*Insights & Analyses*

# The Implementation of New Technologies in Anti-corruption Policies

Federica De Simone*

**Abstract**

The text examines the impact of new technologies in the field of criminal law, focusing on the prevention and repression of corruption. It explores the advantages derived from the use of tools such as artificial intelligence and advanced algorithms, highlighting the opportunities to improve investigation efficiency and increase transparency. However, it also examines the risks associated with the automation of judicial decisions, including the potential increase in inequality and the threat to fair justice. Finally, it emphasizes the importance of a balanced and mindful approach in adopting such technologies, with particular attention to protecting fundamental rights and the need for adequate regulations to mitigate emerging risks.

## I. Preface about the Relationship Between Technological Development and the Legal System

With a view to introducing the topic of the relationship between new technologies and criminal law, two basic premises are indispensable.[1]

The first consideration is of a general nature and relates to technological progress and the speed with which new tools are becoming part of our lives, sometimes even without us becoming aware thereof. It is there for all to see that mankind is going through the most innovative period ever seen, in which scenarios that were unimaginable only a short time ago are coming to fruition and offering remarkable opportunities. The Marxist conception of progress considers the latter (which is of a technological nature) to be the rule that underpins evolution,[2] with the result that any attempt to block or even delay development would be impossible (and futile). History has, in fact, taught us that the fear of apocalyptic scenarios following the introduction of new scientific discoveries have often vanished, making way for positive epoch-making changes. This was the case with writing, which, according to the Greek philosophers, would lead to a loss in the ability to

* Lecturer in Criminal Law, University of Campania Luigi Vanvitelli.

[1] The topic seems to be altogether new. Attempts to implement computational calculations in judicial decisions go back, however, as far as Leibniz. Cf P. Moro and C. Sarra, *Tecnodiritto* (Milano: Franco Angeli, 2017), 32. For a general overview, see L. Picotti, 'Diritto penale e tecnologie informatiche: una visione d'insieme', in A. Cadoppi et al eds, *Cybercrime* (Torino: UTET, 2019), 35.

[2] K. Marx, 'Das Kapital, Hamburg 1867-1894', III, in A. Macchioro and B. Maffi eds, *Il capitale* (Torino: UTET, 2017), 3.

remember by heart, narrate and use one's own imagination. The same was the case with the advent of the printing press, which - according to its detractors - would, by making knowledge available to everyone, have led to a serious crisis in humanity, as well as television, which was accused of negatively affecting man's ability to socialize with his fellow human beings.[3]

The idea that artificial intelligence could play a role in improving the timeframe within which justice is served, rather than just being a system of neural networks to be used in the fight against corruption is to be welcomed, albeit with an adequate degree of caution.

The second premise is of a technical nature and concerns the need - which can no longer be postponed - for legislation to be introduced that regulates the use of new technologies on the basis of legal principles. This is a need felt by many and also clearly transpires from the numerous documents generated at both supranational and national level, starting from the Ethical Charter on Artificial Intelligence[4] of 2018 and the European Commission's White Paper[5] of 2020 and going so far as the Proposal for a Regulation on a European Approach for Artificial Intelligence presented by the European Parliament and the European Council in 2021.[6]

The European Union is, in fact, of the opinion that the risks generated by the massive use of these technologies may, regardless of their field of application, be too high, especially when compared to the need to protect human rights. The most obvious risks arise from privacy and personal data infringements and discriminatory behavior, as well as the denial of access to justice. However, this list is for illustrative purposes only and there may be many other rights that are infringed or endangered.[7]

Internationally, the European position is not shared by everyone. Diametrically opposed - for example - is the American position, which favours a liberal approach (in the same vein of the free marketplace of ideas espoused by John Milton).[8]

One could theoretically agree with such a position if it were posited as being the basis for freedom of the press alone. The full and unconditional guarantee of the right to freedom of speech in all its forms could, in fact, lead to truth being affirmed in the same way as goods impose themselves in a free marketplace.

[3] W. Schmitz, *Oltre Benjamin. «La riproducibilità tecnica della scrittura» e la diffidenza verso la stampa tipografica nell'Europa del Quattrocento* (Bologna: TECA, 2021), 7, 11.

[4] Available at https://tinyurl.com/yus24dwf (last visited 30 September 2024).

[5] Available at https://tinyurl.com/4kzf394h (last visited 30 September 2024).

[6] The regulation proposal, presented by the European Commission on April 21, 2021, named the Artificial Intelligence Act, is in the final stages of adoption by the European Parliament and the Council (the approval of the final text occurred on 2 February 2024), according to the ordinary legislative procedure. Available at https://tinyurl.com/ydsdr8ea (last visited 30 September 2024).

[7] Available at https://tinyurl.com/pke4bfdd (last visited 30 September 2024).

[8] John Milton conceived the metaphor of the free market applied to ideas when he wrote the essay 'Areopagitica' in 1644. See M. Gatti and H. Gatti, (for the Italian version thereof), *Discorso per la libertà di stampa* (Milano: Bompiani, 2002). See how the marketplace of ideas theory is explained by, among others, G. Pitruzzella et al, *Parole e potere. Libertà di espressione, hate speech, fake news* (Milano: Egea, 2017).

Nonetheless, the idea of specifically applying the principle of competition to the circulation of ideas seems somewhat inappropriate and, in fact, encounters a first limitation when dealing with the problem of fake news.[9]

Currently, there is an uncontrolled dissemination of fake news through the Internet that can in no way be circumscribed. Several studies have, in fact, emphasized the risks that this may entail in terms of the resilience of democratic systems, so much so that lawmakers have been called to intervene on several levels.[10]

The American approach that has been adopted appears even less acceptable if it is also applied to the use of new technologies such as artificial intelligence, algorithms and neural networks. It is hard to see how the approach of leaving the free market to decide which technologies may - for example - solve the problem of bias, let alone the so-called *black box*, could be successful. Indeed, rather than responding to a need to provide safeguards and protections, this approach seems to conceal far less noble aims, such as those of a predominantly commercial and consumerist nature. We need only mention the policies of giants such as *Facebook* or *Amazon,* which employ in the US discriminatory or tracking algorithms that would not be allowed in Europe precisely because of the soft law and hard law rules that already in force.

Lastly, the Chinese approach does not attempt to disguise the objectives of exercising full control over society and explicitly intends, with a view to maintaining the *status quo*, to exploit precisely those aspects that are, for us Europeans, of vital importance for our fundamental rights.

The unstoppable nature of progress and the need that is felt at the same time to regulate it seem an essential pre-condition for acknowledging that the law has a central role and is called - as always happens in moments of epoch-making change - to perform the immunizing and stabilizing role theorized by Luhmann.[11] This is particularly significant when using artificial intelligence systems, which find themselves playing very different roles within society and having implications of both a legal and ethical nature.

[9] See on this topic T. Guerini, *Fake news e diritto penale* (Torino: Giappichelli, 2020).

[10] At European level, the last relevant measure on this subject has been the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC of 15 December 2020, on which agreement was reached on 23 April 2022. Unfortunately, the measure was rejected by the Parliament on 13 June 2022 on account of the fact that the text was deemed not to be in line with the contents of the agreement. It is, nevertheless, an important legislative point of reference and it will most likely see the light of day once an agreement is reached. The debate in the Italian Parliament has given rise to some legislative proposals, which have - however - not been followed up. We take the liberty of referring to F. De Simone, ' "Fake news", "post truth", "hate speech": nuovi fenomeni sociali alla prova del diritto penale' *Archivio Penale web*, 1, 1-49 (2018).

