https://doi.org/10.6092/issn.1825-1927/17200 ISSN 1825-1927

Implications of Artificial Intelligence in the Field of Law
Crime Prevention Tool

Alba Maria Gallo*

Abstract: The advent of digital technologies has profoundly changed the logic of the system, generating a cultural revolution and also impacting on the inspiring principles of law. The investigation focuses on the use of AI as a crime prevention tool: the activities of law enforcement agencies are highlighted where predictive policing software is used, which by exploiting the wealth of information offered by innumerable quantities of data is able to provide useful outputs for crime prevention. The central issue is to identify the compatibility of these systems with the protection of the right to privacy and the protection of personal data.

Keywords: predictive policing; artificial intelligence; big data; data protection; privacy

1 Big data and profiling

The use of algorithms in crime prevention strategies, widely employed in the Anglo-Saxon system, is also gaining importance in the European landscape. Innovative software is being developed that can quickly provide the necessary outputs to prevent the commission of crimes by utilizing vast amounts of data[1]. The dangers posed by the exploitation of big data for privacy protection and personal data security are evident. It is therefore important to focus on the potential intrusions into the protection of the right to privacy and personal data that arise from the use of these systems. These systems, through the immense volume of data, their storage and aggregation across various databases, and profiling techniques, assist law enforcement agents. With the increase in available data, there is a need to effectively collect and store it to derive the maximum advantage and value from it (data performance). In particular, profiling is a technique that involves cross-referencing data from different sources using algorithms to prevent the commission of crimes and identify crime hotspots or develop individual criminal profiles[2], as will be discussed later.

Multiple data storages are crossed and retrieved from various sources such as law enforcement databases or acquired from data brokers, social networks, the internet, or closed-circuit systems.

For these reasons, precautions have been provided by Directive 2016/680 specifically regarding profiling: "automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to an individual, in particular... concerning professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[3]

*Università Giustino Fortunato; ✉ a.gallo2@unifortunato.eu

1. Agenzia per l'Italia Digitale March 2018 White Paper, *L'intelligenza artificiale al servizio del cittadino*, where it is explained that: "...while representing a mine of information, data need adequate tools to be exploited to their full potential. In particular, information retrieval and filtering models and methods based on semantic technologies and shared ontologies are needed'.

2. A. Babuta, 2017, *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities*, in Royal United Services Institute for Defence and Security Studies.

3. Directive (EU) 2016/680 of the European Parliament and of the Council, dated 27 April 2016, regarding the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of crime prevention, investigation, detection, and prosecution, as well as the enforcement of criminal sanctions, and the free movement of such data, repealing Council Framework Decision 2008/977/JHA, published in the Official Journal of the European Union (OJ L 119) on 4 May 2016, pages 89 onwards; Article 3, paragraph 4

It should be noted that Article 11 of the directive establishes the prohibition that decisions made by law enforcement authorities are based "solely on automated processing, including profiling, which produces legal effects or significantly affects the data subject." The directive also highlights the safeguards, including cat least the right to obtain human intervention on the part of the data controller."[4]

Profiling becomes illegitimate when it leads to "discrimination of individuals based on special categories of personal data." In fact, it could happen that the data inputted into the system is tainted with biases[5] concerning the individual's ethnicity or social background. In such cases, the algorithm, working through machine learning, may produce a biased outcome[6].

Profiling carries evidently dangerous risks, as the European Parliament believes that: «the risk of data being used for discriminatory or fraudulent purposes and the marginalisation of the role of humans in these processes, leading to flawed decision-making procedures that have a detrimental impact on the lives and opportunities of citizens, in particular marginalised groups, as well as bringing about a negative impact on societies and businesses».[7]

The European Parliament defines big data[8] in these terms: 'big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytics)'.[9] It was considered appropriate to quote verbatim to verify the anonymous nature of the same, referring, however, to Directive 2016/680, which precisely deals with the protection of personal data in law enforcement activities, aimed at the prevention, investigation and detection of crimes. It excludes the use of anonymous information, i.e. 'information that does not relate to an identified or identifiable natural person'[10] or which concerns 'personal data rendered sufficiently anonymous so that the data subject can no longer be identified'.[11]

In order to be able to identify a natural person, it is necessary that 'all means, [...], taking into account both the technologies available at the time of processing and technological developments, be taken into account'[12] .

