CORPORATE CRIMINAL LAW, ARTIFICIAL INTELLIGENCE AND BIG DATA: THE HUAWEI CASE AND ITS IMPLICATIONS FOR GLOBAL SOCIETY

Paula Andrea Ramírez Barbosa[1]

ABSTRACT

The impact of artificial intelligence can be significant in determining corporate risks. In turn, Big Data can provide relevant information on events that impact the business world as concrete dangers. This should be done by evaluating endogenous and exogenous variables that can be interpreted together. However, this approach requires the development of additional strategies in the company that are aimed at education, training and updating technological notions and digital innovation tools. This is because Big Data and Artificial Intelligence complement each other and can represent a potential change in the parameters of cyber criminal law.The Huawei case is a representation of the industrial revolution, economic and data-driven digital intelligence revolution, reflecting the repercussions of the actions of a multinational company that allegedly violated the regulations of a third country, in this case the United States. As it is a major corporation that provides services in the telecommunications devices and equipment market, its operation broadly affects the global economy and the digital society. The criminal process against the company by the United States may affect the operational, reputational and commercial capacity of the company in transnational relationships for technological and digital exchange on a global scale.

Keywords: artificial intelligence, Big data, criminal law, corporate crime, diigital society, Huawei, telecommunications.

[1] PhD in Law, at Universidad de Salamanca. Professor of Criminal Law at Universidad Externado de Colombia and Universidad Católica de Colombia. Email: **pauramirez2003@yahoo.es**

1. **Introduction**

Corporate crime is a global reality. It is transnational, organizational and of occurrence in different industrial sectors in the countries in which it generates negative effects on the economic and social order. Its repercussions are multiple, not only of a legal and social nature, but also in terms of financial damages and losses that it causes, implications for the transparency of business, damage to the reputation of companies, alteration of prices in the markets, quality of products and confidence in commercial sectors. Corporate crimes are committed against the interests of companies by their members or third parties, affecting their chartered business goals. These crimes can also be carried out by deviating the purposes of the company to affect the rights of third parties and may include crimes committed by directors or members of the company for their benefit and damages to corporate interests.

The catalog of conduct that is included in corporate crime is broad. Some of the prominent forms of corporate criminality include accounting fraud, corporate scams, money laundering, business bribery, anti-trust violations, the use of privileged information and international corruption, among others. The individuals that typically commit these crimes are characterized by their professional knowledge, business skills and professional fields of action, which they use to carry out prohibited behaviors. Prominent reasonsfor committing corporate wrongdoing are associated with the excessive pursuit of economic advantage outside of the legal or regulatory regimes governing a particular industry.

The sophistication of criminal behavior is highly prominent in corporate criminality.This is why the use of virtual coins, tax havens, off shore companies, internationalization of operations and the use of new information technologies is critical in understanding their implications for investigating and prosecuting this conduct. Expanding the effects of these expressions of crime is facilitated in cyberspace, virtual banking and economic exchanges on a large scale with a single electronic movement. In this context, analyzing the new frontiers of corporate criminal law is critical. Specifically, artificial intelligence and Big Data, both for the

commission of crimes that affect the company and by carrying out business crimes that abuse the company's corporate purpose. In this panorama, the Huawei case is of special interest given its global implications but also given its unique technological, legal and economic aspects.

2. **Corporate crime through new technological frontiers**

Corporate crime includes actions or omissions carried out in companies, through their workforce, that affect their chartered corporate purpose and are expressed in organized irregularities. These may include classical business crimes such as pyramid schemes and insurance fraud to complex crime involving securities fraud, market manipulation, money laundering, anti-trust violations and accounting fraud among others. In the modern industrialized business world, most forms of such corporate crime are carried out through the use of information technology.

Corporate criminals attempt to hide their crimes through complicated financial maneuvers, the existence of multiple bank accounts, the creation of altered identities in cyberspace, encrypted communications and other schemes that are difficult to trace and enable their expansion. In this environment, corporate crime actors use the advances in computing and the agility provided by technologies to perfect the transnationality of operations and the opacity of the effects of their criminal activity.