[11] N. Luhmann, 'Ausdifferenzierung des Rechts: Beiträge zur Rechtssoziologie und Rechtstheorie, Frankfurt 1981', in R. De Giorgi ed, *La differenziazione del diritto: contributi alla sociologia e alla teoria del diritto* (Bologna: il Mulino, 1990), 1-397.

## II. Some Possible Classifications

The legitimate and illegitimate uses of new tools also hold relevance for criminal law, prompting reflections on cases where there is a need to counter new criminal phenomena, as well as those where new technologies prove to be effective tools against ordinary crime. This is why, in the absence of specific regulations capable of providing adequate responses to the new challenges posed by artificial intelligence, it may be useful to briefly review the various roles that new technologies can assume in the field of criminal law.[12] This not only allows for the identification of possible existing and future scenarios but also highlights any regulatory gaps that lawmakers may be called upon to fil.

New technologies could be classified in a number of ways for the purpose of categorizing the legislation that is applicable to the topic that is being dealt with here (with particular regard to criminal law).

A first category could lead to distinguishing new instruments on the basis of whether they are actively or passively involved in the criminal offence and whether they take on the role of perpetrator or victim of the offence.

The situations in which artificial intelligence behaves in the same way as an offender are part of a fairly well-known and wide-ranging case history that is not without its critical aspects. First of all, a distinction must be made between situations in which the system in question has been created for the purpose of committing a criminal offence and situations in which, on the other hand, the criminally relevant fact stems from a mistake made by the machine itself. Non-exhaustive examples of the first type of scenario are software designed to disseminate false information and/or injure the reputation of others, systems designed to destroy other IT facilities, autonomous weapons that engage in conduct that is punishable under the wartime military criminal codes. On the other hand, all those situations in which new technologies negligently cause injury to protected legal assets come within the scope of the second scenario, even though the use thereof is legal.

Cybersecurity encompasses most of the cases in which new systems can be considered victims of crime, since they are victims of cyberattacks that lead to data being lost, and systems being altered and even destroyed.[13] What appears to be a first and obvious distinction stemming from the classic categories of the

[12] For a more in depth exploration of this point, please refer to the following resources, F. Basile, 'Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine' *Diritto penale e uomo*, 29 September 2019, 9; for an analysis of the ethical issues raised by the use of new systems, please see G. Tamburrini, *Etica delle macchine. Dilemmi morali per robotica e intelligenza artificiale* (Roma: Carocci, 2020); P. Benanti, *Oracoli. Tra algoretica e algocrazia* (Roma: Luca Sossella editore, 2018).

[13] Denial of service attacks are the most commonly used tool for damaging IT systems in general and, in such cases, there are many different victims. Not only can artificial intelligence, in fact, be damaged, but the loss of data, for instance, can lead to a violation of data protection rules. Reference is made to F. De Simone, 'La rilevanza dei delitti contro l'integrità dei dati dei programmi e dei sistemi informatici al tempo della guerra russo-ucraina' *Giurisprudenza Penale Web*, 6 July 2022, 7-8, 125.

theory of crime encounters a significant limitation in the consideration that the use of the terms *perpetrator* and *victim* in the case of artificial intelligence cannot be used in the technical sense of the term, since no form of legal personality has yet been recognized that could justify such a *status*.[14] Under current legislation, the role played by AI in both cases should be taken up by the system's owner, and even then the identification thereof is not easy, since there are many players involved.[15] It would, therefore, be more appropriate to consider the new systems as an instrument or as a material object of the crime, at least until the issue of the recognition of so-called *electronic personality*[16] is not dealt with.

The introduction of a third category alongside physical and legal liability could have far-reaching consequences and require the system to be rethought, especially with regard to the issue of punishment and the list of penalties to be imposed.

A second category could be identified by taking into account the functions performed by artificial intelligence when preventing crime and when ascertaining criminal offences at trial. In particular, reference is made to cases in which the new systems are used as if they were a technical expert. This is a role that can be played in support of the criminal investigation police while predicting, preventing and detecting crime, or assisting the courts to assess the social dangerousness of an individual or even decide the fate of a case.[17] Tools such as *XLaw*[18]that are used at the Naples police headquarters for the purpose of preventing crime, or algorithmic

[14] S. Riondato, 'Robot: talune implicazioni di diritto penale', in P. Moro and C. Sarra eds, n 1 above, 1, 85.

[15] The parties affected by the way in which artificial intelligence works are the owner of the system, the operator and his programmer. It is debated which of these should be legally liable and to what extent. On this point see C. Piergallini, 'Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?' *Rivista Italiana di Diritto e Procedura penale*, 4, 1745 (2020).

[16] Art 59(f) of the European Parliament's Resolution of 16 February 2017 containing recommendations to the Commission about civil law rules on robotics (2015/2103(INL), states that account must be taken of the impact of creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently. Available at https://tinyurl.com/ypsejyw9 (last visited 30 September 2024). The field in question is that of civil liability and has raised many criticisms and dissenting opinions. The possibility of introducing a third category of personality that also has criminal law implications has already been examined in depth by legal scholars. See G. Hallevy, 'The Basic Models of Criminal Liability of AI Systems and Outer Circles' *SSRN*, 11 June 2019; U. Ruffolo, 'The Problem of Electronic Personhood' *Journal of Ethics and Legal Technologies*, 2 April 2020, 2(1), 75.

[17] V. Manes, 'L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia', in U. Ruffolo ed, *Intelligenza Artificiale. Il diritto, i diritti, l'etica* (Milano: Giuffrè 2020), 547.

[18] G. Di Gennaro and E. Lombardo, 'Intelligenza artificiale e politiche di sicurezza urbana: verso quali modelli?', in G. Riccio et al eds, *Intelligenza artificiale tra etica e diritti* (Bari: Cacucci editore, 2020); M. Iaselli, 'X-LaW: la polizia predittiva è realtà' *Altalex*, 28 novembre 2018; E. Lombardo, *Sicurezza 4P - Lo studio alla base di XLAW per prevedere e prevenire i crimini predatori* (Venezia: Mazzanti libri, 2019).

systems such as *Compass*[19] in the USA and *Hart* [20] in England used to assess the risk of recidivism when deciding whether to apply an alternative measure, have already been successfully used for some time now by the police or the courts, even though there are a few critical issues arising therefrom that will be discussed below.

The use of algorithmic consultants in legal proceedings should be less perplexing than the use of artificial intelligence for predictive purposes. Indeed, codes of procedure already envisage the possibility of an expert assisting the judge in his or her work and, in this specific case, the expert would put a much greater quantity of data at the justice's system disposal than would be the case if a human expert were involved. What raises doubts in jurists is the use of AI for predictive purposes, even though they (and in particular criminal lawyers) should be accustomed to probabilities and percentages, given that they are the norm when having to establish the causal link between an event and conduct.

Indeed, as far as predictiveness is concerned, a distinction must be made between prediction, predictability and probability, also on account of the fact that the term predictive in Italian does not have an unequivocal meaning. The common feeling is, in fact, that predicting a given event is tantamount to guessing the future as if one were an oracle.[21] For its part, the notion of probability refers to a statistical inference, that is to say the process of inferring a result from a given percentage, which, even though it does not mean certainty from a scientific point of view, gives a precise idea of the uncertainty thereof (which, when looking at predictability, is in turn a dystopian idea that instead recalls in a certain sense certainty).