In particular, Article 20 of the directive stipulates the use of appropriate organisational techniques, such as pseudonymisation, which aims at data protection and the adoption of all necessary measures to ensure that only useful personal data, in terms of quantity, scope of processing, storage period and accessibility, can be processed by default.

Pseudonymisation is the processing of personal data through which they 'can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organisational measures to ensure that personal data are not attributed to an identified or identifiable natural person'.[13] However, the article does not perfectly guarantee data protection and data anonymity; in fact, the danger also identified by the European Parliament remains: 're-identification of individuals by correlating different types of anonymised data', with effects underlined by the Special Rapporteur on the right to privacy, who to the question "do de-identification processes deliver data that do not interfere with individuals' information privacy rights?"[14], can only answer negatively.

The increasing attention that both the EU and international institutions pay to data protection is therefore well known, but there are restrictions on the right to privacy and the protection of personal data, which Directive 2016/608 itself, the GDPR[15] and the

4. Directive (EU) 2016/680, cited above, Art. 3(4).

5. C. Burchard. 2019.,*L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica dela società,* in Riv. it. dir. proc. pen., p. 1932 ff.

6. T.P. Woods.2017. The Implicit *Bias of Implicit Bias Theory,* in Drexel L.Rev., 10, p.631.

7. European Parliament, Report on fundamental rights implications of big data: privacy, data protection, nondiscrimination, security and law-enforcement, 2016/2225(INI), Committee on Civil Liberties, Justice and Home Affairs, 20 febbraio 2017, par. M.

8. G. Della Morte. 2018. *Big data e protezione internazionale dei diritti umani. Regole e conflitti,* Editoriale Scientifica.

9. European Parliament, Report on fundamental rights implications of big data, cit., para. A)

10. Directive (EU) 2016/680, cited above, para. 4

11. Directive (EU) 2016/680, cited above, para. 4

12. Directive (EU) 2016/680, cited above, para. 4

13. Directive (EU) 2016/680, cit, Art.3(5).

14. Report of the Special Rapporteur on the right to privacy, A/72/43103, 19 October 2017, para. 95.

15. Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data, in OJ L 119, 4 May 2016, 1 ff. ('GDPR').

European Convention on Human Rights ('ECHR') legitimise in order to safeguard public security[16].

Directive 2016/680 authorises Member States to use data where it is 'a necessary and proportionate measure in a democratic society with due regard for fundamental rights and legitimate interests of the natural person concerned so as: (a) not to jeopardise official or judicial enquiries, investigations or procedures; (b) not to jeopardise the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) to protect public security; (d) to protect national security; (e) to protect the rights and freedoms of others'.[17] The same approach is followed by the ECHR, in Article 8(2), which states that interference by public authorities with the right to privacy is unlawful unless it 'is provided for by law and constitutes a measure which, in a democratic society, is necessary for national security, public safety, the economic well-being of the country, for the defence of law and order and the prevention of criminal offences, for the protection of health or morals, or for the protection of the rights and freedoms of others'. Along the same lines is Article 23 of the GDPR, which legitimises the restriction of recognised rights as long as they respect 'the essence of fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society' to ensure public and national security and the prevention of crime.

The General Data Protection Regulation (GDPR), adopted by the European Union in 2016 and enforced in 2018, delves deeper into the issue of profiling and grants a set of rights and obligations to both businesses and individuals regarding the protection of personal data.

According to the GDPR, profiling encompasses any automated processing of personal data aimed at analyzing or predicting specific aspects regarding the preferences, interests, behaviors, location, or movements of an individual. This practice allows for automated decision-making that can significantly impact individuals, such as in the field of crime prevention.

We will therefore discuss the reasons why the GDPR is particularly significant for regulating AI, justifying the choice to use this source as a model for analysis. We will highlight some principles and rules that form the pillars of the GDPR, in order to evaluate the level of protection offered, the potential, and above all, the limitations of this discipline.

The GDPR establishes several fundamental principles concerning profiling and the privacy of personal data. These principles include:

1. Transparency: Businesses are required to provide clear and understandable information regarding profiling activities and the potential consequences for those involved.
2. Legal basis: The processing of personal data for profiling purposes must be based on one of the legal grounds provided by the GDPR, such as explicit consent from the individual, the performance of a contract, or compliance with a legal obligation.
3. Rights of the data subjects: Individuals have the right to be informed about profiling, to object to it, to request access to their data, and to request correction or deletion if the data is inaccurate or no longer necessary.
4. Security measures: Businesses must implement adequate measures to protect the personal data used in profiling from unauthorized access or potential loss.

