Legal Studies in International,
European and Comparative Criminal Law 7

Lorena Bachmaier Winter
Stefano Ruggeri *Editors*

Investigating and Preventing Crime in the Digital Era

New Safeguards, New Rights

Springer

Legal Studies in International, European and Comparative Criminal Law

Volume 7

The main purpose of this book series is to provide sound analyses of major developments in national, EU and international law and case law, as well as insights into court practice and legislative proposals in the areas concerned. The analyses address a broad readership, such as lawyers and practitioners, while also providing guidance for courts. In terms of scope, the series encompasses four main areas, the first of which concerns international criminal law and especially international case law in relevant criminal law subjects. The second addresses international human rights law with a particular focus on the impact of international jurisprudences on national criminal law and criminal justice systems, as well as their interrelations. In turn the third area focuses on European criminal law and case law. Here, particular weight will be attached to studies on European criminal law conducted from a comparative perspective. The fourth and final area presents surveys of comparative criminal law inside and outside Europe. By combining these various aspects, the series especially highlights research aimed at proposing new legal solutions, while focusing on the new challenges of a European area based on high standards of human rights protection.

As a rule, book proposals are subject to peer review, which is carried out by two members of the editorial board in anonymous form.

Lorena Bachmaier Winter • Stefano Ruggeri
Editors

Investigating and Preventing Crime in the Digital Era

New Safeguards, New Rights

Springer

Editors
Lorena Bachmaier Winter
Law School
Complutense University Madrid
Madrid, Spain

Stefano Ruggeri
Law Department
Messina University
Messina, Italy

ISSN 2524-8049 ISSN 2524-8057 (electronic)
Legal Studies in International, European and Comparative Criminal Law
ISBN 978-3-031-13951-2 ISBN 978-3-031-13952-9 (eBook)
https://doi.org/10.1007/978-3-031-13952-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Part III
Fact-Finding and Human Rights Challenges in the Digital Era

AI-Powered Investigations: From Data Analysis to an Automated Approach Toward Investigative Uncertainty

Giulia Lasagni

Abstract Criminal law might sometimes be perceived to be at the margins of the automation process that involves increasing sectors of our society. While the expansion of automated-driven cars is by now an established fact, the technological upgrade of criminal justice mechanisms still tends to evocate sci-fi images and Minority-report-style dystopian scenarios to the non-specialists.

However, the high variety of applications that can already be counted in this domain, and the acceleration of this process in the last few years, clearly speaks for a tangible expansion of AI technology also in the field. In particular, against some more-established scenarios, especially related to phenomena of so-called predictive policing, Multi-Agent Systems (MAS) open today the perspective of a much deeper involvement of automated technologies in the very shaping of investigative proceedings.

The chapter offers an analysis of such potential, both with respect to their possible contribution to the efficiency of investigations (in their preventive and repressive dimension), and to avoid or reduce certain negative biases typical of "purely human" investigation processes, first of all, the tunnel vision effect.

1 Challenging Traditional Models of Decision-Making in Criminal Justice

It is difficult to measure the width of a change while you are right in the midst of it, and the advent of AI surely is one that might take more than a lifetime to get used to.

G. Lasagni (✉)
Department of Legal Studies, University of Bologna, Bologna, Italy
e-mail: giulia.lasagni6@unibo.it

L. Bachmaier Winter, S. Ruggeri (eds.), *Investigating and Preventing Crime in the Digital Era*, Legal Studies in International, European and Comparative Criminal Law 7, https://doi.org/10.1007/978-3-031-13952-9_8

Thanks to an ability to record and process information that yet finds no terms of comparison, and a capillarity similar to that of law itself,[1] AI and algorithms are today transforming most human activities, and in particular decision-making processes. Renown is the statement by Balkin, according to whom we are rapidly moving towards

> the Algorithmic Society [...] organized around social and economic decision-making by algorithms, robots, and AI agents, who not only make the decisions but also, in some cases, carry them out.[2]

Along the same line, other authors talk about a 'transition from history to hyperhistory', a change implying that

> "our current life world can no longer be described by dichotomizing online and offline, which suggests that we require a new term to more adequately depict our current predicament" and partake "in a new kind of world that we are still discovering".[3]

It is worth mentioning that one of the latest paradigm-shifts in AI development led to the adoption of data analysis-induced knowledge methods, which largely set aside traditional approaches based on symbolic representations of human specialist expertise. The fact that most successful AI systems are currently based on Machine Learning (ML) techniques, applied to large masses of (big) data, has indeed become common knowledge.[4]

Equally well known, especially among criminal law scholars, is one of the main technical limitations of ML systems: As much as they are capable of high performances in terms of result accuracy, their functioning, as well as the reasons underlying their outcome, are still not fully explainable. Such technologies are thus also known as 'black boxes', *i.e.*, systems in which input and output are observable, while their internal functioning remains obscure even to their own programmers.[5]

---

[1] As highlighted by Ubertis (2020), pp. 76–77.

[2] Balkin (2017), p. 1219.

[3] Cf. Floridi (2014), pp. 1–24; Hildebrandt (2015), p. 42. See also European Commission, *Explanatory Memorandum to the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act)* {SEC(2021) 167 final}—{SWD(2021) 84 final}—{SWD(2021) 85 final}, Bruxelles, 21.4.2021, COM(2021) 206 final, pp. 1 ff, highlighting the need to make AI "a tool for people" and "a force for good in society". For some aspects of this proposal see also in this volume Neroni Rezende, Sect. 2.

[4] One of the most remarkable features of such technology, especially from a legal perspective, precisely concerns the decision-making approach: Instead of carrying out its assessments following a set of rules (algorithm) predefined by the programmer, ML systems build their own model of the domain, applying a learning algorithm to analysis of the training data, cf., for all, O'Neil (2016); Russell and Norvig (2010), pp. 525 ff; Ferguson (2018), pp. 504 ff; Henderson (2018), pp. 527 ff.; Lagioia and Sartor (2020), pp. 280 ff; Goodfellow et al. (2018), p. 56 ff.

[5] For all, cf. Pasquale (2015).

As largely observed, the resemblance with an 'oracle'—though gifted with great statistical accuracy—makes it especially critical to deploy such systems in the criminal justice domain.[6]

Indeed, the duty to state reasons, especially in case of decisions affecting core values, like personal freedom, lays at the roots of democratic models of modern justice delivery.[7] It is thus apparent, that without a satisfactory explanation on how and why the decision-maker has assessed the elements at its disposal in a certain way, challenging a decision with reasonable chances of success becomes virtually impossible.[8]

The conclusion, however, does not suggest an ontological incompatibility between AI systems and criminal justice.[9] Actually, the potential of such systems in the field, for instance to improve consistency and predictability of legal interpretation,[10] is rather widely accepted.

Deployment of AI and algorithmic technology is then especially common in the preventive and investigative phases, with various levels of success around the world. This seems to largely depend on the fact that defence rights are considered to be more freely constrainable in the preliminary phases of criminal proceedings, not to mention during intelligence activities. The use of promising technology, though 'inexplicable', is thus regarded as relatively unproblematic in numerous jurisdictions.