Business crimes are often unreported because victims may be immediately unaware of the affectation or injury of their economic interests or because they may perceive a risk of corporate reputational embarrassment as victims of fraud, embezzlement or other organizational victimization. In turn, corporate crimes harm the proper functioning of the economy as well asboth domestic and foreign markets. Such is the case of crimes like transnational bribery and money laundering, among others. Faced with these forms of criminality, corporate reaction to criminal activity usually occurs late after a noticeable impact through events that are difficult to mitigate or repair. In other cases, these crimes receive less publicity since the victims are usually considered to be partly

responsible, or a notion emerges that the State's action facilitated the execution of the crimes in the company and, therefore, it is the company who should sustain economic losses(Feijoo, 2016, p. 66).

> These new frontiers of corporate crime are focused on achieving an increased patrimony beyond the possible profits for the type of company. In turn, the uncontrolled objective of obtaining illegal profits by skilled business actors is one of the predominant factors in corporate crime. In this context, it is necessary to verify whether individuals or business entities related to corporate crime amass unjustified income or increase in assets in violation of market rules. The foregoing implies knowing what the mechanisms are within the organization to prevent, detect, mitigate or prove fraud and thus prevent the expansion of its effects inside or outside of the business organization to, among other actions, contaminate legal money with that derivative of crime(Gómez-Jara Diez, 2006, p. 10; Kuhlen, 2013, p. 73).

In light of the foregoing, the pursuit of corporate crime assets takes on relevance in a dual direction. On the one hand, as an instrument of real deterrence and guarantee that crime is not a viable alternative, and on the other, as a sanction mechanism through the use of the dividends of crime for the reparation of victims, crime prevention and the strengthening of justice, among others.

3. **Big Data and Corporate Criminal Law: new realities and frontiers**

The increase in multilateral businesses, transnational and digital communications, and the use of new means of economic exchange is a reality. This makes it more difficult to detect crime linked to the corporate world. Companies have adapted to these changes, with an outstanding use of technologies, on the one hand,

to more efficiently fulfill the provision of goods and services, and on the other, to safeguard the interests of their customers and detect practices contrary to legality, thus fighting business crime.

New information technologies that are based on predictive analysis and Big Data have been strengthened in the study of potentially harmful or dangerous situations for specific interests and in crime prevention, which makes law enforcement more proactive and less reactive. However, the large-scale use of Big Data can create distortions that negatively influence legal decision-making due to the centralized nature of data collection and applicationthat restricts and even eliminates heterogeneity of behaviors (Fallon, J, 1997, p. 3)

In this framework, through the use of Big Data and artificial intelligence, tools that can detect illicit transactions which pose risks to the interests of the company can be identified. Data gathered must be thoroughly analyzed towards meeting the standards established for good corporate governance and regulatory compliance. (Navas, 2017, p. 25). Corporate policies that incorporate compliance together with the effective detection of potentially harmful conduct through Big Data and information technologies, can anticipate protection barriers against this form of risk, which must be formulated taking into account objective factors such as the type of company, number of workers, links with third parties, national and international scope of action, among other relevant aspects.

The business world is characterized by being automated, with the use of technologies. Signals that increase corporate risks are analyzed and interpreted due to their virtual harm in affecting corporate interests. Big Data can be used to strengthen the preventive processes of detection and mitigation of the dangers that may affect the corporation and also streamline procedures and maximize resources by automating procedures that allow this treatment, which can be reflected in cost reduction and an environment of better knowledge of corporate activities. (Borge, 2017, p. 140).

One of the key tools of Big Data analysis is technology, which can contribute to the strengthening of the most traditional solutions in the prevention of crime in companies and the anticipation of optimal responses to business risk factors that affect the realization of corporate crime. Big Data analysis stores information and then directs inquiries to specific data. However, this system can yield evaluation criteria that can only be considered together with objective elements of rational weighing of the facts, focused on the particular circumstances of crime, so as to not err while seeking prevention and control (Valls, 2017, p. 17).