These principles, as we will see later, do not always provide complete protection for individuals subject to predictive policing software. The GDPR also introduces the concept of "Data Protection Impact Assessment" (DPIA), which requires businesses to carefully assess the effects of profiling and adopt appropriate measures to ensure the security of personal data. It establishes specific rules and regulations to ensure that profiling and the processing of personal data are conducted transparently, lawfully, and securely, preserving the rights and privacy of individuals.

It can be argued that the right to privacy not only involves a personal interest but also a public interest, considering the implications on individual political decisions based on the collected, stored, and processed information about profiled individuals. In addition to individual profiling, the ease of database cloning unites individuals and organizations in the same type of activity. Both private

16. A. Terrasi. 2017. *Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo In M. Distefano* (ed.), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale.* Napoli : Editoriale Scientifica.

17. Directive 2016/680, cit., art.13.

and public entities, including government agencies, can be subjected to espionage, and their most confidential information can be used for various purposes.[18]

In this case, indeed, a complementary aspect of cybercrime is cyberwarfare, where actions are not carried out by individuals but by sovereign institutions.[19]

Although the focus of this document is on the protection of personal data, the inclusion of the GDPR in the proposed analysis is appropriate. In fact, from the discipline concerning personal data, relevant principles for data in general can be extracted, considering the "dynamic" perspective that accompanies the circulation and use of data.[20]

Furthermore, many of the data processed by AI decision-making mechanisms, which are relevant for this contribution, can be considered as personal data, making the GDPR a fundamental reference point for regulating such technologies. It is important to note that the very concept of "privacy" has undergone a long evolution and a kind of "reinvention," as it now provides a guarantee for the "protection of data."[21].

This concept needs to be distinguished from "privacy" itself and offers a broader control over information.[22]

However, the intrinsic limitations of the current discipline cannot be ignored, as it alone and in its formulation appears to be inadequate in fully addressing the violations of fundamental rights perpetrated by artificial intelligence systems. Therefore, throughout the discussion, other principles will be mentioned that attempt to fill some legislative gaps.

To highlight some general issues with the GDPR, it is important to consider how the exclusive reference to "personal data" poses a limitation. The distinction between personal and non-personal data, as well as between the public and private spheres, has become blurred with new technologies. It is unclear if the fundamental principles of the GDPR also apply to data and information derived from the processing of personal data through big data analysis, especially after they have been anonymized or transformed into group profiles[23].

European regulations protect personal data by clearly identifying the "data subject," whose information is subject to "processing." However, in the era of AI, data is constantly circulating and transforming, which means that any individual, at any moment, could potentially become subject to processing and therefore interested in the protection of their data. However, it becomes increasingly challenging to relate this to the protection provided by the GDPR[24].

Furthermore, European regulations ensure the protection of personal data by focusing on the concept of a well-defined "data subject," whose data is subject to "processing." However, in the era of AI, data is constantly circulating and transforming, which means that every individual can potentially become the subject of processing and therefore interested in the protection of their data. However, it becomes increasingly difficult to associate this with the protection guaranteed by the GDPR. Moreover, the GDPR is designed to protect the individual data subject but not the group, which is not recognized as the holder of the right to data protection[25].

As mentioned earlier, the analysis of big data and machine learning operates not only on individual data but also on aggregated clusters of data. Another critical aspect of the regulation is its limited applicability during the development phase of AI systems, specifically in the collection and use of data to "train" algorithms and generate the machine learning model. Additionally, under certain conditions, the regulation applies only when the system makes decisions about individuals during the processing phase. However, it does not apply to the intermediate and crucial data processing phase, such as within an artificial neural network, after

18. O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, Yale Law School FacultyScholarship Series, Paper 3852, 2012: http://digitalcommons.law.yale.edu/fss_papers/3852.

19. F. Romeo, 2017, Privacy digitale e governo della tecnica, I-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale Rivista quadrimestrale on-line: www.i-lex.it

20. C. Colapietro, A. Iannuzzi, I principi generali del trattamento dei dati personali e i diritti dell'interessato, in L. Califano, C. Colapietro (a cura di), Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679, Editoriale Scientifica, Napoli, 2017, 87.

