mančos universitete, Laikymosi ir baudžiamosios teisės magistrantūros studijas IDPEE ir Baudžiamosios teisės bendrosios dalies magistrantūros studijas IBCCRIM/IDPEE. Autorius yra įgijęs teisės bakalauro laipsnį Estadual Paulista universitete (Universidade Estadual Paulista – UNESP).