It sounds like a tongue twister but it is not because - as mentioned earlier - these are concepts that are particularly close to criminal lawyers' hearts. Probability is at the basis of the causal link[22] that connects the event to the perpetrator's conduct. Predictability is the basis of the principle of legality enshrined in Art 25, para 2 of the Italian Constitution, but we also find it, for example, in the assessment of the subjective element, whereas predictability seems to be placed, for example, in the context of the assessment of the risk of recidivism. On the other hand, the assessment of dangerousness and so-called risk assessment are concepts created at the beginning of the 20th century by criminological science. When a judge makes an assessment of the dangerousness of an offender while deciding whether an

[19] S. Carrer, 'Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin' *Giurisprudenza Penale Web*, 24 April 2019, 4; Han-Wei Liu et al, 'Beyond State v Loomis: artificial intelligence, government algorithmization and accountability' *International Journal of Law and Information Technology*, 12 February 2019, 27, 2, 122–141.

[20] M. Oswald at al, 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality' *Information & Communications Technology Law*, 27, 2, 223-250 (2018).

[21] R. Berk, *Machine learning risk. Assessment in criminal justice settings* (Switzerland: Springer, 2019).

[22] Legal scholars argue that causal models - as well as the subsumption thereof under the scientific laws covering them - can be combined with predictive models, provided that these are accurate and can be interpreted; R. Berk, n 21 above, 155.

alternative measure should be granted, no one asks whether he is predicting the future or applying a statistical probability.[23]

Artificial intelligence encapsulates, through the machine-learning process on which it is built, all of these characteristics and should not cause alarm *per se*, since these processes are analogous to those developed by humans, with the difference that new technologies achieve better results with respect to the purposes for which they are programmed. This is only possible thanks to the enormous amount of extra data that artificial intelligence is capable of processing in comparison to the human mind (and nothing else).[24]

## III. Problematic Aspects

Even before circumscribing this issue's scope with respect to the matters dealt with in criminal law, we must spend some time on the problems - that do not seem easy to solve - posed by the introduction of new technologies, starting with the definition thereof.

Machine learning and deep learning, weak and strong artificial intelligence, neural networks, algorithms, chatbots and blockchains are not terms to be used in the alternative as synonyms, but indicate different technologies that have their own peculiarities, to which different regulations should be partly addressed.

At the same time, it is probably wrong, in light of the speed at which they are being updated, to pretend to hamper new technologies with precise technical definitions that could force lawmakers to continuously adapt legislation thereto. The difficulty of introducing precise definitions in this area is currently such that even the European Parliament advises against doing so,[25] especially avoiding the risk of provisions of law that do not keep up with the speed at which technologies are updated.

Having posed the question of definitions in this manner, a contradiction becomes evident that seems insurmountable, insofar as the decision not to adopt flexible definitions meets the need to update new systems in real time, but cannot be reconciled with the respect of certain principles, first and foremost that of crafting definitions without fail. This could be satisfied if lawmakers were to adopt a legislative technique that proceeded by cases and hypotheses. Such choice would, however, give rise to many difficulties, starting with the risk of legislative overkill.

[23] The assessment of criminal risk in terms of anti-social behaviour is based on probability and the identification of risk factors. See S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion* (Switzerland: Springer, 2020), 147.

[24] B. Occhiuzzi, 'Algoritmi predittivi: alcune premesse metodologiche' *Diritto Penale Contemporaneo*, 21 May 2019, 2, 393.

[25] The European Parliament promoted, in its 2015 motion for a resolution on robotics, the search for a common yet flexible notion that had precisely this in mind. Available at https://tinyurl.com/3pcn9nt9 (last visited 30 September 2024).

Great weight must, therefore, be given to the problems posed by the so-called *black box*, that is to say the protection of data used for machine learning, and the quality thereof. These are all issues for which lawmakers, even though they have envisaged specific rules therefor, do not seem to offer effective solutions.[26]

An obvious example of this is the fourth principle of the Ethical Charter,[27] which, in introducing technical transparency and knowability, refers to the possibility of reconstructing the machine's decision-making process.[28] This principle is, in fact, difficult to implement, insofar as the self-learning system rules out, by its very structure, such a possibility. The legal claim cannot, in fact, even be satisfied by the machine's programmer, who maintains control exclusively over the initial data packet with which he commenced the learning process.

The complexity of this issue transpires, even before constituting a legal problem, from the scientific validation thereof: if a method cannot be proven, the result cannot be validated. This is Galilei's dogma of reproducibility[29] that can be extended well beyond strictly scientific confines: just think of the impact that such systems can have when used to present the prosecution's case in criminal proceedings. What is the law to be applied, when a piece of evidence is indicated and the path that led to it cannot be identified precisely on account of the problem of the *black box*? This question has arisen, for instance, with reference to the *Zero Trust* algorithm that is employed for the purpose of the prevention and prosecution of corruption in China discussed below.

The impossibility of scientific validation is also inferred from the seventh of the Asilomar 23 principles[30] drawn up in 2017, in the drafting of which some of the most influential scientists took part. This provision states that, should an artificial intelligence system cause harm, it *should* be possible to ascertain why (with the use of the verb in the conditional tense suggesting the real possibility of it being implemented).

As far as the problem of data and its quality is concerned, the myth of the neutrality of machines is no longer believed by experts, even though the belief that artificial intelligence is more objective than human beings and is, as such, preferable,[31] persists in the public at large. It is, by now, a well-known fact that new tools suffer - like humans - from so-called biases, (ie the prejudices that condition the programmers' thinking and that, inexorably, spill over into the data fed into

[26] See C. Casonato, 'Intelligenza artificiale e giustizia: potenzialità e rischi' *Diritto Penale Contemporaneo online*, 16 October 2020, 3, 3369-3389; B. Occhiuzzi, n 24 above, 393.

[27] See European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment adopted by the CEPEJ at its 31st Plenary Meeting (Strasbourg, 3-4 December, 2018), available at https://tinyurl.com/yus24dwf (last visited 30 September 2024).

[28] M. Annany and K. Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability' *New Media and Society*, 20, 3, 973 (2016).

[29] G. Galilei, *Le idee filosofiche, il metodo scientifico* (Brescia: Scholé – Editrice Morcelliana, 2021).

[30] Available at https://tinyurl.com/2vy7v355 (last visited 30 September 2024).

[31] A. Garapon and J. Lassegue, *La giustizia digitale. Determinismo tecnologico e libertà* (Bologna: il Mulino, 2021), 241, underline the risks of the myth of delegating to machines.

systems). This problem is even more acutely felt in the case of artificial intelligence, since systems learn and evolve precisely thanks to the packages of initial data entered by programmers that initiate machine learning, with the result that biases have an impact not only on the initial phase, but also on the entire learning process.

The threats posed to fundamental rights and legal assets by biases are, in fact, increasing in an exponential manner. Examples include *Amazon's algorithm*,[32] which for a time preferred men to women when they were being recruited because the data used for machine learning was based on the recruitment of male staff in previous years, or *Deliveroo's Frank system*[33] that discriminated against riders on the basis of performance. There are also all those cases in which biased data is being used that we are completely unaware of, such as, for example, the case of mortgage lending practices, which are very often conditioned by data such as postcodes.

This issue of data is, therefore, is of primary importance. On the one hand, if there were no big data and open data to feed the new technologies, their very potential would be lost; on the other hand, ensuring the quality of data is essential for preventing a system error from becoming the system itself.[34]

## IV. Corruption and Artificial Intelligence, an Effective Combination?

In light of the problematic aspects reported thus far, the benefits of employing new tools emerge, particularly in the prevention and counteraction of criminal phenomena connected not only to predatory and serial offenses, for which the likelihood of positive are rather high,[35] but also to corruption crimes, for which the use of both neural networks and artificial intelligence systems has been experimented with.

