Introduction – AI in the economic sector: prevention and responsibility

(https://doi.org/10.47907/livro2021_4c1)

Susana Aires de Sousa[1]

> 'What sort of things do *you* remember best?' Alice ventured to ask.
> 'Oh, things that happened the week after next,' the Queen replied in a careless tone. 'For instance, now,' she went on, sticking a large piece of plaster on her finger as she spoke, 'there's the King's Messenger. He's in prison now, being punished: and the trial doesn't even begin till next Wednesday: and of course the crime comes last of all.'
> 'Suppose he never commits the crime?' said Alice.
> 'That would be all the better, wouldn't it?'
>
> Lewis Carroll, *Through the Looking Glass*

I. A digital transition is happening in the economic sector[2]. New technology – machine learning, language processing, robotics, electronic platforms, blockchain, cognitive computing, quantum computing… –, although all these are at different stages of development, is already integrating innumerable economic and financial activities. However, technologically accelerated evolution, in parallel with the digitalization of markets and the massive creation of data, have together favoured the emergence of algorithms capable of extracting and structuring, from

---

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

[2] Theo Lynn / John G. Mooney / Pierangelo Rosati / Mark Cummins (Editors), *Disrupting Finance. FinTech and Strategy in the 21st Century,* Macmillan, 2019; also, dedicated to the challenges of Blockchain and AI, the *Journal of Corporation* Law, Volume *46, Number 4 (2021*), https://jcl.law.uiowa.edu/volume-46-number-4

big data, relevant (and economically valuable) information[3]. Typical advantages of complex computerized systems, such as the enormous capacity for data analysis (already impossible for human intelligence) are now upgraded with new AI techniques, with predictive and prescriptive skills. This predictive ability makes AI algorithms particularly suitable for and efficient at performing several tasks such as compliance obligations, fraud detection, cyberattacks prevention or as a simple commercial tool (in customer service and assistance, for example).

These advantages have long attracted the attention of several stakeholders in the economic sector. The impact of AI on the financial and banking system is undeniable. As the financial sector navigates risky choices based on probability judgements, the most favourable scenario is fashioned for algorithms "to do their thing", e.g., credit risk assessment, market risk analysis, economic operations performance (calculating measuring and identifying risks, probabilities and strategies), and fraud detection, etc.

Exposed in recent decades, in the wake of the 2008 financial crisis, to enormous pressure from regulators in the pursuit of their business, banks have found solutions in the advantages offered by new technologies. "Banking has always been particularly open to technical innovation and progress"[4]. However, the appearance of AI has brought about a real revolution in the financial field. Just consider the veritable digitalization of the institution, with the emergence of fully digital banks, without any physical existence. The securities market has also undergone profound changes with the introduction of trading algorithms capable of automating and accelerating transactions, increasing efficiency, velocity and liquidity[5]. The threat of a systemic risk linked to the behaviour of algorithms is however a recurrent concern and should not be ignored.

---

[3] Anabela Miranda Rodrigues / Susana Aires de Sousa, «Algoritmos em contexto empresarial: vantagens e desafios à luz do direito penal», *Julgar 45*, p. 193--215.

[4] Pedro Maia, Part I, Chapter 1.

[5] Douglas W. Arner / Janos Barberis / Ross P. Buckley, «The Evolution of FinTech: A New Post-Crisis Paradigm?», University of Hong Kong Faculty of Law Research Paper No. 2015/047, UNSW Law Research Paper No. 2016-62, SSRN: https://ssrn.com/abstract=. Also Gregory Scopino, *Algo bots and the Law*, Cambridge University Press, 2020, p. 177

Technologies do allow costs to be cut, switching from people to algorithms, and do enable better risk management[6]. A risk analysis of operations and operators, in compliance with the obligations imposed by regulators, seems to offer means of detection or even prevention of financial fraud, "evaluating the best ways to protect their systems, their data, and ultimately their clients"[7]. It should therefore come as no surprise that algorithms, with their ability to analyse patterns and detect suspicious movements, have established themselves as a powerful tool for compliance and fraud prevention and detection. AI solutions, although expensive[8], promise automated continuous monitoring, relieving the company of the costs associated with self-regulation and, on the other hand, making it easier for the regulator to quickly access information in case of non-compliance[9]. Fraud can be a financial sign or transfer, whose irregularity – undetectable to the human eye – is easily identifiable or flagged by an algorithm capable of comparing and analysing big data.

FinTech (Financial Technology), RegTech (Regulatory Technology) and SupTech (Supervisory Technology) represent this digital shift, both on a practical as a narrative level: whether in the banking sector or in the field of capital markets, architecture, structure, management and operations have been profoundly altered by networks of computerized systems that guide countless digital movements and transactions[10]. In a subsequent step, artificial intelligence techniques have revealed

---

[6] Butler / Brooks, «On the role of ontology-based RegTech for managing risk and compliance reporting in the age of regulation», *Journal of Risk Management in Financial Institutions*, Vol. 11 (2018), p. 19 e ss.