Naturally, practice had already shown how illusory such an impression is, especially where, due to copyright protection or excessive privatisation, AI tools are applied without any effective control by public authorities. Several of the tools raising such substantial critical concerns (well-known, but not isolated, the case of COMPAS) have incidentally been largely discussed in literature; hence, they will be mentioned here only to provide the necessary context to the main argument of the contribution.

---

[6] See, *ex multis*, Balkin (2015), pp. 54 ff; Quattrocolo (2020a), pp. 94 ff; Contissa and Lasagni (2020), p. 282. The issue is however relevant also in other fields, see for instance Lagioia and Contissa (2020), pp. 1 ff, with regard to the health care system.

[7] Cf. ECtHR, *Moreira Ferreira v. Portugal* (no. 2), App. no. 19867/12, 11 July 2017, §84; *Papon v. France* (dec.), App. no. 54210/00, 15 November 2001.

[8] For a specific analysis on the profile of the right to an effective remedy in this context, and some constructive proposal, see Contissa and Lasagni (2020), pp. 288 ff.

[9] Firstly, because "inexplicable" decisions are far from unknown, and even accepted to a certain extent also in "purely human" proceedings (Caianiello 2019, pp. 267 ff); Moreover, computer scientists are currently working on the AI technical limitations concerning explainability, and thus might soon produce satisfactory explicable models (Guidotti et al. 2018, pp. 1 ff). In any case, proposals have already been launched, to achieve legal and technical solutions that ensure compliance with fair trial rights, even with the current state of technical development (cf. Kroll et al. 2017, pp. 633 ff and, with specific reference to criminal proceedings, Contissa and Lasagni 2020, pp. 300 ff).

[10] Especially in multilevel legal orders; in this sense, see Caianiello (2021), p. 4, according to which "legality constitutes [. . .] a promise never fully kept", against which "AI and ML systems could satisfy, in the end, that relentless quest".

Its starting point is that AI and algorithms can be deployed in preventive and criminal investigations also with perspectives different from those experienced in predictive policing.

Certain AI systems, known as *Multi-Agent Systems* (MAS), for instance, point to a much deeper involvement of AI technology in the very shaping of the investigative proceeding. These tools have already proven to be an essential support in certain stages of the investigations, especially in the digital forensics' analysis of big data.

This study argues that MAS technology and in particular some of their specific application, like *MultiAgent Digital Investigation Toolkits*, could actually make a significative contribution also in a different and potentially groundbreaking direction: That of supporting fairness during investigations, by intervening in the formulation, assessment and selection of investigative hypotheses.

To this end, the chapter first offers a brief recollection of the most common criminal justice applications of AI and algorithmic systems, mostly of 'predictive' nature (Sect. 2). Second, the main traits of MAS technology will be introduced, to highlight what makes these tools especially valuable for investigative and preventive purposes (Sect. 3).

Finally, an analysis of the potential of MAS tools will follow, to shed light on how a mindful application of such systems could actually contribute to avoiding or at least reducing some typically human mistakes in investigation processes, capable to generate substantial miscarriages of justice, like the so-called *tunnel vision effect* (Sect. 4).

2 AI and Algorithms for Criminal Justice "Predictive" Purposes: State of Play

Although criminal law is sometimes perceived to be at the margins of the automation process that involves increasing sectors of our society, the high variety of applications that can already be counted in this domain, and the acceleration of this process in the last few years, show quite a different reality.

The deployment of AI and algorithms in criminal justice is often associated to so-called 'predictive' goals. As highlighted by legal scholars, however, the notion of 'prediction', when referred to such technology, needs be cautiously used. AI and algorithmic systems, indeed, can at their best 'only' produce highly accurate statistical analysis, which—as such—does not necessarily have a projection into future behaviours.[11] Hence, the decision to attribute a certain binding value to the assessment produced by these tools entirely relies on the discretionary policy choice of the legal system at stake.

Understood in these terms the general potential of 'predictive' systems, it is worth briefly recalling two main directions towards which they are mostly oriented,

[11] Cf. Quattrocolo (2020b), pp. 17–18; see also Caianiello (2021), p. 8, highlighting how statistics "cannot tell us with precision anything that concerns the position of a single individual".

namely: (1) supporting law enforcement in certain phases of the investigations (*predictive policing*); (2) support courts in judicial decision (*predictive justice*).

2.1 Predictive Policing

Predictive policing is today a very operational reality in several countries worldwide. In this regard, AI and above all algorithmic systems may be used for different purposes, mostly either to 'predict' some objective element of criminal activities (*e.g.* time and place of possible offences; potential victims), or to 'predict' the occurrence of individual behaviours with potential criminal relevance.[12]

Critical implications for the protection of fundamental rights however significantly vary in the two cases.

The first approach reflects traditional investigative techniques to map criminal activities in a given area, by analysing data on social, demographic, economic, environmental, and criminal background.

Its deployment mainly aims at optimising the allocation of human resources and equipment, channelling forces to areas where criminogenic risk is higher.[13] Examples of such tools, largely examined by legal scholars and mostly directed at predicting where street offenses are likely to occur, are, for instance, *PredPol*,[14] *XLaw*,[15] *Delia*,[16] *CAS*,[17] *PreCobs*,[18] *CAPP-PGH*,[19] or *KLB-Operativ*.[20]

[12] For a comprehensive overview, see Perry et al. (2013), pp. 8 ff; cf. also Isaac (2018), pp. 543 ff; Joh (2018), pp. 559 ff.

[13] The use of such systems is so common, that online databases have been created to check which software finds deployment in a certain local district, cf. https://atlasofsurveillance.org/search?utf8=%E2%9C%93&location=&technologies%5B86%5D=on.

[14] Developed by the police and the University of California, Los Angeles, the system makes forecasts based on three classes of data (type of offence, place where the offence was committed, and the date/time of its commission), that allow to identify, on a Web interface based on Google Maps, the high-risk areas in certain time periods, cfr. https://www.predpol.com/law-enforcement/#predPolicing; cf. also Huq (2019), p. 1070; Joh (2014), pp. 44–45.

[15] Designed by the Questura of Napoli, to predict the geographical and temporal occurrence of thefts and robberies, cf. https://www.xlaw.it/presentazione/index_eng.asp.

[16] Developed by the company *KeyCrime*, created by a former police officer and currently in use by the Milano police department, cf. https://www.keycrime.com/, on which see also Parodi and Sellaroli (2019), pp. 56 ff.

[17] *Crime Anticipation System*, created by the Amsterdam police (https://documen.site/download/crime-anticipation-system_pdf), on which see Mutsaers and van Nuenen (2020), pp. 1 ff.

[18] *Pre Crime Observation System*, http://www.ifmpt.de/, cf., *e.g.*, Bayerisches Landeskriminalamt (2015).

[19] *Coalition against Predictive Policing*, cf. https://capp-pgh.com/files/CPP%20Teach-in%2007-16-2020.pdf.

[20] *Kriminalitätslagebild*, https://atlas.algorithmwatch.org/datenbank/klb-operativ/, on which see Seidensticker et al. (2018), pp. 1 ff.

These systems can be appreciated, for their potential in contributing to a better management of law enforcement personnel and know-how, improving investigative performances at the local level in conditions of limited resources. Yet, their deployment has been long criticized in literature,[21] although in recent times such tools started to be considered relatively less problematic, at least in comparison with individual risk assessment technology.