Despite its promise, the legal dynamics of Big Data develop several restrictions. First, the varieties of types of laws applicable to each business sector and the various data of interest that are handled organizationally, make it impossible to interpret in detail what happens in each company. Second, variations in the political, social, legal system and exogenous factors that affect the economy and the market rules that are dynamic and constant. Thus, Big Data cannot predict exactly what may happen or the how these changes will impact the company. (Mallada, 2019, p. 7). Third, the use of Big Data can become a distraction factor that obviates the imperceptible changes in the market and society and focuses on corroborating the notorious. This can represent the prediction of phenomena that can be common to all kinds of organizations but that do not detect the particularities of the company, the characteristics that distinguish them from others and the real effect on the verification of crimes that may affect the organization (Ballester, 2019, p. 589).

A vision of corporate criminal law focused on Big Data as a possible solution to supporting prevention policies and good corporate governance, far from guaranteeing greater regulatory compliance, could generate flat organizational decisions in terms of deterrence, risk mitigation and crime prevention. Technology undoubtedly has a significant impact on companies and their best development, but these measures are usually complementary to the approach based on the optimization of ethical, cultural and organizational values that are mainly aimed at individuals and organizations and not algorithms as the best option (Ramírez, 2019, p. 20).

To the reality of Big Data must be added the appearance of new economic exchange systems such as virtual currency, defined by the European Central Bank since 2014 as "a digital representation of value, which is not issued by a central bank or a public authority, not necessarily connected to a fiat money, but it is accepted as a means of payment and can be transferred, stored or exchanged electronically (Navarro, 2017, 2017, p. 270).

Given that corporate crime evolves permanently, the methods to combat it must be adjusted to technological advances and to the predictive study of crime, without this implying the exclusion of other crime prevention instruments based on internal control, an early reporting system and environment of a culture of legality that radiates throughout the company, which ultimately implies the establishment of an effective and comprehensive management model. However, the combination of 'Big Data', algorithms, block chain, 'machine learning' and crypto currencies is a reality that is perceived in the various forms of sophisticated, transnational and technological crime that advance on a large scale and that require effective action by the Criminal law (Ramírez, 2019, p. 5).

4. **Corporate criminal law and artificial intelligence**

The artificial intelligence opinion of the European Economic and Social Council on its consequences for the single digital market, production, consumption, employment and society, considered that artificial intelligence is the “scientific discipline that deals with creating computer programs that perform operations comparable to those performed by the human mind, such as learning or logical reasoning of people”[2].

Companies are using artificial intelligence to prevent and detect crimes that are committed within the corporation or the conduct of its members and employees related to the company's corporate purpose, such as money laundering, bribery, accounting fraud and the use of privileged information. The tools derived from artificial intelligence make it easier for companies that apply it to carry out better

[2]In https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018IE1473&from=ES.

risk management and faster and more responsive fraud detection, and even to predict and prevent crime (Quest, 2018).

Currently, machine learning uses predictive rules that recognize anomalies in data sets in real time through the use of advanced algorithms, which require specific criteria in the handling of information to detect whether or not the risks the companypredicts are correct. By using artificial intelligence, companies can identify areas of possible crimes, evaluating their potential and how they can be confronted with mitigation measures and effective control, without replacing the assessment of specialized professionals who analyze and evaluate human behavior and the specific dangers that may affect the development of the business model[3].

Big Data and artificial intelligence undoubtedly assist companies in facing the challenges demanded by the prevention, detectionand prosecution of corporate crime. Thus, criminal law must adapt to economic and technological changes and the digitization of information, among others.In this vein, the implications of algorithms, cryptography and block chain technology inevitably arise in an environment of industrial and commercial revolution that interconnects the physical and digital. These are aspectsthat on the one hand, support the commission of crimes, as their detection is very difficult through their complex trails. On the other hand, they facilitate the detection of crimes and evidence collection.