[7] Saqib Aziz / Michael Dowling, «Machine Learning and AI for Risk Management», *Disrupting Finance*, Palgrave Macmillan, 2019, p. 43.

[8] Aldridge and Krawciw note that in recent years investment in financial technology has grown by 201% worldwide, cf. «Real-time risk: What investors should know about FinTech, high-frequency trading, and flash crashes» Hoboken, NJ: Wiley, *apud* E. Monaco, «What Fintech can learn from high-frequency trading)», *Disrupting Finance*, Palgrave Macmillan, 2019, p. 52.

[9] Cf. Tom Butler / Leona O'Brien, «Artificial intelligence for regulatory compliance: Are we there yet?», *Journal of Financial Compliance*, Vol. 3, N 1, 2019, p. 45.

[10] Douglas W. Arner / Janos Barberis / Ross P. Buckley, «The Evolution of FinTech: A New Post-Crisis Paradigm?», University of Hong Kong Faculty of Law Research Paper No. 2015/047, UNSW Law Research Paper No. 2016-62, SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676553

themselves to be an auspicious instrument for monitoring transactions and consequently as a powerful tool in the investigation of fraudulent practices in the financial market. Financial cybersecurity has been in fact one of the sectors leading this field.

These aspects, among others, are covered in depth in the first part of this book, which is entitled *Prevention*.

Pedro Maia in "Intelligent Compliance" describes the compliance obligations felt by the banking sector and the way in which new technologies have allowed institutions to respond to these demands. The complexity of the compliance system to which banking institutions are subjected, as a part of a "legislative tsunami" unleashed by the 2007-2008 financial crisis are described and analysed in detail. Technology became a powerful instrument of compliance responding to a duty of risk identification and mitigation. At the same time, the author does not omit to warn us of the possible consequences and costs of unlimited trust being placed on algorithms: the exposure of the financial system to new and significant risks, making the system – again – more fragile.

Alexandre Soveral Martins, in the chapter "Algo-trading", unveils a set of reflections on algorithmic trading, pointing out both its advantages and volatility risks. The reaction to the risk of instability, leveraged by High Frequency Trading (HFT), forced regulators to act in order to ensure or determine the conditions of trust that are essential to the functioning of this market. Risky behaviours facilitated by HFT are also listed by the author. Many of these behaviours are associated with market manipulation such as ping orders, phishing, quote stuffing, spoofing, wash trading, slow traders, etc.

José Ricardo Marcondes Ramos, in the chapter "The use of Big Data and Artificial Intelligence to prevent and detect fraud", explores the ideas of digital forensics through the use of AI. This paper focusses on the discussion about the role that AI is already playing in fraud detection. The enormous amount of data collected and extracted from all sort of technologies and devices (computers, platforms, phones, smart watches, etc.) is feeding the development of this new type of digital forensics based on AI techniques. Big data allows supervised and unsupervised training (alongside other methods as social network

analysis) to transform AI into a powerful tool capable of identifying patterns of fraud or suspicious activities connected with financial fraud, money laundering, financing of terrorism, market manipulation or corporate crimes.

II. However, the use of AI comes with risks and costs, in particular risks connected with algorithmic unpredictability that may cause harm to protected interests, whether individually or collective owned (altered prices, market manipulation, manipulated advertising, privacy attacks).

Scholars have pointed out numerous examples of automated decision systems going wrong such as traffic accidents with automated driving systems[11], spoofing orders on the market securities, phishing threats favoured by the internet of things[12], or even racist or biased outcomes[13].

The risks signalled of AI may indeed materialize in harmful wrongdoing, bringing about the question of who is responsible for them. A new set of problems emerge. The dystopian nature of complex computational systems make imputational categories seem inadequate. From the perspective of the human or corporate person involved in the manufacture, programming or use of the system, the intervention of the machine renders, sometimes, the harmful event unpredictable. Are our responsibility systems and the existing models of liability adequate to respond to harmful events connected with algorithmic decisions?

---

[11] Mihalis Diamantis, Part II, Chapter 2.

[12] Steven Furnell, «Technology Use, Abuse, and Public Perceptions of Cybercrime», *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan (ed. Thomas J. Holt / Adam M. Bossler), 2020, p. 45 e ss.

[13] Alan Rubel / Clinton Castro /Adam Pham, *Algorithms and Autonomy. The ethics of automated decision systems*, Cambridge University Press, 2021, p. 137 e ss., point out some examples: in 2018, an Uber-automated driving system failed to recognize a bicyclist, whom it struck and killed; in 2012, the Target Corporation received international attention when, based on predictive analytics and an automated advertising system, it sent fliers targeting women seeking prenatal products to a minor before she had revealed her pregnancy to one of her parents; in 2017, the news organization ProPublica was able to use Facebook's automated system to make an ad buy targeting users with anti-Semitic affiliations.