This is not tantamount to say that they are devoid of critical aspects. Nonetheless, these systems seem to 'merely' perpetuate criticalities that already characterize the same activities when they are carried out by human beings, rather than being strictly related to the functioning of AI or algorithmic technology.

Moreover, although even severe discrimination cannot be excluded, these preventive systems are usually applied to guide the action of law enforcement, and not to directly issue decisions with binding legal effects.

Definitely more problematic are the instruments designed to issue individual assessments.

To put it simply, such systems—thanks to mathematical models and ML techniques, and by accessing huge amounts of data, otherwise often not available to law enforcement agencies—correlate statistical risk factors with specific individuals.

In many countries, case law has in the last few years started to attach legal value to such score risks, for instance by making the granting of probation or of alternative measures dependent upon a low-risk result. This phenomenon raises a number of concerns about the protection of fundamental rights, which have been repeatedly flagged by legal scholars and specialized working groups on both sides of the Atlantic.[22] In this sense, notorious is the case of COMPAS,[23] and of its judicial aftermaths in the *Loomis* case.[24] However, there are several more examples of tools

[21] For instance, by incorporating human bias, *e.g.* encouraging law enforcement to oversee certain neighbourhoods (not unfrequently, characterized by non-white communities) and thus making it more likely that the people living there will be subject to stop-and-frisk practices, cf. Huq (2019), p. 1109; Brayne (2017), pp. 977 ff; Epp et al. (2014), pp. 117–119. As it will be discussed below, however, once aware of such biases, AI can also be used to correct them (cf. n 55).

[22] Among which, as widely discussed, many of the USA national jurisdictions, and, to a lower extent, the United Kingdom; for a reference to the vast literature on the matter, see Garapon and Lassègue (2018); Huq (2019), pp. 1043 ff, Council of Europe (2017), pp. 10 ff.

[23] Developed by Equivant, a private company based in California (https://www.equivant.com/practitioners-guide-to-compas-core/), and currently adopted in several US states to calculate the rate of recidivism, as when issuing decisions on alternative measures or suspended sentences. The data used by COMPAS to issue its predictions are only partially known to the public, due to intellectual property rights on the software, and have already been strongly accused of creating discriminatory effects by non profit organizations, cfr. *ProPublica* Reports: Angwin et al. (2016) and Larson et al. (2016). See also Huq (2019), pp. 1047 ff.

[24] *State of Wisconsin v. Loomis*, 881 N. W.2d 749 (Wis. 2016), 36. Among the vast literature commenting the case in a critical perspective, see, *ex multis*, Lightbourne (2017), pp. 327 ff; Recent cases (2017), pp. 1530 ff; De Miguel Beriain (2018), pp. 45 ff; Quattrocolo (2020a), pp. 166 ff; Gialuz (2019), pp. 1 ff; Caianiello (2021), p. 16; Freeman (2016), pp. 75 ff. An unpublished case, similar to *Loomis* and issued by the Supreme Court of the District of Columbia, is reported by Quattrocolo (2020a), pp. 161 ff.

deployed worldwide to issue individual risk assessment, in the US (SASSI, LSI-R,[25] or PSA,[26] just to mention a few), as well as elsewhere (*e.g.* the British *HART*[27]).

Also, goal pursued by individual assessment risk tools can vary. For instance, in certain legal frameworks, they are reportedly used to perform like a polygraph (and with the same controversial implications[28]). This is, for instance, the case of the Spanish *Veripol*, used to 'measure' the truth of statements released by witnesses in car insurance proceedings, with the goal of avoiding insurance fraud.[29]

2.2 *Predictive Justice*

In contrast to the relatively consolidated application of predictive policing tools, instruments of predictive justice are still sensibly underdeveloped.

A comparison with civil proceedings especially reveals a significant gap in the field of criminal justice. In the civil law domain, indeed, AI and algorithms are increasingly deployed not only to support human decision-making, but also to directly substitute it, at least for cases with limited monetary value.[30] In criminal law, on the contrary, predictive justice is, at most, in a testing phase.

Examples of such projects may be found in several jurisdictions, although especially renown are the attempts to predict the behaviour of the United States Supreme Court Justices,[31] or the decisions of the Court in Strasbourg.[32] Regardless for the progressive improvement of their accuracy,[33] similar systems are still

[25] Level of Service Inventory-Revised (LSI-R) and Substance Abuse Substance Subtle Screening Inventory (SASSI), on which cf. *Malenchik v. State*, 928 N. E. 2d 564, 574 (Ind. 2010).

[26] The *Public Safety Assessment* is an individual risk assessment tool developed especially for the pretrial phase by the Laura and John Arnold Foundation and currently used in dozens of jurisdictions in the United States and in some of the largest cities in the country, such as Phoenix, Chicago Houston. To distance PSA from the numerous criticisms moved to *Compas*, the creators of this system decided to make information about its functioning public and to reveal the different weight of each of main nine factors used in the risk assessment calculation, cf. https://www.psapretrial.org/about.

[27] The Harm Assessment Risk Tool has been developed by the Durham Police and the University of Cambridge. It makes predictions based on 33 different metrics, including the offender's criminal record, age, and postcode. The parameters used by HART have been made at least partly accessible to the public, allowing to identify a number of relevant criticalities (*e.g.* that the tool is designed to promote false positives over false negatives, which means that it is more likely that a low-risk individual is wrongly classified as a high-risk person rather than the other way around, see Oswald et al. (2018), p. 236).

[28] See, for all, Steinbrook (1992), pp. 122 ff.; Brett et al. (1986), pp. 544 ff.

[29] https://www.rtve.es/noticias/20180918/inteligencia-artificial-para-detectar-denuncias-falsas-policia/1801640.shtml, on which see Liberatore et al. (2019), pp. 89 ff.

[30] See for instance the Estonian example, cf. Niller (2019).

[31] Cf. Katz et al. (2017) and Guimerà and Sales-Pardo (2011).

[32] Cf. Altreas et al. (2016), pp. 2 ff.

[33] Average accuracy could be estimated around 80%, or—at least—most renown studies are within that range, cf. Katz et al. (2017), p. 14: "over nearly two centuries, we achieve 70.2% accuracy at the

generally deemed too low performers to play a significant role in the resolution of criminal cases.[34]

Perhaps because of their reference to the trial phase, rather than to the less defence-oriented investigative stage, accuracy seems indeed to be examined in this context through much narrower lenses than in their predictive policing correspondents.[35]

At least for the time being, hence, these instruments continue to retain no legal binding value and are widely regarded as mere scientific experiments.

3 Much More than Predictions: Exploring New(er) Frontiers for AI-Powered Investigations

'Prediction', however, represents only a fraction of the AI and algorithmic potential in criminal proceedings, and perhaps not even the most groundbreaking one.[36]

Data analysis carried out through AI tools, for instance, although less cinematographic, has drastically changed both the way evidence search is pursued by law enforcement, and the realistic expectations of privacy in most of our daily activities.

In truth, against a massive and constant production of digital data in every field of private and professional life, relying on AI seems an increasingly appealing option for the law enforcement, struggling to find a sustainable way to select relevant information.

