ANGELO GIRALDI[*]

ALGORITHMS AND BIG DATA TOWARDS A CRIME-PREVENTING GROUPWARE[**]

ABSTRACT. *The scientific and technological progress has bumped into Criminal Law in terms of artificial intelligence systems and predictive policing software. The different crime prevention strategies and its innovative methods may struggle with the legal limits set up by the law. This paper aims at analysing the usefulness of artificial intelligence in Criminal Law, with particular regard to the investigations carried out by the authorities, and at urging the legislator to regulate the matter within the living juridical boundaries.*

[*] Ph.D. Candidate in Criminal Law and Teaching Assistant, Roma Tre University. Researcher and Lecturer of Criminal Law, University of Murcia (Spain).

[**] The paper is the result of the research work carried out by the author within the project "*Intelligenza artificiale e giustizia penale*", funded by the European Parliament and directed by Prof. Antonella Massaro.

1. Criminal Investigations Grapple with Artificial Intelligence

One of the most useful and productive advantages of artificial intelligence undoubtedly regards the first stage of criminal proceedings, which is made of the investigation activities. The investigative stage, in fact, is the fulcrum of criminal justice: on one hand, the activity of predictive investigation is functional for the security of the individual and the community, in its intent to effectively identify planned crimes or, in any case, future ones; on the other hand, the operations of the authorities entrusted with the *post-factum* investigation are functional to trace the conduct back to its author and possibly the criminal organisation behind him or her.

The scientific and technological progress that is sweeping across today's society is also the harbinger of innovation in the predictive and investigative sector, which characterises the first stage of the criminal proceedings.[1] Under this perspective, the idea that decisions, both pre-trial and in Court, should be based on the maximum rigour possible is gaining more ground.

From this particular point of view, a brief acknowledgement of the heuristic methodologies dominating the thought of the judicial operator can be useful: this person, grappling with the different forms of crime, must carry out the investigation, be he or she a police officer or a public minister, in the exercise of his or her function.

In the search of the facts and the truth, as well as of the various sources of investigation, the tasked person uses a methodology that is undoubtedly imbued with subjective characteristics which, almost unanimously, are defined as risky.

Since the dawn of social and philosophical thought, the myth of justice remains anchored to both the criteria of impartiality and objectivity which, in practice, encounter grey areas where the objectivity is pervaded by outside influences. One cannot omit to

[1] For an in-depth examination of artificial intelligence as the ultimate purpose of Criminal Law, see C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in «Rivista italiana di diritto e procedura penale», n. 4, 2019, p. 1908 et seq.: «gli algoritmi intelligenti sono in grado attraverso la tecnologia di affrontare, a vantaggio di tutti, problemi quotidiani che, tuttavia, vanno oltre le capacità umane; e certamente meglio, più velocemente e in modo più economico rispetto ai decisori umani». See also V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, edited by U. Ruffolo, Giuffrè, Milan 2020, p. 547 et seq.

say that the same legal heuristics, as a social science, has been practised so far by physical people, whose reasoning is also irrationally determined by personal psychological factors that have nothing to do with the committed or to-be-committed crime.

An interesting study dates back several years.[2] Eight Israeli judges were examined over a period of ten months, for a total number of fifty daily sessions. The individual judge, in those occasions, was asked to decide on requests for conditional release put forward by convicts in different prisons. The days were divided into three moments: firstly, the early hours of the morning, in which the judge started his or her work; secondly, the second part of the morning, which started after a break; finally, the rest of the working day after lunch.

The intention was to relate the judicial decisions with the times that they were adopted, in an attempt to understand how much of those decisions could be attributed not just to the discretionary interpretation of the magistrate – always anchored to the canons of the law – but, rather, to his or her psychological situation, completely independent of the legal cases.

The result that the study reached was evident as it emerged, clearly and eloquently, that the percentage of petitions for conditional release approved at the start of every time frame in the day was by far greater than those dealt with once half of the time span in question had passed. In fact, if the favour towards conditional release was granted in around 65% of the petitions dealt with in the early hours of the morning, it tended to zero as time went by, until the magistrate's refreshment. Once the next time frame started, there were no changes and the percentages, initially high, of granting the benefit dropped drastically as time went by.