21. P. De Hert, S. Gutwirth, Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action, in S. Gutwirth, Y. Poullet, P.D. Hert, J. Nouwt, C.D. Terwangne (a cura di), Reinventing data protection?, Springer, Berlino, 2009, 3 ss

22. S. Scagliarini, In tema di privacy: virtù e vizi della cultura giuridica, in Ars Interpretandi, 1, 2017, 49 ss.

23. I.S. Rubinsten, Big Data: The End of Privacy or a New Beginning?, in International Data Privacy Law, 3, 2, 2013, 78

24. F. Pizzetti, La protezione dei dati personali e le sfide dell'Intelligenza Artificiale, Giappichelli, Torino, 2018 , 40 ss.

25. L. Taylor, L. Floridi, B. Van Der Sloot (a cura di), Group Privacy: New Challenges of Data Technologies, Springer, Dordrecht, 2017.

the AI system has been built but before it makes decisions[26]. The GDPR partially addresses these aspects through the discipline of "profiling," which is defined as "any form of automated processing of personal data intended to evaluate certain personal aspects relating to an individual" for the purposes of analysis or prediction.

In light of all the principles mentioned above, the GDPR alone is not sufficient. Furthermore, the use of big data and reliance on algorithms can potentially result in violations of individual rights. However, leveraging these technologies does provide a significant advantage in terms of speed and resources, given the inherent impossibility for a human being to collect such an immense amount of data.

The use of predictive policing software, which is already operational in Italy, should therefore be conducted with 'greater algorithmic accountability and transparency'[27], precisely to highlight their unquestionable potential in the fight against crime[28]. In the next section, the functioning of predictive policing software will be examined, highlighting its advantages and criticalities.

2 Predictive policing software

Artificial intelligence presents itself as a powerful tool for preventing crimes from being committed. In fact, through the use of predictive policing software, it is possible to make predictions about the identification of suspicious locations (crime hotspots) or the elaboration of criminal profiles of persons at risk (predictive composites).

Depending on the method of operation and the software system used, there will be: placed based system[29] or person based system[30]. Such systems cross-reference different data of different origins, working out the profile of the perpetrator of certain crime categories, this is the exploitation of the technique of machine learning, which represents the core of artificial intelligence applied to software. It should be noted that the use of algorithms undoubtedly has an impact on reducing the crime rate, but there are also a number of critical points to be noted, but first we should dwell on the three main softwares adopted in Italy: KeyCrime in use at the Questura di Milano, X- Law adopted by the Questura di Napoli and Pelta Suite, currently being tested at the City of Caorle (VE).

The contribution aims to focus on a single software: the keyCrime.

The KeyCrime software has been used since 2008 in the municipality of Milan and, since 2009, in the entire province of Milan. It was created by the policeman Mario Venturi, who immediately noticed that some crimes were closely linked to others of the same kind, so that by processing the data and aggregating them together, it was possible to quickly solve the case, especially in the identification of serial perpetrators[31]. The software, once it has identified the common thread of a series of crimes (crime linking), aggregates the data, and hypothesises the place and time when the next crime will be committed. The basis of the system stems from the idea that certain types of crimes occur in a circumscribed geographical area and time frame[32], which makes it easier to identify the perpetrator and predict his future moves.

The efficiency of Keycrime has been extensively analysed and studied by a research conducted by Essex University, which found that the Keycrime sotfware, unlike other predictive policing devices, which work on a statistical basis, also identifies how and where a particular crime is committed. The aim of the software is to predict where the individual will strike. It is in fact used to identify the (serial) perpetrators of shop and bank robberies, noting that around 70 per cent of robberies can actually be traced

26. F. Pizzetti, La protezione dei dati personali e le sfide dell'Intelligenza Artificiale, cit., 42 ss.

27. European Parliament, Report on fundamental rights implications of big data: privacy, data protection, nondiscrimination, security and law-enforcement, cit. par. 8.

28. A. Bonfanti. 2018. *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in MediaLaws - Journal dir. media, 3

29. R. Brauneis, E.P. Goodman. 2018. *Algorithmic Transparency for the Smart City*, in Yale J.L. & Tech. ,20, p. 146 ff.

30. M. Oswald, J. Grace, S. Urmin, G. Barnes, " *Algorithmic Rick Assessment Policing Models: Lessons from the Durham HART Model and Experimental Proportionality",* in Info. & Comm. Tech. L., 3 April 2018, p. 223 ff.