This is a task for which a specific form of this technology, namely Multi-Agent Systems (MAS), seems to offer a particularly promising contribution.

---

case outcome level and 71.9% at the justice vote level. More recently, over the past century, we outperform an *in-sample optimized* null model by nearly 5%"; Guimerà and Sales-Pardo (2011), p. 4: "For these artificially–generated ideal courts, we find that both the majority rule and the stochastic block model algorithms correctly predict 71% of individual justices votes [. . .] For real courts, on the other hand, the block model algorithm correctly predicts 83% of the individual justices' decisions"; Altreas et al. (2016), p. 2: "Our models can reliably predict ECtHR decisions with high accuracy, i.e., 79% on average".

[34] In this sense also the Council of Europe (2017), p. 11, according to which the low level of accuracy "is therefore considered premature at the current time to imagine such systems replacing judges".

[35] Garapon and Lassègue (2018); Manes (2020), pp. 551 ff.

[36] Other relevant applications of AI technology in this domain, just to mention a few, concern facial recognition (specifically dealt with in this volume by Neroni Rezende). Although this specific sector has somehow long received less attention by legal scholars (see, however, Susskind (2017), pp. 11 ff; Caianiello (2021), pp. 2 and 5, also with regard to the advantages for legal entities), extremely relevant is also the deployment of AI technology in providing support to the defence counsels' activity, today addressed by several dedicated platforms, see, *e.g.*, CrossJustice (*Knowledge, Advisory and Capacity Building Information Tool for Criminal Procedural Rights in Judicial Cooperation*) developed within the EU Justice Programme (GA no. 847346), available at: https://crossjustice.eu/en/index.html.

As it will be argued further below, though, the potential of MAS technology could actually be even greater, bringing to an util now unprecedented level of integration between human and machine skills in carrying out investigations.

Before moving to this analysis, however, a brief clarification on MAS functioning is in order.

Multi-Agent Systems are a development of AI technology, characterized by a set of specific features.

The main idea behind its development is that there are problems too complex to be solved with predefined reasoning settings.[37] Such problems hence call for different approaches: structured and, at the same time, granted with a certain versatility.

MAS present a number of characteristics that made this technology particularly suitable to address these challenges, especially where solutions do not appear easily pre-definable—as it could well be a criminal case scenario.

As the term reveals, Multi-Agent Systems are based on the coordinated action of several 'agents', that cooperate with each other to deliver a result. Such agents may be defined as *autonomous*, *reactive*, and *interactive*. The action of each agent is indeed shaped by *intention*, in other words, by the goal that the agent aims to achieve through its assigned task in a rational and not-predefined way.[38]

Another fundamental element of MAS technology is that agents "should be somehow *organized*".[39] To this end, norms must be established, that agents should obey or comply with. It follows that agents could be structured in a hierarchical framework, under the supervision of an operational or strategic manager,[40] which could, for instance, take care of task allocation.[41]

[37] Hindriks (2014), p. 4; Wooldridge (2009), p. 19 ff.

[38] Cf. Hindriks (2014), p. 2; Wooldridge and Jennings (1995), pp. 115 ff; Rao and Georgeff (1991), pp. 473 ff.

[39] Hindriks (2014), p. 4.

[40] Hoelz et al. (2009), p. 884.

[41] Different organization models can actually be designed, whose complexity depends on the system and the needs emerging from the case at stake. For a quite structured organizational system, see *e.g.* Ganesch (2018), p. 97: The "strategic manager receives different cases to perform the forensic analysis. According to the organization's priorities, the strategic manager defines the order of execution and amount of resources (number of computers) for each case. A tactical manager is the[n] assigned to one specific case which can contain several evidences, like a number of hard drives. The tactical manager defines the priority of its evidences and distributes them to the available operational managers, which are limited by the resources available to that case. The operational manager will employ the necessary specialized agents to perform the different tasks it deems important to examine a piece of evidence".

4 MAS: Shaping a New Way to Carry Out Investigations

As anticipated, MAS technology has proven a very valuable tool for digital investigations.[42]

This is indeed one of the contexts where, *par excellence*, investigators must struggle not only in identifying the potential solution of a case, but, preliminarily, in determining which elements are potentially relevant to that end.[43] Given the vast amount of information that might be present on a device, or on the cloud, this step is inherently challenging, especially if similar activities need to be carried out in almost every criminal case.

It is therefore not surprising that several tools have been developed, in the last decades, precisely to support human investigators in such tasks.[44] Examples in this regard are, for instance, the *Open Computer Forensics Architecture* (OCFA),[45] the *Digital Forensics Framework* (DFF),[46] *Fiwalk*,[47] the *Advanced Automated Disk Investigation Toolkit* (AUDIT).[48] Among the vast range of MAS technology deployed in this field, particularly interesting for this contribution is then the *MultiAgent Digital Investigation toolKit* (MADIK).

MADIK systems are composed of a set of intelligent software agents, set to perform different analysis on pieces of digital evidence. The rationale behind the use of such technology is to facilitate the classification of digital information, through a score system that differentiates from "Absolutely Irrelevant" to "Probably Case-Relevant".[49]

To do so, each agent contains a set of rules and knowledge base, derived from human expertise (*e.g.* from law enforcement officers). Thanks to it, agents are enabled to examine the elements at their disposal and determine which piece(s) of information are most pertinent to the case.

Such tools can be applied within criminal investigations, as well as, actually, to any other forms of digital investigations in other sectors (for example, labor law disputes).

At the same time, MAS systems may also be usefully deployed in preventive investigations.

---

[42] Cf., *e.g.*, Beebe and Clark (2005), pp. 147 ff; Karabiyik and Aggarwal (2016), pp. 379 ff.

[43] Cf. Brighi and Ferrazzano (2021), pp. 43 ff.

[44] Among the first to propose such deployment, Stallard and Levitt (2003), pp. 160 ff. See also the further proposals by Liao et al. (2009), pp. 1881 ff; Fizaine and Clarke (2013), p. 73.

[45] Vermaas et al. (2010), pp. 45 ff.

[46] www.digital-forensic.org, France, 2016.

[47] Garfinkel (2009), pp. 73 ff

[48] Karabiyik and Aggarwal (2016), pp. 381 ff.

[49] Hoelz et al. (2009), pp. 883 ff; Ganesch (2018), pp. 96 ff.

Perhaps the most immediate reference in this sense goes to inquiries carried out on social media, to identify potential offenders or crime patterns and reduce victimisation.[50] Concrete applications can hence vary enormously, from anti-hate speech control to terrorism or organized crime.

The use of MAS alike technology is also increasingly appealing in the fight against financing of terrorism and money laundering. As Suspicious Activity Reports by financial institutions are steadily increasing, Financial Intelligence Units throughout the world struggle to keep up with a preventive action that has already gone way beyond human-only capacities.[51] Deployment of AI technology hence more and more appears as a compulsory choice, to trace back the 'digital trail' of suspicious financial flows in a globalized and hyperconnected world.[52]

4.1 Not Only Digital Forensics: An AI Approach to Investigative Uncertainty

The potential of MAS systems, however, could extend also to goals which go far beyond digital data analysis.