Essentially, it clearly emerged from the study that tiredness, fatigue, the need for sustenance and the tedium of the judicial authority were risk factors. In fact, the convicts' chances varied considerably according to the psychological/physical status of the decision-maker.

[2] The study is briefly reported in the introduction to a contribution on the reasoning of judges made by science logicians and philosophers. The original study is however to be attributed to Danziger, Levav and Avnaim-Pesso (2011) and was published on PNAS (the prestigious Review of the American National Academy of Science). Significant critical comments on the details of the study, especially on its interpretation, can be found in G. Cevolani, V. Crupi, *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive*, in «Criminalia», 2017, p. 181 et seq.

The above-mentioned study, although emblematic, is only a part of the numerous studies on human reasoning, which, obviously, can also be applied to a court sitting. Reasoning and human logic are analysed by a growing number of scholars, the data for which are not in the least comforting. The mental characteristics of the individuals reveal that the basic mechanisms of our cognitive and decision-making activities (also with regard to the most banal daily activities) constantly deviate from what is prescribed, abstractly, by the so-called theories of correct reasoning.

This cannot necessarily be attributed to mixed factors of human nature. Circumstances completely extraneous to the person, which cannot be predicted by him or her, can also influence the final decision in one way or another.

This is the case, for example, with *anchoring*, which was experimented on a group of German jurists with judicial experience.[3] The former magistrates were proposed a case of theft, the fruit of the authors' imagination, on which they had to make a judgement. The people participating in the study were divided into two groups, each of which received an accurate description of the case together with two loaded (unbeknown to them) dice.

Each of the groups were asked to throw the dice to get, by adding up the results, the number corresponding to the months of conviction requested by the prosecution. In the first group, the throw of the dice was programmed so that a result of three months was obtained (*low anchor*), corresponding to a relatively restrained request for conviction by the prosecution. Instead, in the second group the figure obtained was greater and added up to nine months (*high anchor*).

The result of the study, though significant and satisfying from a scientific point of view, was rather disappointing in light of the law. The first group, which was supplied with a low anchor, completely unpredictable from the participants' point of view, opted to convict the defendant to five months of imprisonment. The second group, on the other hand, having received a high anchor, set the penalty at eight months. As shown by the analysis carried out, the anchoring effect played a fundamental role in the

[3] B. Englich, T. Mussweiler, F. Strack, *Playing Dice With Criminal Sentences: The Influence of Irrelevant Anchors on Experts' Judicial Decision Making*, in «Personality and Social Psychology Bulletin», n. 32, 2006, p. 194.

decision-making process of the involved judges. The fact that all the people in the first group had calibrated the sentence for an amount considerably lower than the participants in the second group could not be attributed to a purely causal mechanism.

It would seem that the external influence on the decision-makers may be attributed to the reliability which the prosecution often generates on the judge, because the result of the throwing of the dice was considered as a proposal for conviction by the Public Prosecutor. Yet, the participants – people with an education level above the average, and already invested with jurisdictional powers – were fully aware that the prosecution was represented by an inanimate object totally incapable of thinking and providing rational proposals. In this sense, the fact that the participating jurists trusted (so-called anchoring) an external, inanimate and completely random element is astounding: the judgement of the professionals in question was broadly conditioned by numbers that were apparently alien to matters.

In the wake of these exemplary experiences, artificial intelligence intervenes to mitigate the subjective influences of the individuals who operate in the world of justice, in an attempt to remove, as objectively as possible, the biases that pervade criminal proceedings.[4]

2. The "Artificial" Attempt to Unveil "Unknown Values"

The idea that decisions, because they potentially refer to every individual, must be based on a rigorous analysis of data through scientifically recognised methods has already taken hold in the current doctrine.[5] Thus, data processing, appropriately collected and analysed, is reaching almost uncontrollable quantitative levels. At the base

[4] On the problem of prejudices (biases), see *amplius* O. Di Giovine, *Il* judge-bot *e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in «Cassazione penale», n. 3, 2020, p. 951 et seq.

[5] The theme of data analysis and its use in scientific terms is very topical in the contemporary and international doctrinal debate. See *ex plurimis*, N. Hart, M. Yohannes, *Evidence Works: Cases Where Evidence Meaningfully Informed Policy*, in «Bipartisan Policy Center», 2019, available at: <https://bipartisanpolicy.org/report/evidenceworks> (accessed on 02.11.2021).

of the artificial intelligence programs, including predictive and investigative software, lie big data, characterised in the first place by their huge quantity.[6] It is not by chance that the algorithms on which said computerised applications of mathematics and statistics are more efficient the more data they possess.