31. M. Venturi, 2014, *KeyCrime©. Le chiavi del crimine*, in PrimoPiano, 12/2014, 4, available at www.onap-profiling.org.

32. K.J. Bowers, S.D. Johnson, 2004, *Who commits near repeats? A test of the boost explanation*, in Western Criminology Review.

back to serial conduct[33] . Keycrime provides output data, the system creates links between the various crimes, detecting among the available data the link that connects the chain, which can be attributed to the same perpetrator, and forecasts the next crime[34].

It should be specified, nonetheless, that the software, including Keycrime, belongs to private companies using industrial secrecy and is covered by intellectual property rights, so the individual authorities will not be able to find the source codes of the software.

The operation of the software is made possible thanks to the strategic issuing and acquisition of georeferenced predictive alerts, generated by the Machine Learning model, which precisely establish the time and place where an offence is most likely to occur[35] . Needless to point out that such software provides a considerable advantage in terms of time savings, as well as precise analysis accuracy, but the risks are also obvious, and it is precisely on this aspect that the agenda of future legislators should focus. In fact, there are several issues that need to be addressed. The first issue concerns the way in which the predictive policing software is set up and used, especially the risk of a sort of 'militarisation' of a given area, considered hot by the algorithm, to the detriment of other urban areas[36] : essentially, the system would intensify controls only in a given area, and would continually record crimes, even of a different nature, leading to an increase in the crime rate in that controlled area. What is more, dwelling on the concept of safeguarding the fundamental rights of the individual, concerns surface, as already analysed in the previous paragraph, regarding the danger that analysing and managing such an infinite amount of data would generate a sort of generalised surveillance that is difficult to reconcile with the protection of privacy, a protection that is further strengthened by the provision of the European matrix prohibition, also transposed by our legal system,[37] concerning decisions based exclusively on automated processing, including profiling, which would certainly lead to negative consequences for the person concerned.

For these reasons, the European Parliament on 6 October 2021 called for a moratorium on all Member States regarding the use of any kind of activities involving forms of mass surveillance[38] .

Software could also return, due to biased data fed into the system, biased outcomes (so called Critical garbage in, garbage out, or even bias in, bias out), in which case it would be very complex to trace the logical path taken by the algorithm, which is based on the software's capacity for self-learning. Furthermore, the systems, as has already been widely mentioned above, belong to private companies and even imagining their collaborative attitude, the programmers would find themselves in a black box, unable to trace the algorithm's systemic process.

Connected to the intrinsic problem of the algorithm, there is also a question of accountability, as it could happen that the tool returns an incorrect prediction evaluating an area or a subject at risk, thus generating false positives or false negatives[39].

The issue of discrimination caused by algorithms is undoubtedly one of the prominent themes raised by the technological evolution of our society[40].

Discrimination perpetrated through machines has generated significant interest and has prompted extensive analysis and reflections in various legal disciplines, such as labor law, constitutional law, criminal law, and even philosophy of law[41]. We are witnessing the emergence of a new regulatory landscape, where "ordinary" regulatory activities are transposed into the technological realm. This involves the identification of subjects and behaviors typical of a specific situation, the enforcement of mandates, and the promotion of law-compliant behaviors through targeted warnings or suggestions, as seen in the concept of "nudge."[42] Given its inherently technological nature, algorithmic discrimination cannot be excluded from this context.

33. G. Mastrobuoni, 2020, *Crime is Terribly Revealing: Information Technology and Police Productivity*, in The Review of Economic Studies, vol. 87.p. 2732.

34. R. Pelliccia, 2019. *Polizia predittiva: il futuro della prevenzione criminale?,* in www.cyberlaws.it

35. Information available at www.pelta.it

36. F.Basile. 29 September 2019. *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in Dir. pen. uomo, p.13

37. As already analysed in the previous paragraph: Article 22 of the Gdpr and Article 11 of EU Directive 2016/680, as well as Article 8 of Legislative Decree No. 51 of 18 May 2018, which transposed the prohibition into domestic law, implementing the Directive.

38. Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) , 21/04/2021

39. P. Severino, 2022*, Intelligenza artificiale: Politica, economia, diritto, tecnologia*., Luiss University Press, p. 93.

40. C. O'Neil, 2016, Weapons of math destruction: How big data increases inequality and threatens democracy, Portland, Broadway Books.