Particularly interesting, in this regard, is the aforementioned MADIK system and its so-called 'distributed nature'. The idea behind this feature refers to the fact that a task (*e.g.* identifying relevant information on a device) can best be carried out not only by one single agent at the time, but, simultaneously, by several agents.

Each of them is thus performing its own assessment of the given problem. This profile has a direct impact on the way in which decision-making is shaped within these tools. Since different agents can produce diverging results, it is indeed for the system operational manager to solve divergences. Several rules can be established in this regard.

For instance, Hoelz et al. describe a system where the manager decides to rely on those agents which—due to their specific training—have better performed in the past with regard to similar tasks.[53] If the results provided by a specific agent are deemed to be inaccurate, the 'confidence' of the manager on its ability to answer to the given

[50] As supported by several political instances, cf. Rifkind (2014), pp. 143 ff; Toor (2016). For some examples of technical implementations, see Gonçalves Evangelista et al. (2020), pp. 1 ff.; Scrivens et al. (2019), pp. 179 ff; Panagiotou et al. (2019), pp. 1 ff; Ball (2016), pp. 147 ff.

[51] For an in-depth comparative examination of AML/CFT regimes, cf. Vogel and Maillart (2020); for a recognition of Financial Intelligence Units' structure and powers, see Lasagni (2019), pp. 93 ff.

[52] IBM (2019), pp. 1 ff; Deloitte (2018), pp. 1 ff; on the compatibility of such systems with fundamental rights in the EU, see Maxwell et al. (2020), pp. 5 ff.

[53] Similarly to the machine learning procedure, the correctness of the agents' results relies—at least at first—on a review interface used by the human experts, cf. Hoelz et al. (2009), p. 886; Ganesch (2018), p. 97: "MADIK uses case-based reasoning (CBR) to determine which agents are better employed in which kind of investigation. This also allows the agents to reason about the evidences in a way that is more adequate to the special case in question".

problem will diminish. Its performances will thus likely bear less weight in future queries of the same sort. On the contrary, where the performance of the agent is deemed positive, the manager's confidence increases, and this 'appreciation' will be recalled also in future investigations.[54]

This, however, does not represent a fixed rule. Different rule models could be developed, for example by diminishing the role of precedents, in order to reduce potential investigative blind spots caused by overreliance on past assessments.

Against this background, MAS show a broad range of potential for AI technologies in criminal justice.

Indeed, those who promote the recourse to AI and algorithmic systems often do so with the aim (or the hope) of objectivizing or standardizing the human based criminal justice system towards more accurate outcomes. In other words, to obtain a fairer justice by making it less subject to variable, subjective and potentially discriminatory influences.[55] Making it simpler for human beings to assess a complex and uncertain situation is certainly a positive and desirable goal that poses in favour of a mindful deployment of AI technology to the criminal matter. This aim, however, is not the only goal that can be pursued thanks to Multi-Agent Systems.

MAS, and especially MADIK systems, open also to a different perspective, that is a use of AI technology not to pursue (legal) certainty, but to rationally manage (legal) uncertainty. Indeed, these AI systems seem already capable of living with a certain degree of complexity and unpredictability, typical of human vicissitudes. Due to their characteristics, MAS show us that machines can today be deployed for tasks other than simplifying the performance of complex human activities, requiring a certain predictive reasoning or high statistical calculating skills.

Said otherwise, the AI potential to "reduce the noise"[56] in criminal proceedings—for instance, by selecting *the* relevant information in digital investigations among a bulk of available data—is only one of its possible applications.

Especially in the early stages of the proceedings, also a different skill does reveal its crucial importance, *i.e.* the capacity to leverage the notion of conflict, instead of avoiding it, thus ensuring fairness to the whole procedure.

Building on the illustrated features, a further use for MADIK technology (or alike) could hence be foreseen, namely a deployment aiming *precisely to preserve the necessary degree of uncertainty* that is typical of the investigative phases.

As is well-known, one of the features that makes initial stages of criminal proceedings so sensitive to potential miscarriages is the difficulty of detecting the best investigative hypothesis among the different possible ones.

[54] Cf. Hoelz et al. (2009), p. 886.

[55] Cf. Sunstein (2019), pp. 499 ff; illustrative in this sense also the expression by Deskus (2018), p. 243: "A judge's bad day or heavy docket does not affect the algorithm". Highlighting the influence of daily activities (such as breakfast or lunch time schedules) on the harshness of human sentencing, Eagleman (2015), p. 266; see also Sartor and Lagioia (2020), pp. 63 ff.

[56] This is often the desired outcome: cf. famously Kahneman et al. (2021).

Philosophers and social scientists have long recognized how human understanding is usually quite struggling in dealing with multiple-option contexts, observing that, once we have

> adopted an opinion, [it] draws all things else to support and agree with it. And though there be a greater number and weight of instances to be found on the other side, yet these it either neglects and despises, or else by some distinction sets aside and rejects; in order that by this great and pernicious predetermination the authority of its former conclusions may remain inviolate.[57]

This almost involuntary tendency towards simplification has significant repercussions for criminal investigations. This is the reason why forensic psychologists identify a substantial safeguard against miscarriages of justice in the capacity of investigators not to pre-determine their minds.[58]

The reference, in particular, goes here to the so-called *tunnel vision effect*, according to which criminal justice actors tend relatively early to focus on a specific suspect or investigative trail. The significance of evidence and clues that could 'build a case' supporting the adopted insight gets thus elevated, while elements which appear inconsistent with it are overlooked or dismissed as irrelevant, incredible, or unreliable.[59]

Tunnel vision effect, however, "is more often the product of the human condition as well as institutional and cultural pressures, than of maliciousness or indifference".[60] To this regard, social scientists highlighted that the human tendency to "typically consider only one hypothesis at a time and often make the assumption at the outset that that hypothesis is true" does not exclude a potential for improvement, achievable by "training people to think of alternative hypotheses early in the hypothesis-evaluation process".[61]

4.2 MAS as a Tool to Ensure Fairness in Criminal Investigations?

Against this background, MAS technology could be a way to make those aspirations viable. To this end, it is argued here that the same approach developed for digital

[57] Cf. Bacon (1939), original work published in 1620, p. 36; more recently, see *e.g.* Nickerson (1998), pp. 176 ff.

[58] See, among others, Wason (1960), pp. 129 ff; Lange (1975), pp. 311 ff; Nickerson (1998), p. 193, inquiring also on the potential causes that lead to this confirmation bias tendency (pp. 197 ff); Meissner and Kassin (2004), pp. 85 ff; Findley and Scott (2006), pp. 291 ff; Dror et al. (2006), pp. 74 ff; Forza (2018), pp. 395 ff.

[59] Cf. Martin (2002), pp. 847–848; Raeder (2003), pp. 1327–1328.

[60] Findley and Scott (2006), p. 292.

[61] Nickerson (1998), p. 211, according to whom "evidence provides reason for optimism that the approach can work".

evidence could be applied by Multi-Agent Systems also with regard to investigative hypothesis.

The idea is, that AI might be usefully deployed to support human investigative decision-making *by guaranteeing that divergent reconstructions within criminal investigations remains unsolved, at least to a certain stage*.