The theme of corruption specifically is of great interest, since the annual cost of corruption worldwide is estimated at USD 1 trillion[36] and in the European Union alone it is worth EUR 5 trillion per year. Moreover, in Italy, the centrality of crimes against public administration in criminal policies is evidenced by the

[32] G. Gaudio, 'Le discriminazioni algoritmiche' *Lavoro Diritti Europa. Rivista nuova di Diritto del lavoro*, I, 1-26 (2024); F. Meta, 'All'intelligenza artificiale di Amazon non piacciono le donne, scartati i cv femminili' *Corriere comunicazioni*, available at https://tinyurl.com/2p8yfjue (last visited 30 September 2024).

[33] L. Fassina, 'L'algoritmo Franck, cieco ma non troppo' *Lavoro Diritti Europa. Rivista nuovadi Diritto del lavoro*, I, 1 (2021). The discriminatory nature of the algorithm used by Deliveroo wasalso established by Tribunale di Bologna 31 December 2020, available at https://tinyurl.com/bdasjv2s (last visited 30 September 2024).

[34] C. Buchard, 'L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società' *Rivista Italiana di Diritto e Procedura Penale*, IV, 1909, (2019).

[35] Empirical results can be found, for example, in the assessments of the functioning of systems like *XLaw* used by the Police Headquarters in Naples. See E. Lombardo, n 18 above, 1-190. See also R. Pelliccia, 'Polizia predittiva: il futuro della prevenzione criminale?' *Cyberlaws*, 9 May 2019; G. Di Gennaro and E. Lombardo, n 18 above.

[36] See International Monetary Fund Report, *Fiscal Monitor. Curbing Corrupting*, 2019, available at https://tinyurl.com/3tpjmynv (last visited 30 September 2024).

continuous reform interventions by the legislature,[37] rendered necessary by the circumstance that corruption accounts for 13% of the GDP.[38]

The purpose of this contribution is, therefore, to analyze the application of new technologies in combating corruption, with a focus on Chinese and Spanish experiences. Indeed, the aim is to explore how these technologies have been used for the prevention and repression of acts of corruption and to highlight their criticalities in terms of respect for fundamental principles, so that their use can be evaluated even in the Italian context, characterized - as mentioned - by a high pervasiveness of this phenomenon.

Using a distinction borrowed from common law countries, the IMF's value of corruption includes both so-called *Grand corruption* and *Petty corruption*. The distinction refers to the two most widespread forms of corruption, namely the payment of a bribe by a private individual to a public official in order to obtain a service due from the public authorities, and the misuse of high offices and institutional practices for the purpose of obtaining benefits for individuals or a small social group.

It is precisely for this reason that the European Union considers the fight against corruption of vital importance for the rule of law. It played, in fact, an important role in the adoption of the Resolution on the fight against corruption adopted by the UN General Assembly in June 2020, which then led to the UN General Assembly Special Session on Challenges and measures to prevent and combat corruption and enhance international cooperation held in June 2021.[39]

Corruption has reached such levels that it is no longer possible, in most cases, to make a distinction between the public and private spheres. Indeed, it not only pollutes institutions by undermining democracy, but has a strong impact on businesses. In this regard, the European Commission has repeatedly emphasized the need to monitor the effect corruption has on the business environment, which is why anti-corruption actions are considered to be one of the most important

[37] The reforms that have affected crimes against public administration are numerous, and it is not possible to provide a comprehensive overview here; the most recent ones are those that have partially revisited the provisions of legge 6 November 2012 no 190, with particular reference to legge 9 Juanary 2019 no 3. Finally, parliamentary proceedings are underway for the approval of the so-called Nordio bill (disegno di legge 19 July 2023 no 808): a new legislative intervention in this area, mainly focused on the repeal of the crime of abuse of office and, therefore, subject to extensive criticism. The bibliography on the subject is vast, covering all aspects: AAVV, *Diritto penale* (Milano: Giuffrè, 2022), I; V. Mongillo et al, *I delitti contro la personalità dello stato e i delitti contro la pubblica amministrazione, artt. 241-360,* III (Milano: Giuffrè, 2022), 377-412; M. Catenacci, *Delitti dei pubblici ufficiali contro la pubblica amministrazione*, *Trattato teorico-pratico di diritto penale Reati contro la pubblica amministrazione* (Torino: Giappichelli, 2022); M.C. Ubiali, *Attività politica e corruzione: sull'opportunità di uno statuto penale differenziato* (Milano: Giuffrè, 2020).

[38] Available at https://tinyurl.com/bdfvk56u (last visited 30 September 2024). The RAND Research Center has estimated that corruption in Italy costs around 237 billion euros.

[39] Available at https://tinyurl.com/u8phath7 (last visited 30 September 2024) and at https://tinyurl.com/4xry52pu (last visited 30 September 2024).

components of Recovery and Resilience Plans.

Up until now, experiential data about the awareness of corruption has revealed how corruption is, more than anything else, perceived. In this regard, the international non-governmental organization *Transparency International* provides every year data from the *Corruption Perception Index*, which since 1995 has been the main statistical indicator of the level of corruption perceived in the public sector and politics in numerous countries around the world. We are, however, talking about a perception,[40] whereas real data is, on account of offshore jurisdictions, not known. Many governments are, in fact, reluctant to monitor corruption, for which there is no data.

This scenario is rapidly changing thanks to new technologies: the digitization of procurement procedures and the creation of online portals, has - by making a large amount of data on public tenders, contracts and suppliers public - provided a more detailed view of corruption and its causal relationships.[41] Big data and open data give automated monitoring tools unprecedented power, so much so that this has prompted the European Commission to adopt a number of operational tools, such as the *open contracting data standard*[42] (which is a guide that has been developed with a view to alerting governments about data to be published that detects cases of corruption), and the *open tender* platform,[43] which uses algorithms to scan data provided by programmers and which is cross-referenced with data from other sites for the purpose of obtaining information about open tenders, as well as the history and positions of the companies taking part in such tenders and any possible connections they may have with politicians. The interpretation of this data generates corruption risk indicators, which can, with a view to an in-depth investigations being conducted that could lead to further information being requested, be used to suspend a suspicious tender.[44]

[40] F.M. Romano et al, 'La misurazione della corruzione attraverso le sentenze: una proposta metodologica con strumenti di text mining' *Federalismi.it*, 2 December 2020, 169-170, who underline the ontological imprecision of indicators built on perceptions. This may give rise to the paradox that 'a greater level of enforcement of (repressive or preventive) anti-corruption policies leads to an increase in the degree of collective and individual perception of this criminal phenomenon, given that it becomes much more visible (or to be more precise, there is a much greater 'level of noise of the marketplace' ('strepitus fori')'. This is the so-called *Trocadero paradox*, which G. Tartaglia Polcini, has written about in 'Il paradosso di Trocadero' *Diritto penale della globalizzazione*, 1 (2017).

[41] L. Nannipieri, 'Il nuovo casellario informatico dei contratti pubblici di lavori, servizi e forniture', in M. Trapani ed, *La prevenzione della corruzione. Quadro normativo e strumenti di un sistema in evoluzione. Atti del convegno, Pisa 5 October 2018* (Torino: Giappichelli, 2019), 187; E. Belisario, 'Open Government e Open Data: la trasparenza e le nuove tecnologie come strategia per la lotta alla corruzione', in M. Trapani ed, ibid 197.

[42] See A. Pheteram at al, 'The next generation of anticorruption tools: big data, open data and AI' *Oxford Insight Research Report*, available at https://tinyurl.com/4u25cf3t (last visited 30 September 2024).