41. P. Dunn, 2022, Moderazione automatizzata e discriminazione algoritmica: il caso dell'hate speech, in Rivista italiana di informatica e diritto, 4 (1), p. 12.

42. R.H. Thaler, C.R. Sunstein, 2009, Nudge: Improving decisions about health, wealth, and happiness, New York, Penguin.

The applicability of privacy legislation to predictive policing tools, both place-based and person-based systems, is a complex and debated issue. Predictive policing systems, as we have seen, use algorithms and data analysis to identify potential criminal activities or high-risk areas. However, the use of such tools can raise concerns about privacy and discrimination, as discussed earlier.

Regarding the applicability of privacy legislation, laws and regulations on personal data protection, such as the GDPR in the European Union, generally apply to the data used in predictive policing systems. This is because these systems often require the collection and processing of personal data, such as demographic, criminal, or location information.

However, the issue becomes more complex when considering specific aspects of using sensitive data and balancing public security with privacy protection. It is necessary to carefully evaluate the application of principles such as consent, purpose, and proportionality in the context of using predictive policing tools.

Furthermore, the applicability of privacy legislation may vary at the national and regional levels, as each jurisdiction may have specific rules on data protection and the use of intelligence and security tools.

The question of the applicability of privacy legislation to predictive policing tools requires a thorough analysis of local laws and regulations, as well as the ethical implications and fundamental rights involved. It is important to balance the effectiveness of public security measures with respect for privacy and the protection of individual rights. When applying privacy legislation to predictive policing tools, various factors need to be considered, such as the nature of the data collected, the purposes of processing, the legal basis for processing, and the rights of individuals involved. Additionally, regulatory authorities and courts can play a key role in interpreting and applying privacy laws in relation to predictive policing tools.

Moreover, one has to reckon with the large legal vacuum, so how can these findings be admitted in criminal proceedings? And it is precisely on this question that the legislator's attention must focus, as there is a complete lack of regulatory guidance on the legitimate use of predictive policing.

3 Conclusions

The road to complete regulation of predictive policing is certainly still tortuous, but both international bodies and the European Union are aware that the growing dependence on data poses major dangers to fairness and justice, precisely in the absence of careful monitoring underlying the creation, review and maintenance of the data themselves. Indeed, both Big Data, and consequently predictive analytics, are an advantageous tool for crime suppression, but the right balance between effective law enforcement (and crime prevention) and the rights of the individual must be struck.

It would be desirable for predictive policing activities to be conducted with 'greater algorithmic accountability and transparency'[43], i.e. through the provision of technical and methodological measures to ensure the transparency of data, avoiding the occurrence of negative consequences in terms of discrimination and violation of the right to privacy and the presumption of innocence, findings that could arise from automated decisions on individual behaviour.

Through the respect of such guarantees, the incompatibility between the use of software and the protection of fundamental rights could be rebalanced, regularising the use by law enforcement agencies of algorithms that unquestionably promise great potential in the fight against crime, as well as the maintenance of public safety.

This is a crucial issue in the contemporary scientific debate, which poses complex questions that are difficult to resolve. For this reason, a number of initiatives are worth mentioning, oriented towards the promotion of cooperation and the exchange of best practices, always paying the utmost attention to respect for human rights. In particular, the study 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights'[44] commissioned by the European Parliament highlighted how the current European legislation on data protection does not meet the need to protect the individual and therefore explicitly calls for the intervention of the legislator 'to guarantee EU fundamental rights in the field of law enforcement and criminal justice'[45]. .

43. European Parliament, Report on fundamental rights implications of big data: privacy, data protection, nondiscrimination, security and law-enforcement, cit. par. 8.

44. The findings of the study were published on 15 July 2020: https://europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)656295

45. https://europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)656295

Despite the initiatives that have been put in place, there is currently no legislation regulating artificial intelligence in a reasonably precise and punctual manner. Certainly, the phenomenon is running so fast in the perception of the legislator, it is transforming and amplifying itself to such an extent that it cannot even be defined in a shared manner, considering then the already examined profiles of incompatibility of predictive policing techniques with the protection of privacy and personal data.

Therefore, it is necessary to establish an international technical forum for dialogue where concerns regarding compatibility issues can find a point of connection with the objective potential of using software that leverages big data for crime suppression. In this forum, the jurist must embrace the extraordinary role of a designer, as echoed by Kevin Kelly[46] in an interview from a few years ago. Kelly emphasized that the challenge to counter the potential dystopian impact of machines lies not in envisioning utopias but in creating prototypes.