Multi-Agent Systems can support human law enforcement in the selection process of investigative insights, at the same time maintaining a certain degree of openness to the material examined. This is so, because the different reconstructions produced by the autonomous 'agents' are brought back to (a certain) unity only with the intervention of the operating manager.

Until then, MAS distributed nature could be exploited to ensure that agents composing the investigative team are sufficiently diversified, so as to be able to spot, and develop, as many investigative hypotheses as possible.

Naturally, the identification of a precise timeline (until when shall the uncertainty of investigations be preserved?) is far from being a straightforward task. The demand not to preclude any potential investigative lead, to ensure a more comprehensive examination, shall indeed also be balanced with the necessity of safeguarding the rights of the individuals that might become involved in the investigations (defendants or other third parties). Needless to say, the use of AI in this domain should be carried out carefully.

It should be considered, however, that the risk to either close too early or broaden too much the investigations already exists in purely 'human' scenarios. As it is the case for all AI applications, MAS or MADIK technology do not contain a predefined magic formula that suddenly erases all human biases, although they can make them more visible.

Thus, a crucial role will continue to be played by the principle of proportionality and by the supervisory mechanisms already in place to oversee on the correct performance of criminal investigations (first of all, judicial review).

Also, the capacity of such systems to operate as a 'mind-openers' clearly depends on how much human experts carried out a diversified training of automated agents. Machine training is however an 'old' issue, which risks undermining the effectiveness (and fairness) of all Machine Learning technology, and not of MAS exclusively.[62]

If proper training is ensured, the potential of MAS technology could be groundbreaking. The analysis carried out by automated agents could help testing the soundness of diverging investigative hypotheses or identifying reconstructions of the event difficult to spot.

AI expertise might be used, for instance, in contexts where it is not possible to deploy enough human agents to ensure an adequate variety of investigative perspectives since the beginning of the proceeding, due to limited human resources. MAS

[62] Cf., *e.g.*, Miller (2014), pp. 106 ff; Quattrocolo (2020a), p. 67; Roberts et al. (2021), pp. 199 ff, highlighting the limits of ML technology with regard to the Covid-19 pandemic.

technology could also help deciphering unintelligible crime scenes, where clues or relevant material is scarce or hard to interpret.

Regardless of the subject matter, the reasoning model of Multi-Agent Systems could indeed be deployed to prevent relevant investigative insights be lost at an early stage of the proceeding, due to time or resources constraints.

Lastly, it is worth recalling that MAS technology could be successfully exploited also by actors other than law enforcement and prosecutors.

Such tools could actually be used also by the counsellors representing the defendant or the victim, to check whether all potential investigative leads had been duly pursued. In this regard too, therefore, AI technology could find so far unexplored, but potentially revolutionary areas of applications within the criminal justice system.

5 Conclusion

This contribution aimed at lifting the veil on a new possible deployment of AI technology within preventive and criminal investigation.

To do so, an inventive effort is requested to lawyers, legal informatics and computer scientists, with a view to trying to walk unexplored paths for criminal justice principles to find effective implementation in the 'hyperhistory' time that we are living.[63]

Obviously, mistakes are in order in this quest, and options that seem easy to realise on paper do not necessarily share the same fate in practice. This awareness should not however discourage from insisting on trying.

Multi-Agent Systems, for once, seem to open interesting and innovative perspectives over an AI-enabled version of the ancient Socratic method. Falsification[64] as a way to achieve procedural fairness is an essential feature of modern criminal justice systems. In most legal orders, however, fair trial principles find only a partial application in the investigative phase.

Here it is argued that MAS technology could help extend their safeguarding value also to the very beginning of the proceeding, giving new tools to law enforcement, as well as to defence lawyers, to better perform in their respective roles.

Of course, the limited remit of this contribution only allowed to begin shedding light on a new potential for AI in criminal investigation.

Its provisional conclusion will need to be further substantiated, also to face the many questions that arise any time AI technologies are at stake. Actual technical capacities of MAS tools in this domain, for once, will have to be specifically tested, and highly specialized investigative training shall be carefully designed to transform the illustrated potential into operational reality.

[63] For the term, see again Floridi (2014), p. 24.

[64] On which, see, famously, Popper (2002), original work published in 1934.

Who worries that investigative procedures may be "dumbed down"[65] by excessive human reliance on automation, however, should feel reassured: Human skills are far from becoming irrelevant in the process. Training, in particular, clearly draws a dividing line between a true empowerment of human investigative skills and a mere digital re-proposition of old biases and prejudices.

AI technology is here to stay; as famously stated, all we have to decide is what to do with the time that is given to us, and, of course, with its challenges.

Finding new ways to put automated technology at the service of fairness in criminal justice, and not just of its (supposed) efficiency, might be a good idea. In other words, the question is not whether humans are still making a difference, we do. Point is: We have to make it an encouraging thought.[66]

References

Altreas N, Tsarapatsanis D, Preoțiuc-Pietro D, Lampos V (2016) Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective. PeerJ Comput Sci (Open Access). https://peerj.com/articles/cs-93.pdf

Angwin J, Larson J, Mattu S, Kirchner L (2016) Machine bias: there's software used across the country to predict future criminals. And it's biased against blacks, 23.05.2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bacon F (1939) Novum organum. In Burtt EA (ed) The English philosophers from Bacon to Mill New York, Random House, pp 24–123 (original work published in 1620)

Balkin JM (2015) The path of robotics law. Calif Law Rev 6:45–60

Balkin JM (2017) The three laws of robotics in the age of big data. Ohio State Law J 78:1217–1241

Ball L (2016) Automating social network analysis: a power tool for counter-terrorism. Secur J 29: 147–168

Bayerisches Landeskriminalamt (2015) Abteilung V, Positionspapier zum Einsatz von PRECOBS bei der Bayerischen Polizei, Forum KI am 24./25.06.2015 beim BKA zum Thema Predictive Policing und geografische Kriminalitätsanalyse. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/ForumKI/ForumKI2015/kiforum2015EggerPositionspapier.pdf?__blob=publicationFile&v=1

Beebe N, Clark JG (2005) A hierarchical, objectives-based framework for the digital investigations process. Digit Investig 2(2):147–167

Brayne S (2017) Big data surveillance: the case of policing. Am Sociol Rev 82(5):977–1008

Brett A, Phillips M, Beary FJ III (1986) Predictive power of the polygraph: can the "Lie Detector" really detect liars? Lancet I(8480):544–547

Brighi R, Ferrazzano M (2021) Digital forensics: best practices and perspective. In: Caianiello M, Camon A (eds) Digital forensic evidence: towards common European standards in antifraud administrative and criminal investigations. Wolters Kluwer/CEDAM, Collezione di giustizia penale, pp 13–48. https://site.unibo.it/devices/en

Caianiello M (2019) Criminal process faced with the challenges of scientific and technological development. Eur J Crim Crim Law Crim Just 27(4):267–291

[65] See James and Gladyshev (2013), pp. 2 ff; Meyers and Rogers (2004), pp. 5 ff.

[66] Freely rephrasing Tolkien (2004), original work published in 1954, pp. 51 ff.