Transparency and security must be allied in the business world as prevention tools for the different forms of fraud or crimes that may be carried out within the organization. Thus, artificial intelligencecan provide instruments to facilitate the detection of corporate wrongdoing and to achieve an early glimpse of crimes such as money laundering, transnational bribery, accounting fraud, cybercrime, to name a few. However, its usefulness is complementary to other crime prediction mechanisms, that interconnected can guarantee enhanced possibilities of prevention and control of business risks[4].

[3]Idem.

[4] Consult in https://www.coit.es/sites/default/files/informes/pdf/20180130_informe_coit_gppyr._hacia_la_sociedad_gigabit.luces_y_sombras_vfinal_0_0.pdf

Artificial intelligence cannot replace formal social control mechanisms and specifically the functions performed by criminal law, since it is an inaccurate and mechanical system that requires human intervention. Examples of its imprecision are associated with the modest transparency of its algorithms or the lack of contextualization of their scope, its predictive and linear nature; and the possible manipulation of data[5]. In this context, the corporate environment can make effective use of high-value data on businesses, market behavior, customer requirements and the operation of the specific economic and social order, using 'machine learning' techniques to do so. On the one hand, these allow the identification of patterns and the design of more adequate tools in the safeguarding the corporate charter of the company. On the other hand, they facilitate better knowledge in the prevention of business risks and crimes.

5. THE HAWEI CASE AND THE NEW BORDERS OF GLOBAL CRIMINAL LAW

5.1. The relevant facts in the indictment presented by the United States Department of Justice

As stated in the indictment, as of 2007, Huawei employees lied about Huawei's relationship with a company in Iran called Skycom, falsely claiming that the company was not a subsidiary. The company further stated that Huawei had only limited operations in Iran and that it did not violate US laws or regulations or others related to Iran. After news releases in late 2012 and 2013 revealed that Huawei operated Skycom as an unofficial affiliate in Iran and that one of its employees had served onthe Skycom board of directors, Huawei employees continued to lie to the company's banking partners about Huawei's relationship with Skycom[6].

Huawei employees falsely claimed that Huawei had sold its interest in Skycom to an unrelated third party in 2007 and that Skycom was simply Huawei's

[5] Martin Hilbert, Big Data guru, on the battle for Huawei: "Any digital iron curtain can only be detrimental to the development of Latin America", https://www.bbc.com/mundo/noticias-america-latina-48480019.

[6] *https://www.justice.gov/opa/press-release/file/1125021/download.*

local business partner in Iran. Skycom was actually Huawei's Iranian affiliate and Huawei orchestrated the 2007 sale to appear as an arm's length transaction between two unrelated parties, when in fact Huawei actually controlled the company that bought Skycom.

According to the indictment, Huawei conducted global banking operations that included the processing of transactions in US dollars across the United States. During this time, the laws and regulations of the United States generally prohibited banks from processing Iran-related transactions through the United States. Thus, baking institutions in the United States were subject to civil or criminal penalties for processing transactions that violated the country's laws or regulations. Based on Huawei's repeated misrepresentations, its partner banks continued their banking relationships with the company.

Eventually one of Huawei's top global banking partners (identified as "Financial Institution 1" in the indictment) decided to sever its relationship with the company in 2017 due to Huawei's risk profile. The indictment also outlines that the corporation made additional false statements to several of its banking partners in an effort to maintain and expand those relationships.[7]

In 2017, when Huawei learned that U.S. authorities were investigating it, the company and its subsidiary, Huawei USA, allegedly attempted to obstruct the investigation by making efforts to move witnesses with knowledge of the company's business in Iran to the People's Republic of China. This placed those witnesses beyond the jurisdiction of the US government. The company also allegedly hid and destroyed evidence of Huawei's business in Iran that was located in the United States.

5.2 The crimes charged by the United States Department of Justice

Chinese telecommunications conglomerate Huawei and the company's chief financial officer, Wanzhou Meng, were charged with financial fraud in the United States District Court for the Eastern District of New York(Brooklyn, New York)in a 13-count indictment. Huawei Technologies Co. Ltd. (Huawei), is the largest

[7] *https://www.justice.gov/opa/press-release/file/1125021/download.*

manufacturer of telecommunications equipment in the world, based in the People's Republic of China (PRC), whose operations are carried out worldwide[8].