[43] A. Pheteram et al, n 42 above.

[44] With regard to the role played by big data in measuring corruption, see M. Gnaldi et al, *Misurare la corruzione oggi. Obiettivi, metodi, esperienze* (Milano: Franco Angeli, 2018), 90.

Therefore, data mining can be considered the main anti-corruption weapon on account of the fact that it has proactive risk-analysis features, is repeatable and can, as a result thereof, be justified even when it is subjected to post-facto scrutiny. Having a large amount of data at one's disposal is, however, not enough. One must, in fact, have a good knowledge of analysis methods and decision-making models, as well as a thorough understanding of the business to which the data refers. Indeed, it is not an easy task to extract the right indicators from such data. The analysis of data that measures, for instance, the extent to which corruption and organized crime are intertwined, often only reveals, in fact, mere risk correlations.[45]

So far, data has been used for the purpose of analyzing the extent of corruption and interpreted for the purpose of understanding it. The next step forward is that of programmers using this data as a basis for commencing and feeding artificial intelligence machine learning processes, as well as for using artificial neural networks, which, in imitating the human brain in its ability to establish connections, are capable of detecting relationships, links and anomalies.

*Oxford Insights*, which is a London-based governmental organization, supports research on new technologies precisely on account of the fact that they are seen as the next anti-corruption frontier. Its partners believe that the availability of data is not a problem, since there is an abundance of huge data sets coming from both government sources (such as tax systems, in those situations in which such systems are transparent) and from open public procurement systems and public registers and other sources. Apart from digitized money transactions and services, there are 300 million legal entities in the world whose data could be cross-referenced, harmonized and shared for the purpose of uncovering cases of fraud, corruption and scams.

If anything, the real problems at the moment are twofold: the inability to harmonies data and the fact that data is not standardized and shared, on the one hand, and the fact that the applicable legislation is fragmented and complex, which affects the quality of data and information and risks jeopardizing the AI self-learning process, on the other hand.

This is what needs to be addressed in the near future before this type of technology can be used in anti-corruption policies.

There is, moreover, a further aspect that has to be assessed, namely the ability of new technologies to stimulate legislation. Artificial intelligence can, by analyzing different data sets, bring to light aspects of corruption that have so far escaped lawmakers, thus directing the criminal policy choices that are to be made by them. This is, however, not all. By being able to link all the relevant legislation together, AI can correct it and make it more effective by also identifying any gaps in such legislation.

The case history of artificial intelligence systems and neural networks used in the fight against corruption is so far not very extensive and mostly concerns money laundering and tax evasion. However, some uses or experiments that

[45] See, on this point, M.F. Romano et al, n 40 above, 168.

have so far been carried out by several countries can already be studied.

They have so far dealt with three different scenarios: Artificial intelligence systems can be used as a public policy tool in cases of corrupt behavior engaged in by public officials or private individuals to the detriment of government authorities, where such acts have already been committed. Neural network systems can then be used as predictive tools that are capable of identifying a specific geographical area that finds itself at a greater risk of corruption. Lastly, they can be used, with a view to preventing risks of corruption, by private individuals in corporate compliance procedures, especially with a view to verifying whether corporate models comply with the applicable laws and regulations.

The latter scenario has, so far not occurred in connection with legal persons and we must, therefore, await future developments that can give us a better understanding of the effectiveness thereof and the critical issues arising therefrom.

Some artificial intelligence tools that discover and ascertain corruption harming public authorities have, on the other hand, been successfully experimented in various parts of the world, even though critical issues have, in some cases, arisen that cannot be overcome as things stand.[46]

This was the case in Ukraine, which is a country that was considered to have the highest level of corruption in Europe until the 2015 scandals involving many members of the government occurred. On that occasion, two different types of tools were introduced: the *Prozorro* platform[47] and the *Dozorro* software.[48] The first tool was designed by a group of activists and international NGOs and all public tenders totaling 1.67 million and worth 50 billion were published there. The second tool is, on the other hand, software that was able, in its first version, to reveal ongoing corruption by analyzing 35 risk indicators, with the limitation that the publication of such indicators allowed criminal organizations to adjust their corrupt conduct accordingly, nullifying the system as a result thereof. A new version was then

[46] See P. Aarvik, 'AI – a promising anticorruption tool in development settings?', available at https://tinyurl.com/28hj4u8e (last visited 30 September 2024). The author provides a broad overview of current experiments around the world that have an anti-corruption objective. In Mexico, for instance, the Open up Guides project monitors public procurement procedures through artificial intelligence, whereas the Project Insight system identifies, in India, high-value transactions, firstly comparing them with spending patterns and then comparing them with citizens' statements. These are only a few examples, but the problematic issue for all of them is the ability to react once the risk of corruption has been identified.

[47] The open-source model is the result of collaboration between the Ukrainian government, the business sector, and civil society, enabling collaboration between the central database and an infinite number of commercial markets through a graphical interface accessible directly to users. Upon completion of a tender procedure, through Prozorro's online analysis module, all data can be accessed, including the list of all participants, their offers, the decisions of the tender committee, and all qualification documents. Available at https://tinyurl.com/yc3dnxup (last visited 30 September 2024); https://tinyurl.com/2wtnup4h (last visited 30 September 2024); https://tinyurl.com/3jw2aue6 (last visited 30 September 2024).

[48] See also A. Pheteram et al, n 42 above, 11. For a better understanding of the *Dozorro system*, please refer to https://tinyurl.com/yw5dd7s7 (last visited 30 September 2024).

adopted, which was not tied to pre-established indicators or formulas and which had a 90% accuracy rate in detecting corruption, leading to a significant increase in the efficiency of corruption-related investigations. As a result of these technologies being introduced, the country has seen a great decrease in corruption, thus climbing several positions in Transparency International's rankings.

### 1. The Chinese Zero Trust System

The system par excellence in the fight against corruption is undoubtedly the one developed in China that goes by the name of *Zero Trust*,[49] whose very high rate of efficiency is directly proportional to the critical issues it raises. Put into place in 2012 and tested in only 30 counties and cities covering 1% of the country's total administrative area, it has uncovered 8,721 cases of public employees involved in corruption, embezzlement, abuse of power, and misappropriation of public funds.[50]

This sophisticated artificial intelligence system makes use of one hundred and fifty government databases for the purpose of monitoring the actions of public officials, flagging cases where a pre-determined threshold of probability of corruption is reached. The data that is being used is very heterogeneous, ranging from banking data to land registry data, from movable goods to information collected with satellite images.[51] It is able to detect any discrepancy between a person's lifestyle and his or her earnings that raises a suspicion of probable corruption. The results are analyzed by officials wielding disciplinary power who make the final decision as to whether to investigate or not the public official in question.