Caianiello M (2021) Dangerous liaisons. Potentialities and risks deriving from the interaction between artificial intelligence and preventive justice. Eur J Crim Crim Law Crim Just 29(1): 1–23
Contissa G, Lasagni G (2020) When it is (also) algorithms and AI that decide on criminal matters: in search for an effective remedy. Eur J Crim Crim Law Crim Just 28(3):280–304
Council of Europe (2017) Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, 6.10.2017. https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a
De Miguel Beriain I (2018) Does the use of risk assessments in sentences respect the right to due process? A critical analysis of the Wisconsin v. Loomis ruling. Law Probab Risk 17:45–53
Deloitte (2018) The case for artificial intelligence in combating money laundering and terrorist financing. A deep dive into the application of machine learning technology, pp 1–40. https://www2.deloitte.com/id/en/pages/financial-advisory/articles/the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.html
Deskus C (2018) Fifth amendment limitations on criminal algorithmic decision-making. N Y Univ J Legis Public Policy 21:237–286
Dror IE, Charlton D, Péron AE (2006) Contextual information renders experts vulnerable to making erroneous identifications. Forensic Sci Int CLVI(1):74–78
Eagleman D (2015) The brain. The story of you. Pantheon Books/Canongate Books, New York/Edinburgh
Epp CR, Maynard-Moody S, Haider-Markel D (2014) Pulled over: how police stops define race and citizenship. University of Chicago Press, Chicago
Ferguson AG (2018) Illuminating black data policing. Ohio State J Crim Law 15:503–525
Findley K, Scott M (2006) The multiple dimensions of tunnel vision in criminal cases. Wisconsin Law Rev MMVI(108):291–397
Fizaine J, Clarke N (2013) A crime-dependent automated search engine for digital forensics. Adv Commun Comput Netw Secur 10:73–87
Floridi L (2014) The 4th revolution. How the infoshpere is reshaping human reality. Oxford University Press, New York
Forza A (2018) La psicologia nel processo penale. Giuffrè, Milano
Freeman K (2016) Algorithmic injustice: how the Wisconsin Supreme Court failed to protect due process rights in State v. Loomis. NCJL Technol 18:75–106
Ganesch V (2018) A cyber crime evidence collection and multiagent digital investigation toolkit. IJCRT 6(1):94–99
Garapon A, Lassègue J (2018) Justice digitale: révolution graphique et rupture anthropologique. PUF, Paris
Garfinkel S (2009) Automating disk forensic processing with SleuthKit, XML and Python. In: Proceedings of the fourth IEEE international workshop on systematic approaches to digital forensic engineering, pp 73–84
Gialuz M (2019) Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei rischi assessment tools tra Stati uniti ed Europa. Dir pen cont. 29.05.2019. https://archiviodpc.dirittopenaleuomo.org/d/6702-quando-la-giustizia-penale-incontra-l-intelligenza-artificiale-luci-e-ombre-dei-risk-assessment-too
Gonçalves Evangelista JR, Sassi RJ, Romero M, Napolitano D (2020) Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with artificial intelligence. J Appl Secur Res, pp 1–25
Goodfellow R, McDaniel P, Papernot N (2018) Making machine learning robust against adversarial inputs. Commun ACM 61(7):56–66
Guidotti R, Monreale A, Ruggieri S, Turini F, Giannotti F, Pedreschi D (2018) A survey of methods for explaining Black Box models. ACM Comput Surv 51(5), Article 93, 42 pp
Guimerà R, Sales-Pardo M (2011) Justice blocks and predictability of U.S. Supreme Court votes. PLoS ONE 6(11):e27188m. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0027188

Henderson SE (2018) A few criminal justice big data rules. Ohio State J Crim Law 15:527–541
Hildebrandt M (2015) Smart technologies and the end(s) of law. Novel entanglements of law and technology. Edward Elgar, Cheltenham
Hindriks KV (2014) The shaping of the agent-oriented mindset: twenty years of engineering MAS. In: Dalpiaz F, Dix J, van Riemsdijk MB (eds) Engineering multi-agent systems, second international workshop, EMAS 2014, Paris, France, May 5–6, 2014. Revised selected papers. Springer, Cham, pp 1–14
Hoelz BWP, Ghedini Ralha C, Geeverghese R (2009) Artificial intelligence applied to computer forensics. In: Proceedings of the 2009 ACM symposium on applied computing, pp 883–888
Huq AZ (2019) Racial equity in algorithmic criminal justice. Duke Law J 6(68):1043–1134
IBM (2019) Fighting financial crime with AI. How cognitive solutions are changing the way institutions manage AML compliance, fraud and conduct surveillance, pp 1–18. https://www.acfcs.org/fighting-financial-crime-with-ai-how-cognitive-solutions-are-changing-the-way-institutions-manage-aml-compliance-fraud-and-conduct-surveillance-new-ibm-whitepaper/
Isaac WS (2018) Hope, hype, and fear: the promise and potential pitfalls of artificial intelligence in criminal justice. Ohio State J Crim Law 15:543
James J, Gladyshev P (2013) Challenges with automation in digital forensic investigations, Digital Forensic Investigation Research Group, University College Dublin, Ireland. https://arxiv.org/ftp/arxiv/papers/1303/1303.4498.pdf
Joh EE (2014) Policing by numbers: big data and the fourth amendment. Wash Law Rev 89:35–68
Joh EE (2018) Automated policing. Ohio State J Crim Law 15:559
Kahneman D, Sibony O, Sunstein CR (2021) Noise: a flaw in hu-man judgment. Little Brown Spark, New York
Karabiyik U, Aggarwal S (2016) Advanced automated disk investigation toolkit. In: Peterson G, Shenoi S (eds) Advances in digital forensics, XII. DigitalForensics 2016. IFIP advances in information and communication technology, vol 484. Springer, Cham, pp 379–396
Katz DM, Bommarito MJ II, Blackman J (2017) A general approach for predicting the behavior of the Supreme Court of the United States. PLoS ONE 12(4):e0174698. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0174698
Kroll JA, Huey J, Barocas S, Felten EW, Reidenberg JR, Robinson DG, Yu H (2017) Accountable algorithms. Univ Pa Law Rev 165:633–705
Lagioia F, Contissa G (2020) The strange case of Dr Watson: liability implications of AI evidence-based decision support systems in health care. Eur J Leg Stud 12:1–44
Lagioia F, Sartor G (2020) Artificial intelligence in the big data era: risks and opportunities. In: Cannataci J, Falce V, Pollicino O (eds) Legal challenges of big data. Edward Elgar, pp 280–307
Lange EJ (1975) The illusion of control. J Pers Soc Psychol 32(2):311–332
Larson J, Mattu S, Kirchner L, Angwin J (2016) How we analyzed the COMPAS recidivism algorithm. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm
Lasagni G (2019) Banking supervision and criminal investigation. Comparing the EU and US experiences. Springer, Cham
Liao N, Tian S, Wang T (2009) Network forensics based on a fuzzy logic and expert system. Comput Commun 32(17):1881–1892
Liberatore F, Quijano-Sánchez L, Camacho-Collados M (2019) Applications of data science in policing: VeriPol as an investigation support tool. Eur Law Enforc Res Bull IV:89–96. https://www.cepol.europa.eu/sites/default/files/European_Law_Enforcement_Research_Bulletin_Special_Conference_Edition_Nr4_web.pdf
Lightbourne J (2017) Damned lies & criminal sentencing using evidence-based tools. Duke Law Technol Rev 2017:327–343
Manes V (2020) L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia. In: Ruffolo U (a cura di) Intelligenza artificiale. Il diritto, i diritti, l'etica. Giuffrè, Milano
Martin DL (2002) Lessons about justice from the "Laboratory" of wrongful convictions: tunnel vision, the construction of guilt and informer evidence. UMKC Law Rev 70:847–864