This international technical forum would serve as a platform for experts, policymakers, and stakeholders to come together and discuss the complex issues surrounding the use of software powered by big data for crime prevention. It would provide a space for addressing concerns related to compatibility while exploring the potential benefits offered by these software solutions.

By fostering open and constructive dialogue, this forum can help bridge the gap between concerns and possibilities, facilitating the development of innovative approaches that leverage the power of technology while considering privacy, ethical considerations, and fundamental rights. The jurist, in their extraordinary role as a designer, can contribute audaciously to this process. Together, through the creation of prototypes and practical solutions, we can address the challenges posed by emerging technologies and strive for a more balanced and responsible use of software in combating crime

Bibliography

Babuta A., Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities, in Royal United Services Institute for Defence and Security Studies, 2017.

Basile F., Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, in Dir. pen. uomo, 29 settembre 2019, p.13

Bonfanti A.,Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali, in MediaLaws – Rivista dir. Media 3, 2018.

Brauneis R., Goodman E.P., Algorithmic Transparency for the Smart City, in Yale J.L. & Tech. ,20, 2018 p. 146.

Bowers K.J., Johnson S.D., Who commits near repeats? A test of the boost explanation, in Western Criminology Review, 2004.

Burchard C., L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società, in Riv. it. dir. proc. pen., 2019, p. 1932.

Colapietro C., Iannuzzi A., I principi generali del trattamento dei dati personali e i diritti dell'interessato, in L. Califano, C. Colapietro (a cura di), Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679, Editoriale Scientifica, Napoli, 2017, 87.

De Hert P., Gutwirth S., Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action, in S. Gutwirth, Y. Poullet, P.D. Hert, J. Nouwt, C.D. Terwangne (a cura di), Reinventing data protection?, Springer, Berlino, 2009, 3 ss

Della Morte G., Big data e protezione internazionale dei diritti umani. Regole e conflitti, Editoriale Scientifica, 2018.

Dunn P., Moderazione automatizzata e discriminazione algoritmica: il caso dell'hate speech, in Rivista italiana di informatica e diritto, 4 (1), 2022, p. 12.

Hathaway O.A., Crootof R., Levitz P.. Nix H., Nowlan A., Perdue W., Spiegel J., Yale Law School FacultyScholarship Series, Paper 3852, 2012

Matrobuoni G., Crime is Terribly Revealing: Information Technology and Police Productivity, in The Review of Economic Studies, vol. 87, 2020, p. 2732.

46. Il testo integrale dell'intervista è disponibile al link https://bit.ly/3Lrn72W.

Pelliccia R., Polizia predittiva: il futuro della prevenzione criminale?, 2019, in www.cyberlaws.it.

Pizzetti F., La protezione dei dati personali e le sfide dell'Intelligenza Artificiale, Giappichelli, Torino, 2018 , 40 ss.

Romeo F., 2017, Privacy digitale e governo della tecnica, I-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale Rivista quadrimestrale, in www.i-lex.it

Rubinsten I.S. , Big Data: The End of Privacy or a New Beginning?, in International Data Privacy Law, 3, 2, 2013, 78

Oswald M., Grace J.,Urmin S., Barnes G., " Algorithmic Rick Assessment Policing Models: Lessons from the Durham HART Model and Experimental Proportionality", in Info. & Comm. Tech. L., 3 Aprile 2018, p. 223.

Scagliarini S., In tema di privacy: virtù e vizi della cultura giuridica, in Ars Interpretandi, 1, 2017, 49 ss.

Severino P., Intelligenza artificiale. Politica, economia, diritto, tecnologia, Luiss University Press, 2022, p. 92.

L. Taylor, L. Floridi, B. Van Der Sloot (a cura di), Group Privacy: New Challenges of Data Technologies, Springer, Dordrecht, 2017.

Terrasi A., Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo. In M. Distefano (a cura di), La protezione dei dati personali ed informatici nell'era della sorveglianza globale, Napoli: Editoriale Scientifica, 2017.

Thaler R.H. , Sunstein C.R. , Nudge: Improving decisions about health, wealth, and happiness, New York, Penguin, 2009.

Venturi M., KeyCrime©. La chiave del crimine, in PrimoPiano, 12/2014, 4, www.onap-profiling.org.