It sounds like the perfect anti-corruption tool, but clearly it is not, so much so that it has been suspended. Even if it succeeds in preventing government corruption and has a 72% probability of success, no-one (neither the programmers nor the investigators) is, in fact, able to trace the manner in which the evidence is gathered, making it inadmissible at trial. This is not just a *black box* problem (like the one

[49] Z. Sun et al, 'How Does Anti-Corruption Information Affect Public Perceptions of Corruption in China?' 22 *China Review*, 113-143 (2022); E. Consiglio and G. Sartor, 'Il sistema di credito sociale cinese: una «nuova» regolazione sociotecnica mediante sorveglianza, valutazione e sanzione' *Rivista di Scienze della Comunicazione e di Argomentazione Giuridica*, 2, 139 (2021); V. Brigante, 'Corruzione e Appalti Pubblici in Estremo Oriente: moduli di contrasto nella Repubblica Popolare Cinese e in Giappone' *Diritto Pubblico comparato ed europeo* online, 1, 225 (2019); M.C. Leone, 'Detection & Prevention Anticorruzione e Artificial Intelligence (A.I.)' *safetysecurity magazine,* 28 February 2019, available at https://tinyurl.com/pcj9wewd (last visited 30 September 2024); S. Chen, 'Is China's corruption-busting AI system 'Zero Trust' being turned off for being too efficient?' (04.02.2019), available at https://tinyurl.com/4n3k567e (last visited 30 September 2024); B. Zhu; Mncs, 'Rents, and corruption: Evidence from China' 61 *American Journal of Political Science*, 84 (2017); Y. Samson, 'Disciplining the Party: XI Jinping's anti-corruption campaign and its limits' *China perspectives*, 3, 41-47 (2014); K. Kilkon and W. Cuifen, 'Structural Changes in Chinese Corruption' 211 *The China Quaterly*, 718 (2012).

[50] C. Burchard, n 34 above.

[51] The use of satellite imagery serves not only the purpose of verifying the area of residence of the person in question, but also ensures that public money has actually been used to build a planned public work.

that arises in general for all artificial intelligence systems), but is an additional problem that concerns the enormous amount of data that is being used and the complexity of the relationships and connections analyzed by such system. This would force investigators to do additional investigative work for the purpose of proving what has been established by the machine and there is no certainty that a result can be achieved (with a significant expenditure of resources).

This is not all. Public officials have suffered greatly from the psychological pressure of feeling constantly monitored even in their life choices, despite the government's assurances that the purpose of the project is not to punish officials, but rather to intervene before corrupt conduct is engaged in. In most of the cases reported by artificial intelligence, the suspected civil servant kept his or her job and received a warning or, in the most serious cases, was subjected to disciplinary action. Resistance was, however, such that many officials refused to provide the necessary data.

One of the most significant reasons for ending the experiment and decommissioning the system was the violation of the principle of legality, since there are no *ad hoc* provisions in Chinese law that authorize such a technology to gain access to a sensitive database.

The quality of the data used in the training of artificial intelligence also posed many problems.

Those same officials monitoring suspect cases are called upon to support the programmers in the machine learning start-up phase, providing their experience from previous cases and participating in the training of datasets by manually reporting any events that turn out to be unusual. The risk of the data being heavily biased is, therefore, very high.

### 2. The Spanish Experience: So-called *Self-Organising Maps*

What still needs to be analyzed is the situation in which new technologies are used in a predictive manner in order to make a forecast about possible corruption. One example is to be found in so-called *self-organising maps*, which have been developed by researchers at the University of Valladolid in Spain and are valid for certain geographical areas that are more exposed to the risk of corruption.[52]

These are tools that exploit neural network and competitive training technology,[53] according to a mathematical model developed in the field of computational neuroscience that is based on the structure of the human brain, which is organized through links between neurons.

Therefore, a linear combination of input data is organized in nodes or units connected to each other through links that take part in a process known as 'winner

[52] See A. Petheram et al, n 42 above.

[53] The acronym is SOM (*Self-organising Maps*). For a technical analysis thereof, see M.G. Di Bono, 'Comparative analysis of self-organising neural networks', available at https://tinyurl.com/nhv8k9rh (last visited 30 September 2024).

takes all',

> 'at the end of which the node having a vector of weights closest to a certain input is declared the winner, whereas the weights themselves are updated so as to bring them closer to the input vector. Each node has a number of adjacent nodes. When a node wins a competition, the weights of the adjacent nodes are also changed, according to the general rule that the further away a node is from the winning node, the less marked the change in its weights must be. The process is then repeated for each vector in the training set for a certain, usually large, number of cycles. It goes without saying that different inputs produce different winners. Operating in this way, the map eventually manages to associate output nodes with recurring groups or patterns in the input data set. If these patterns are recognizable, they can be associated with the corresponding nodes in the trained network'.[54]

The maps manage to extract in-depth patterns from an enormous amount of data and even do so when no logical connection can be identified. By converting non-linear relationships into more easily identifiable geometric connections, they manage to estimate the probability that corruption will occur. The system facilitates the detection of critical issues and targets monitoring and control actions, taking into account the characteristics of individual regions, whereas potential offenders play an entirely marginal role.

More specifically, with regard to the Spanish provinces in which system was tested, economic and political variables inducing public corruption were identified. The latter included property taxes and rising real estate prices, the same political party remaining in power for long periods of time and economic growth occurring too fast or a growing number of financial institutions. The data was contained in an archive that collected macroeconomic and political data from cases that occurred in Spain between 2000 and 2012, which, when analyzed by the neural network, made it possible to predict public procurement corruption risks even 3 years in advance of them eventually being committed.

The model can also be applied to other countries or regions and can be tailored to the specific characteristics of each of them, with the result that governments could use such systems to identify vulnerabilities and target actions and checks in particular risk areas.

## V. Blockchain as a Tool

Another tool, which is generally associated with virtual currencies, can make

[54] https://tinyurl.com/3vjdp9wc (last visited 30 September 2024). See, also on this topic, S. Russell and P. Norvig, *Artificial intelligence. A modern approach* (Edinburgh: Global edition, 2016), 727.

a significant contribution and ensure that administrative activities are transparent and artificial intelligence is used in anti-corruption policies. This is blockchain, which is a highly innovative technology that guarantees transparency and traceability precisely on account of its ability to track data and trace the manner in which it has been acquired.

Until proven otherwise, the system can neither be modified nor corrupted in any way whatsoever, and it was first used in virtual currencies such as *Bitcoin*. Its use has been extended to many other uses, including(to name but a few) the protection of banks from invoice fraud or any other form of fraud, and the certification of any form of register that secures supply chains, including food supply chains.

Such a tool could contribute to overcoming the problem of the lack of transparency in government activities, which strongly affects the effectiveness of anti-corruption instruments. The *black box* dilemma has, with the due proportions, always afflicted administrative activities in Italy, insofar as the Italian government's relationship with its citizens has long been biased towards the state administration and is characterized by the opaque nature of the procedures involved. Even though the principle of impartiality and efficiency is enshrined in Art 97 of the Italian Constitution, it has only in more recent times been affirmed in practice: nevertheless, the opaqueness thereof continues to be an unresolved problem and contributes in a significant manner to pervasive corruption. To this effect, blockchain can play a dual role, both in public and private business compliance. The system contributes, in fact, to ensuring that Italian government data is increasingly transparent and verifiable, thus allowing Italian citizens to fully take part in the decision-making processes of public institutions. At the same time, it can be used in the internal processes of corporate organizations, certifying all of the actions that have been undertaken and establishing organizational models that can lead to best practices being applied.

The experience in some developing countries, whose democratic life has been strongly affected by corruption, electoral fraud, misappropriation of public funds and illicit party financing, is that blockchain has led to a breakthrough. Indeed, it has allowed a single register to be set up, in which all public transactions are tracked and stored, are shared by all of the public authorities and, above all, can be seen by everyone, guaranteeing further forms of control over the flow of public money.[55]

Blockchain could then be managed by an independent authority, which would guarantee the system's independence.

## VI. The Difficult Balancing Act between Protection and Progress

In Italy, Raffaele Cantone, who is the former president of the National Anti-

[55] See A.I. Sanka and R.C.C. Cheung, *Blockchain: Panacea for Corrupt Practices in Developing Countries, 2019 2nd International Conference of the IEEE Nigeria Computer Chapter* (Nigeria: Institute of Electrical and Electronics Engineers, 2019).