Maxwell W, Bertrand A, Vamparys X (2020) Are AI-based Anti-Money Laundering (AML) systems compatible with European fundamental rights? ICML 2020 Law and Machine Learning Workshop. https://hal.archives-ouvertes.fr/hal-02884824v4/document

Meissner CA, Kassin SM (2004) You're guilty, so just confess! Cognitive and behavioural confirmation biases in the interrogation room. In: Lassiter GD (ed) Interrogations, confessions and entrapment. Springer, New York, pp 85–106

Meyers M, Rogers M (2004) Computer forensics: the need for standardization and certification. Int J Digit Evid 32(2):1–11

Miller K (2014) Total surveillance, big data, and predictive crime technology: privacy's perfect storm. J Technol Law Policy 19:105–146

Mutsaers P, van Nuenen T (2020) Predictively policed: the Dutch CAS case and its forerunners. https://www.researchgate.net/publication/346593158_Predictively_policed_The_Dutch_CAS_case_and_its_forerunners

Nickerson R (1998) Confirmation bias. A ubiquitous phenomenon in many guises. Rev Gen Psycol 2(2):175–220

Niller E (2019) Can AI be a fair judge in court? Estonia thinks so. Wired, 25 March 2019. https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/

O'Neil C (2016) Weapons of math destruction: how big data increases inequality and threatens democracy. Crown Publishers, New York

Oswald M, Grace J, Urwin S, Barnes GC (2018) Algorithmic risk assessment policing models: lessons from the Durham hart model and 'Experimental' proportionality. Inf Commun Technol Law 27(2):223–250

Panagiotou A, Ghita B, Shiaeles S, Bendiab K (2019) FaceWallGraph: using machine learning for profiling user behaviour from Facebook Wall. In: Galinina O, Andreev S, Koucheryavy Y, Balandin S (eds) Internet of Things, smart spaces, and next generation networks and systems - 19th international conference, NEW2AN 2019, and 12th conference, ruSMART 2019, Proceedings. Lecture Notes in Computer Science, vol 11660, Springer, pp 125–134, 19th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networks and Systems, NEW2AN 2019, and 12th Conference on Internet of Things and Smart Spaces, ruSMART 2019, St. Petersburg, Russian Federation, 26/08/1

Parodi C, Sellaroli V (2019) Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco. Riv trim Dir pen cont 6:47–203

Pasquale F (2015) The Black Box Society: the secret algorithms that control money and information. Harvard University Press, Cambridge

Perry WL, McInnis B, Price CC, Smith SC, Hollywood JS (2013) Predictive policing. The role of crime forecasting in law enforcement operations, RAND. Safety and Justice Program, USA, Library of Congress, pp 1–155

Popper K (2002) The logic of scientific discovery, 2nd edn. Routledge (original work published in 1934)

Quattrocolo S (2020a) Artificial intelligence, computational modelling and criminal proceedings. A framework for a European legal discussion. Springer, Cham

Quattrocolo S (2020b) Speech at the debate of 20 October 2020, published in Processo penale e Intelligenza Artificiale, Position Paper/1., Fondazione Leonardo, pp 17 ff.

Raeder M (2003) What does innocence have to do with it? A commentary on wrongful convictions and rationality. Mich State Law Rev 2003:1315–1335

Rao AS, Georgeff MP (1991), Modeling rational agents within a BDI-architecture. In Allen J, Fikes R, Sandewall E (eds) Proceedings of the 2nd international conference on principles of knowledge representation and reasoning (KR 1991), Cambridge, USA, Morgan Kaufmann, April 22–25, pp 473–484

Recent Cases (2017) State v. Loomis, Wisconsin Supreme Court requires warning before use of algorithmic risk assessments in sentencing. Harv Law Rev 130:1530 ff. https://harvardlawreview.org/2017/03/state-v-loomis/

Rifkind M (2014) Report on the intelligence relating to the murder of Fusilier Lee Rigby. House of Commons, Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office
Roberts M, Driggs D, Thorpe M et al (2021) Common pitfalls and recommendations for using machine learning to detect and prognosticate for COVID-19 using chest radiographs and CT scans. Nat Mach Intell 3:199–217
Russell SJ, Norvig P (2010) Artificial intelligence: a modern approach, 3rd edn. Prentice Hall, Englewood Cliffs
Sartor G, Lagioia F (2020) Le decisioni algoritmiche tra etica e diritto, in Intelligenza artificiale. In: Ruffolo U (a cura di) Intelligenza artificiale. Il diritto, i diritti, l'etica. Milano, Giuffrè, pp 63–88
Scrivens R, Gaudette T, Davies G, Frank R (2019) Searching for extremist content online using the dark crawler and sentiment analysis. In: Deflem M, Silva DMD (eds) Methods of criminology and criminal justice research. Emerald Publishing, pp 179–194
Seidensticker K, Bode F, Stoffel F (2018) Predictive policing in Germany. https://www.researchgate.net/publication/332170526_Predictive_Policing_in_Germany
Stallard T, Levitt K (2003) Automated analysis for digital forensic science: semantic integrity checking. In: Proceedings of the nineteenth annual computer security applications conference, December 8–12. IEEE Computer Society, Washington, DC, pp 160–167
Steinbrook R (1992) The Polygraph Test: a flawed diagnostic method. N Engl J Med CCCXXVII (2):122–123
Sunstein CR (2019) Algorithms, correcting biases. Soc Res Int Q 86(2):499–511
Susskind R (2017) Tomorrow's lawyers. An introduction to your future, 2nd edn. Oxford University Press, Oxford
Tolkien JR (2004) The Lord of the Rings. Harper Collins Ebook (original work published in 1954)
Toor A (2016) Automated systems fight ISIS propaganda, but at what cost? The Verge http://www.theverge.com/2016/9/6/12811680/isis-propaganda-algorithm-facebook-twitter-google. Accessed 27 July 2021
Ubertis G (2020) Intelligenza artificiale, giustizia penale, controllo umano significativo. Riv Trim Dir pen cont 4:75–88
Vermaas O, Simons J, Meijer R (2010) Open computer forensic architecture a way to process terabytes of forensic disk images. In: Huebner E, Zanero S (eds) Open source software for digital forensics. Springer, New York, pp 45–67
Vogel B, Maillart JB (eds) (2020) National and International Anti-Money Laundering Law. Developing the architecture of criminal justice, regulation and data protection. Intersentia, Antwerp
Wason PC (1960) On the failure to eliminate hypotheses in a conceptual task. Q J Exp Psychol 12(3):129–140
Wooldridge M (2009) An introduction to multiagent systems, 2nd edn. Wiley, pp 1–453
Wooldridge M, Jennings NR (1995) Intelligent agents: theory and practice. Knowl Eng Rev 10: 115–152