The companies Huawei and Skycom were charged with violating the U.S. federal crimes of bank fraud; conspiracy to commit bank and electronic fraud; conspiracy to commit wire fraud; violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate the IEEPA; and conspiracy to commit money laundering. The companies are accused of conspiracy to obstruct justice, for obstruction acts related to the investigation of the grand jury in the Eastern District of New York. Meng is individually charged with the crimes of bank fraud, wire fraud and conspiracies to commit wire and bank fraud.

The indictment notes that Huawei and its chief financial officer violated US law, in a fraudulent financial scheme that was detrimental to the security of the country, which was executed by carrying out transactions worth millions of dollars that directly violated the Transactions and Sanctions Regulations that the United States has in place against Iran. Furthermore, the indictment indicates that for more than a decade, Huawei used a strategy of lies and deceit to direct and grow its business[9].

The charges highlight Huawei's alleged disregard for United States law and observance of standard global business practices. The charges in this case relate to a long-standing scheme by the company, its chief financial officer, and other employees to mislead numerous global financial institutions and the U.S. Government, regarding Huawei's commercial activities in Iran.

5.3Some implications of the Huawei case in global criminal law

The Huawei case highlights the importance in the application and scope of the principle of extraterritoriality, as it happens with the crimes of transnational bribery, money laundering, accounting, electronic and financial fraud, as well as obstruction of justice, among others. In the application of the

[8]*Defendants include Huawei and two Huawei affiliates, Huawei Device USA Inc. (Huawei USA) andSkycom Tech Co. Ltd. (Skycom), as well as Huawei Chief Financial Officer (CFO), Wanzhou Meng (Meng).*

[9]*https://www.justice.gov/opa/press-release/file/1125021/download*

principle of extraterritoriality, the U.S. Department of Justice, through its investigation and prosecution of corporate crime, develops cases such as the federal crimes of wire fraud, bank fraud, money laundering, tax evasion and conspiracy to commit these crimes, as well as crimes of obstruction of justice to cover up this type of criminal conduct. Related criminal activity may also include falsehoods in reports and statements and obstruction of regulatory or criminal processes.

In the Huawei case, the Grand Jury charged the company with various crimes, including conspiracy to commit bank fraud, conspiracy to commit electronic fraud, conspiracy to defraud the United States, conspiracy to violate the law of economic powers of international emergency or International Emergency Economic Powers Act. Specifically, under the IEEPA Act, the attempt, conspiracy, or violation of any license, order, regulation or prohibition issued by the declaration of the President of the United States, resulting from economic sanctions against Iran is a criminal offense, as provided in title 50 of the United States Code in sections 1705 (a) and 1705 (c), promulgated in the United States Federal Regulations at 83 Fed. Reg. 11,393 (Mar. 14; 2018). Conspiracy to violate IEEPA, IEEPA violations, money laundering conspiracy and conspiracy to obstruct justice were also included as charges, as was an asset forfeiture count.

In the U.S. regulatory framework that works in parallel to the criminal process as to corporate crime, sanctions are civil and administrative in nature. Essentially, these are economic sanctions such as fines, suspensions and court orders. They may include civilly and administratively requesting a federal court to order the company to perform or not carry out an act.

In this context, it is relevant to reflect on the interests of the United States to protect its economic and social system through measures of various kinds such as regulatory and criminal. Since the American concept of the free market, which essentially proposes an economic model in which the quality of products and services, together with real price competition, are the prevailing natural economic forces, other artificial factors that create inequality in the system are illigitimate. This means that the company that resorts to bribes or

crime cannot prevail in the marketplace. In this regard, whoever violates the law simply cannot be rewarded.

The investigation in the Huawei case against the corporate entity and one of its highest-level executives is structured to vindicate violation of United States regulations, which penalize a natural or legal person, entity or country that conducts business with Iran, thus punishing conduct committed outside the United States but has direct or indirect impact on the country.