Corruption Authority (ANAC), has stated that the preparation of corruption maps in Italy should even be a priority for anti-corruption policies.[56] One could, therefore, resort to the neural networks used to build *self-organizing maps*, which act as real advanced topographic maps and offer, therefore, a broader perspective and are capable of detecting connections that are not always obvious.

Even though the debate on new technologies has reached a fairly advanced level,[57] there is still a lot of resistance in Italy to even testing them out as an anti-corruption tool.

The so-called *legge Severino* acknowledged the importance of data collection, on which the Three-Year Plan for Information Technology in Government Activities and Transparency envisaged under decreto legislativo 25 May 2019 no 97[58] heavily focused. There was, however, no trace of any reference to the use of new systems in the Anti-Corruption Authority's Three-Year Plan for the Prevention of Corruption and Transparency presented in May 2021.

Undoubtedly, the Italian authorities' caution is justified by the new technologies' ontological limits that have been mentioned above, namely a lack of transparency and explainability, as well as systems' interpretation of data and biases, which put certain fundamental rights at risk. One can agree with this position, which wants to protect civil liberties when fundamental rights are at stake. On closer inspection, however, some of these obstacles can be overcome, leading to an acceptance at least of forms of experimentation and assessments of the costs/benefits thereof.

It should be remembered, for instance, that the problem of bias not only arises with machines, but also affects the courts' decisions and lawmakers' regulatory powers.[59] The logical arguments underlying judgements handed down by an Italian court are, in fact, the result of a self-learning process that is nurtured throughout a judge's professional life thanks to the latter's knowledge and experiential data. The fact that these, in turn, are inevitably conditioned by the biases that affect

[56] See G. De Blasio et al, 'Predicting Corruption Crimes with Machine Learning. A Study for the Italian Municipalities' *DiSSE Working Papers online*, 16, 7 October 2020.

[57] Several documents have been produced, including the Proposals for an Italian Strategy for Artificial Intelligence drawn up by the Italian Economic Development Ministry's Expert Group on Artificial Intelligence, which are to be found at https://tinyurl.com/2bn3h3z3 (last visited 30 September 2024). The White Paper for AI is available at https://tinyurl.com/3beknwww (last visited 30 September 2024).

[58] This is the Legislative Decree that revised and simplified the provisions on the prevention of corruption, publicity and transparency and corrected legge 6 November 2012 no 190 and decreto legislativo 14 March 2013 no33, pursuant to Art 7 of legge 7 August 2015 no 124 about the reorganization of public offices.

[59] An observation has been made on this matter in M. Versiglioni, *Diritto matematico* (Milano: Pacini Giuridica, 2020), 233, to the effect that the set of rules that make up the legal system and all of the procedures that follow therefrom are the result of an algorithmic process, in which humans provide the initial input (ie the primordial nucleus of rules). The legal system builds all the rest on this, without the possibility of expunging the biases that are inherent in any human mind. See also L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale* (Roma: Edizioni Studium, 2020), 60.

every human mind is known by everyone and often ends up on the front pages of the newspapers when verdicts are issued that are, on account of juries' biases, of an evidently discriminatory nature.

In modern societies, the antidote has been identified in the principle of democracy and pluralism of ideas, with the result that there is more than one level of jurisdiction and collegial bodies are preferred. Similarly, the same solution can be adopted for machines' self-learning processes, envisaging that programming is carried out by an heterogeneous group of people, rather than a single programmer, or even imagining that one system is to be used to control another. There remains, in both cases, a margin of error that cannot otherwise be eliminated and whose risk must be accepted for the benefit of human evolution.

On the other hand, the impossibility of retracing the machine's decision-making path appears to be difficult to solve and poses significant challenges in putting together evidence. This entails investigators expending a considerable amount of additional effort, which may not necessarily lead to results, but above all may lead to a selective investigative focus, which concentrates efforts on certain offenders, leaving out others. It also entails the risk of losing sight of the centrality of the facts, or looking on as the threshold of punish ability is brought forward too much.

What has been said above, however, should not lead to an attitude of distrust and refusal of the various uses to which technology can be put. It should rather lead to a position that is open to experimentation, testing the tools and verifying the costs/ benefits thereof. This could provide an important opportunity to fight corruption, which has such an impact on our legal system's resilience.

What transpires, therefore, is the close connection between new technologies and criminal law: the former can be of help, and give impetus, to the latter.[60] For its part, Italian criminal law is called upon to prevent artificial intelligence from becoming an instrument of power that poses a threat, even though it is a tool that is a last resort, fragmentary and of a subsidiary nature. What is still lacking, however, is a shared view as to whether traditional categories should adapt to the new reality or rather overcome them, favoring innovative scenarios in the Italian legal system.

Whatever choice is made, there is the need to regulate this situation either by enunciating principles that take into account the insurmountable limit of respecting fundamental rights and the importance of maintaining man's centrality or by resorting to a binding set of rules that, in light of the pervasive nature of these instruments, contributes to legal certainty. Empirical science must find a place in anti-corruption policies, constituting the 'precondition for an integrated criminal science'.[61]

[60] With all that this entails in terms of the risk of judgments becoming detached from reality and penal determinism holding sway, as shrewd legal scholars have pointed out. See V. Manes, n 17 above, 13. On this point, see also C. Buchard, n 34 above, 1909.

[61] M.F. Romanoet al, n 40 above, 167.

## VII. Summing Up

In today's world, there seem to be two different ways of approaching the relationship with new technologies. There is, on the one hand, the legal system that is of an understandably cautious nature and, as a result thereof, takes a long time to take decisions and there is, on the other hand, the great expectations of laymen who propose solutions, projects and experiments that increasingly change the real world. There are, to name but a few, the artificial intelligence tool called *Watson*, which has changed the face of government and business activities in South Africa and the Horizon 2020-funded *Digiwhist* project, which uses advanced algorithms to collect huge amounts of data aimed at improving the efficiency of public spending across Europe and increasing transparency and combating corruption, as well as the system commissioned by the World Bank from Microsoft that detects anomalies in public procurement procedures by combining heterogeneous data.

Indeed, it is not easy to sum up this debate. Sometimes it seems as if the issues raised with regard to the implementation, risks and governance of new technologies are to be treated only as augmented reality, for which it would be sufficient to apply the same categories and strengthen the existing tools.[62]

After all, we have always processed data and information has always been falsified and manipulated. This is, therefore, a quantitative issue. Perhaps the Data Protection Regulation, on the one hand, and certain (existing or newly introduced) criminal offences, on the other hand, can also protect the right of *habeas data* - which is now being compared with the right of *habeas corpus* – from such risks.

Just as we have introduced the concept of legal persons' liability, we can also introduce the concept of electronic persons' liability (perhaps not taking the same amount of time...).[63] Just as we accept sharing many aspects of our personal lives on social network sites, we can accept – albeit with a great deal of caution – facial recognition systems that control urban environments.[64]

Even the problem of the *black box* is, in part, surmountable if we also consider the human mind to be such. When faced with the problem of ascertaining whether conduct is willful, reference is made to the so-called *probatio diabolica* (diabolical proof). This is also the case for biases: numerous studies have shown that job interviews are – as much as, and perhaps more than, machines –

[62] See XXI International Congress of Penal Law 2024, *'Artificial Intelligence and Criminal Justice*' available at https://www.penal.org/en/information (last visited 30 September 2024).

[63] Cf A. Celotto, 'I robot possono avere diritti?' *BioLaw Journal*, 28 February 2019, 1, 91-99.