One could argue that those risks may be diminished by creating more accurate machines with exceptional predictive capacities. As Aziz and Dowling emphasise, as the organisation and analysis of data becomes more targeted and focused through AI we are "able to accurately know in advance the risks, be they company, market, operational or credit risks"[14].

Accuracy demands data, big data. Constant monitoring (of agents, transactions, values, connections, financial movements, website visits) becomes one of the main sources of data collecting. This "surveillance" happens both in a limited environment (*e.g.*, the surveillance of employees[15]) or on a wide scale (*e.g.*, internet cookies). And with the extraction and collection of data, privacy – for example – become imperilled.

The paradox is clear: on one hand, the efficiency and predictive capacity of algorithms make them a tool for compliance and prevention of offences; on the other hand, this capacity of the machine, driven by big data, raises disturbing alarms linked to a progressive transformation of legal and social systems. This leads to the final question: faced with an AI capable of assessing risks, anticipating harms and acting to prevent them, does it make sense to have a liability system whose categories are built on an event that took place in the past?

These questions, among others, are raised on Part II, under the title "Responsibility".

Anabela Miranda Rodrigues introduces us to the concept of "intelligent corporation" on the chapter "The Last Cocktail – Economic and Financial crime, Corporate Criminal Responsibility and Artificial Intelligence". In a digital economic market, corporations use AI for many purposes, such as business risk assessment, management or monitoring the company. Algorithms are there, making (automated) decisions with a higher degree of autonomy. If legal compliance seems to get more efficient, adequacy problems may rise when confronting

---

[14] Saqib Aziz / Michael Dowling, «Machine Learning and AI for Risk Management», cit., p. 44

[15] Richard A Bales / Katherine Van Wezel Stone, «The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace», *Berkeley Journal of Employment and Labor Law* 41 1 (2020), UCLA School of Law, Public Law Research Paper No. 19-18, SSRN: https://ssrn.com/abstract=3410655

legal models of corporate liability with harms connected to algorithm behaviour. "Still poorly redone from the trapdoor of vicarious responsibility and ambiguities of the organizational defect, finding models of responsibility for corporate crime is, for criminal lawyers, once again urgent".

Miahailis Diamantis, in the Chapter "Algorithmic Harms as Corporate Misconduct", performs a detailed analysis of the existing conceptions of liability, taking it as a premise that "algorithmic harms" do exist. Addressing the algorithmic accountability gap the author is focused on "figuring how to fit algorithms" into liability regimes based on corporate or natural actions. Answering the challenge, the solution – for the present time – is developed around the idea of "beneficial-control account" as criteria for treating algorithmic injuries as corporate actions, covered by corporate law. However, the gap may be open in a disruptive scenario, if the future brings us a world where algorithms are self-performing, self-executing and operate under the control or for benefit of no one. In that case there is no one – corporate or natural – to hold to account.

Christoph Burchard ends the second part of this book with the Chapter "Artificial Intelligence and the End of Criminal Law. On the Algorithmic Transformation of Society", raising disquietening questions about the social and legal transformations created by algorithms. For example, what transformations would result from the introduction of AI applications (predictive policing or "intelligent" sentencing tools) into the system of criminal justice? In the author's own words "what is the status of freedom (especially in a surveillance society needed to power Big Data driven algorithms), trust (especially under the zero trust paradigm that underlies many risk assessment algorithms) and future (especially when algorithms make predictions based on past data) once AI enters into the administration of criminal justice?" These are indeed questions that the criminal law needs to address today "in order to come up with a criminal law that is both (for pragmatic reasons) open to technology as well as (for humane reasons) sensible".

III. Advances in science and technology can be extremely useful in the pursuit of economic efficiency but also of fairness and justice; they

can also be an accelerated path to a securitarian type of law, capable of sacrificing, in a few steps, values conceived as essential in today's society. Some examples may be briefly pointed out, such as the right to privacy and intimacy or the freedom of expression and of choice. Choosing a securitarian law, based on the potential and possibilities that this new technology presents, can have a very high cost in the restriction of fundamental rights by promoting a criminal response to a crime that does not *yet* exist. And with that, a person "labelled" as high-risk by the machine is deprived of the ultimate eventual possibility of not carrying out the (future) crime. A securitarian law, disconnected, in time and space, from a criminal fact (and, therefore, from a real harm to legal values), centred on the agent . It would be a "punitive law" with punishment but no crime to punish, so well portrayed by Alice's doubts in dialogue with the Queen in the beginning of this introduction.