In addition, the US position in the Huawei case has generated economic reactions, regarding business between the United States and China, and the way ideas, technologies, transactions and business were exchanged despite the Chinese regime's censorship model. The President of the United States signed an executive order that effectively prohibits U.S. companies from doing business with telecommunications companies suspected of posing a risk to the national security of the United States[10]. Therefore, Huawei was added to a list of companies with which U.S. companies cannot trade unless they have a license."[11].

The Huawei case evidences the effect of a corporate and regulatory criminal investigation on big scale technology businesses and the impact of the extraterritoriality of the criminal law of the United States, and has also had repercussions on the development of Huawei's corporate objectives at a globalscale. The case is still under investigation but its transnational implications are evident, not only in business of a technological and economic nature, but also in the probable evolution and expansion of 4G, 5G and subsequent systems. Additional repercussions can be seen in the application of international judicial cooperation instruments such as the extradition and exchange of evidence. Similarly, these types of cases stand out due to the reputational implications for

[10] *The United States Department of Commerce determined that Huawei and its dozens of subsidiaries were included in a list of companies that are considered a risk to the national security of the country. The listing will prevent Huawei from buying US parts and technologies without seeking approval from the US government.*

[11] *Enhttps://www.nytimes.com/es/2019/05/22/huawei-google-android/*

the companies, the imposition of fines, business restrictions with third parties and regulatory controls.

The Huawei case is a representation of the industrial revolution, economic and data-driven digital intelligence revolution, reflecting the repercussions of the actions of a multinational company that allegedly violated the regulations of a third country, in this case the United States. As it is a corporation that provides services in the market for telecommunications devices and equipment, its operation broadly affects the economy and the digital society. The criminal process against the company by the United States may affect the operational, reputational and commercial capacity of the company in transnational relationships for technological and digital exchange on a global scale.

Digital intelligence driven by data and electronic platforms generate reorganization, automation and control of the company as a natural scenario for the provision of goods and services, as well as the anticipation of risks that may affect the company's corporate purpose. Digital security applications become communication instruments to anticipate risk scenarios against which effective control measures can be adopted to safeguard the interests of the company.

Artificial intelligence has been used to identify behaviors and predict crime through the analysis of data. The Huawei cases illustrates that this major global technological company did not leverage its capabilities to avoid the alleged commission of very serious extraterritorial crimes by the corporate entity and its highest-level leadership. In this regard, aside from a cautionary illustration of extraterritoriality in the corporate crime realm and the role of Big Data and Artificial Intelligence in corporate crime deterrence; the overarching lesson from the Huawei case is that compliance with the criminal law and regulatory norms are within reach of multinational firms through the strategic use of these tools. However, this requires corporate commitment to compliance and investment in these technological tools as directed by the highest-level leadership of the company. Despite having the technological tools well within its reach, given its global leadership in telecommunications, Huawei failed to leverage these tools.

In sum, cutting-edge technology such as Big Data analysis and Artificial Intelligence can assist corporations in complying efficiently with the legal and regulatory framework governing their particular industries. Nevertheless, human supervision in the design of preventive models utilizing these tools is critical to any successful launch of this technology. As noted herein, an algorithm can never take the place of thoughtful human judgment aware of the particular business risk environment.

The trend towards utilization of technology to ensure corporate compliance is critical in today's global economy. This sphere should be continuously studied in order to develop common standards that vindicate both corporate equities and legal requirements, including those of an extraterritorial nature.

Referencs

Alazab, m., & Broadhurst, R. (2016). Spam and criminal activity. Trends and Issues in Crime and Criminal Justice. https://doi.org/10.1080/016396290968326.

Archbold, J, (2018). Criminal pleading, evidence and practice. London: Sweet & Maxwell Ltd.

Arkin, R, (2008). Governing lethal behavior: Embedding ethics in a hybrid deliberative/reactive robot architecture part I: Motivation and philosophy. In Proceedings of the 3rd international conference on human robot interaction—HRI'08, https://doi.org/10.1145/1349822.1349839.