[64] This issue is wide-ranging and the debate is intense. We are increasingly bearing witness to the fact that the concept of security is being used in a specious manner. In a situation in which there is a heightened risk of terrorist attacks, economic crises and pandemics, this concept is being increasingly used to stimulate the community's sense of fear and an ensuing demand for protection. This leads to an ever-increasing and unconscious compression of certain fundamental rights through new technologies, which leads to the introduction – for example – of facial recognition systems (of even an emotional nature) that are still hotly debated. See S. Zuboff, *Il capitalismo della sorveglianza* (Rome: Luiss, 2019).

influenced by the biases of human recruiters.

Elsewhere, however, the belief prevails that the risks are not so low-impact and the repercussions that the massive use of new technologies can have on the protection of human rights may be such as to undermine the very resilience of the system.

It has been seen, for instance, how the manipulation and alteration of data and information can even influence political consensus, and how the capacity and speed of the dissemination thereof in respect of the enormous quantity of individuals who may get involved is in itself reason enough for considering the phenomenon to be different from those of the past: echo chambers are not really comparable to the trade unions of the past.

This is why it is important to recover the State's prerogative to issue rules on the governance of data. It is in fact, undesirable for private individuals to maintain any sort of regulatory power, let alone a monopoly. If it is true, in fact, that data, despite the volumes involved, does not necessarily imply having knowledge, it is also true that the indiscriminate use thereof without quality guarantees may give rise to the algorithmic risk that we all fear.

There are countless problems in the field of criminal law. These include delegating such a fundamental concept as social dangerousness to an assessment made by a robot, which in turn gives rise to the risk of moving from criminal law based on fact to criminal law based on the perpetrator (whose dangerousness is, however, assessed not on the basis of his personality, but on degrees of probability provided by statistics). Resorting to predictive tools once again affects the quality of the assessment made by criminal law on the basis of fact, which is brought forward to a moment in which the crime has not yet been committed, with ensuing risks of a self- fulfilling criminalization.

Nor should we underestimate the danger of discharging those in charge of their duties, which could be particularly evident in the field of justice. Should artificial intelligence, in fact, indicate - when the decision is being made as to whether to issue alternative measures – a high degree of risk (for example with regard to an assessment of social dangerousness), a judge is unlikely to reach a different decision. This is the so-called goat effect mentioned by legal scholars[65] that could lead to the judiciary deciding without judging the facts of the case (in the same way as has been the case for some time now in defensive medicine) or even lead to exact but not necessarily fair justice.[66] Likewise, someone might invoke, in the not-too-distant future, the performance of a duty under Art 51 of the Italian Criminal Code following the execution of an algorithmic decision and thus consider himself or herself not to be punishable.

[65] A. Garapon and J. Lassegue, n 31 above, 155.

[66] G. Canzio, 'IA, algoritmi e giustizia penale' *Sistema Penale*, 8 gennaio 2021, 1-7. See P. Moro and C. Sarra, n 1 above, 89. As an instrument of crime, IA could also be subject to confiscation or seizure, as envisaged in the 2005 Council of Europe Convention on Corruption.

Equally risky is the case where algorithms, instead of being used to fight crime, themselves become tools for the perpetration of crimes such as corruption, perhaps managing to conceal the very data and indicators that are subjected to the investigators' computational analysis.[67]

The robotic revolution that we are witnessing should lead – in my opinion – to favoring a neutral approach to the topic, so as to benefit from the enormous potential that these tools are in any case showing that they have. This implies the possibility of a change of point of view even with regard to issues that have so far been considered unchangeable. There might, for example, be a silver lining in accepting – with all the necessary precautions and guarantees – a legitimate form of predictive justice, provided that this could avoid right from the outset any legal asset being harmed[68] and at the same time reduce the need to resort to criminal law, which would once again fulfill its original purpose of being an instrument of last resort. Technology that supports the fight against corruption can only be welcomed. Suffice it to say that, in some countries (in which judicial corruption is particularly rife), recourse has been made to artificial intelligence with a view to verifying, examining and controlling the evidence used during trial, bringing to light any contradictions in the case made by the prosecution.[69] According to some legal scholars, artificial intelligence contributes to the realization of so-called *open* justice, which makes justice measurable and transparent, reducing the arbitrariness of judges.[70] It almost seems as if Beccaria's dream is being achieved, but there are many doubts about whether new systems are capable of doing so, precisely because in light of the foregoing.

Humanity is probably still in time to regulate 'onlife'[71] and avoid the multiplication of risks that would lead to the imposition of unsatisfactory emergency legislation. The increasingly widespread suspicion that artificial intelligence is not so intelligent and that – at the moment – its dependence on human activity is far from negligible may also come to our aid. This also gives rise to another important assessment concerning the significant impact that such systems have in terms of

[67] See P. Moro and C. Sarra, n 1 above, 89. As a tool of crime, AI could also be subject to confiscation or seizure, as provided for in the Council of Europe's Convention on Corruption from 2005.

[68] C. Buchard, n 34 above, 1909, according to whom criminal law can only guarantee the protection of legal goods in a legislative and counterfactual manner, whereas artificial intelligence used in criminal law makes the injury impossible or minimizes it.

[69] On this point C. Yadong, *AI and Judicial Modernization* (Singapore: Springer, 2020), 1-224. The author fully illustrates the functioning of the system in use in the courts of the city of Shanghai.

[70] ibid 38-40. Open justice is a fundamental principle of common law systems and there is already a trace thereof in the Magna Charta. In Australia, hearings can be viewed online and, when secrecy has to be invoked - for example, for acts of terrorism - this constitutes a reason for criticizing the system in terms of the violation of a fundamental principle that should know no exceptions. See, among many, H. Burkhard and A. Koprivica Harvey, *Open Justice. The Role of Courts in a Democratic Society* (Busto Arsizio: Nomos, 2019).

[71] L. Floridi, *The Onlife Manifesto: Being Human in a Hyperconnected Era* (Oxford: Springer, 2015), 1-264.

sustainability and erosion of resources.[72] The use of these tools requires, in fact, large amounts of energy and also poses quite a few problems in terms of disposal. The issue is becoming increasingly pressing at a time when the climate crisis is showing the enormous risks that we are running and the fragility of the environment in which we live.

What will make the difference – in my opinion – will, therefore, be that of continuing to have an anthropocentric focus, respecting fundamental rights and applying principles such as the precautionary principle and the principles of strict necessity and proportionality.

These are three very important aspects that are closely intertwined.

Refuting procedures that are entirely automated and not subjected to any human control necessarily entails involving not only scientists, but also (and above all) those studying the humanities, who are, even more than computer scientists or mathematicians, called upon to play a fundamental role in the very process of data selection. Computational power and predictive capacity depend on the virtuous or unvirtuous management of data, with the ensuing need to guarantee the transparency of the data itself and, at the same time, the synergy between legal and algorithmic tools.

The introduction of a mandatory impact assessment prior to the implementation of new artificial intelligence systems can, irrespective of their scope of application, be a valuable tool for the protection of fundamental rights in both the public and private sectors. The use of monitoring tools and supervisory bodies can, therefore, help ensure a good level of protection, but also a greater sharing and awareness of the importance of such issue in the community.[73]

[72] K. Crawford, *Né intelligente né artificiale* (Bologna: il Mulino, 2021), 35.

[73] On this point, European Agency for Fundamental Rights, 'Preparare un giusto futuro l'intelligenza artificiale e i diritti fondamentali', available at https://tinyurl.com/y7sattje (last visited 30 September 2024).