Ballester, J, (2019), "Compliance y las nuevastecnologías, Ciberseguridad", Madrid, ed. Aranzadi.

Beck, U. (2008) "La sociedad del riesgo mundial. En busca de la seguridad perdida", Barcelona.

Bergman, P, y Berman-Barret, S, (2003), " The criminal law Handbook". 5° Ed. USA: Nolo.

Bixby, M, (2010), “The Lion Awakens. The Foreign Corrupt Practices Act 1977 to 2010”, 12 San Diego Int´l L.J. 89.

Bock, D. (2013) “Compliance y deberes de vigilancia en la empresa” en AAVV, “Compliance y teoría del derecho penal”, Madrid.

Chen, y. C., Chen, P. C., Hwang, J. J., Korba, L., Ronggong, S., & Yee, G. (2005). An analysis of online gaming crime characteristics. Internet Research, 15(3).

Chesney, R., & Citron, D. (2018). Deep fakes: A looming crisis for national security, democracy and privacy? Lawfare, February 21, 2018. https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy.

Feijoo Sánchez, b. (2016), “El delito corporativo en el Código Penal Español”, Pamplona: ed. Aranzadi.

Gómez-Jara Diez, C, (2005), “La culpabilidad penal de la empresa”, ed. Marcial Pons, Madrid.

Khulen, l, (2013), “Compliance y teoría del Derecho penal”, ed. Marcial Pons. Madrid.

Quest L., Charrie, A., andSubas, R. (2018), “The Risks and Benefits of Using AI to Detect Crime”, enhttps://hbr.org/2018/08/the-risks-and-benefits-of-using-ai-to-detect-crime

Mallada Fernández, C, (2019), "Money laundering and ICT: National and European legal framework, modus operandi and cryptocurrencies",ed.Aranzadi.

Morabito, V, (2015), “Big Data and Analytics”. http://37.156.146.163/PUB/BooKs/2014-

2015/Springer%20Publishing%20Big%20Data%20and%20Analytics,%20Strategic%20and%20Organizational%20Impacts%20(2015).pdf

Navas Navarro, S., y otros, (2017), “Inteligencia artificial. Tecnología Derecho”, Valencia: ed. Tirant lo Blanch.

Ramírez Barbosa, P, (2019), “El delito de Corrupción Trasnacional en Estados Unidos y Colombia: alcance del principio de extraterritorialidad de la Ley Penal Norteamericana y Compliance”, en Derecho Penal, Parte Especial, Universidad Externado de Colombia, Bogotá.

Ramírez Barbosa, p, and Ferré Olivé, J.C. (2019) “Compliance, Derecho penal corporativo y buena gobernanza empresarial”, Bogotá. Ed Tirant lo Blanch.

Ramírez Barbosa, P, (2018) “La ley contra las prácticas corruptas en el extranjero. La FCPA de Estados Unidos: “compliance”, extraterritorialidad y responsabilidad de la persona jurídica. Reflexiones acerca del caso Odebrecht” en AAVV, “Desafíos del Derecho penal en la sociedad del Siglo XXI”, Bogotá. Ed. Temis.

Richard H. Fallon, J., “The Rule of Law” as a Concept in Constitutional Discourse, 97 COLUM. L. REV. 1 (1997); Amir N. Licht et al., Culture Rules: The Foundations of the Rule of Law and Other Norms of Governance, 35 J. COMP. ECON. 659 (2007); Daniel A. Farber, The Rule of Law and the Law of Precedents, 90 MINN. L. REV. 1173 (2005) (discussing the relationship between stare decisions and the rule of law).

Valls Prieto, J, (2017), "Criminal legal problems associated with new techniques for the prevention and prosecution of crime using artificial intelligence", Madrid, Ed. Dykinson, pages. 17 a 33.

Submetido em 10.03.2020.
Aceito em 10.03.020
Artigo publicado a convite dos Editores.