The final aim of the algorithm is to discover an initially unknown value, to be reached through the analysis and systematisation of a large set of individual data.[7] In order to better understand the purpose of using this (originally) mathematical method, we must question the concept of the "unknown value" that we are looking for through examining the data available to the operators.

Firstly, the value referring to an event that has already happened can be defined as unknown, because there is (and it could not be otherwise) always an element that the interpreter is not capable of knowing with sufficient certainty. At first sight, one could exclude from the category of past events those for which an audio-visual recording is available, as it is capable of providing the interpreter with the possibility, *ex post*, of entering virtually into the spatiotemporal context of the fact. Yet, even in this case, there would be elements that cannot be known, since human action, though faithfully reproduced with *ad hoc* digital tools, hides a series of indeterminate psychological processes which currently elude every type of recording or understanding by third parties that can be said to be absolutely beyond doubt. Secondly, and for obvious reasons, every type of present and, *a fortiori*, future event falls into the category of unknown values.

On the basis of the observations made, it is appropriate to analyse the term "predictive" in more detail. It is often used as an attribute referring to software and policing algorithms, meant in the broad sense as increasingly effective tools for predicting and preventing crime.

In fact, if one of the aims of artificial intelligence is to find "unknown values" referring to future and chance events (hence the term "predictive"), one cannot overlook

[6] For an in-depth examination of big data and the interference with Criminal Law, see C. Momsen, C. Rennert, *Big Data-Based Predictive Policing and the Changing Nature of Criminal Justice. Consequences of the extended Use of Big Data, Algorithms and AI in the Area of Criminal Law Enforcement*, in «Kriminalpolitische Zeitschrift», n. 5, 2021.

[7] F. Provost, T. Fawcett, *Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking*, O'Reilly Media, Sebastopol 2013.

the relationship between the new technological tools and facts belonging to the past and present. In this perspective, predictive policing algorithms – and the related software – must not solely mean the methods exploited to estimate the probability of future crimes, but also those adopted to aggregate the useful data to bring clarity on crimes that have already been committed and on the permanent offences perpetrated in the present.[8]

Thus, the term predictive must be considered in its double meaning of prediction and investigation. In the first case, predictive policing will be aimed at anticipating future crimes; in the second, it will act as the main character in the search for the author of the crime or, in broader terms, the attribution of the latter to a superordinate organisation. It should be noted that the two proposed meanings are strictly interconnected: the investigative activity and the characteristics of the facts and authors flow into the data used for predicting future crimes; conversely, the successful outcome of the strictly predictive activity greatly facilitates any subsequent investigation operation.

The true usefulness of predictive policing lies in the discovery of similarities and analogies from the analysis of variables that are constantly related to each other. In this sense, the change of pace is remarkable compared to the "traditional" tools tied to "natural" intelligence, which have been applied right up to contemporary times.[9] The margin for reducing crime is expanded with the new heuristic methodologies tied to the science of probability and the development of technology. This is mainly due to the fact that the resources, though limited, and the data held by the authorities are exploited in an optimised manner as compared to the past. In fact, on one hand, a similar use of resources allows, *mutatis mutandis*, an investigative "Pareto efficiency" to be achieved; on the other hand, it allows the Criminal Police to organise more efficient operating strategies and decision-making.

[8] The Organization for Security and Co-operation in Europe bears witness to this in its report *OSCE Guidebook. Intelligence-Led Policing*, available in several languages at: <https://www.osce.org/es/chairmanship/455536> (accessed on 02.11.2021).

[9] See *amplius*, G. Tuzet, *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in «MediaLaws», 2019.

After all, it is not by chance that important studies in the field of environmental psychology have shown some uniformity and regularity in delinquency; in fact, it seems that criminals tend to act in known places, without travelling afar and in determined or determinable times or places.[10]

3. Algorithms and Big Data: A Testbed for Defining AI

An indispensable condition for drawing up effective strategies and reliable predictions is the availability of data.[11] At the same time, this condition is one of the most significant limits of artificial intelligence that exists today. The big data held by the authorities are nothing but resources produced by the authority itself: a vicious circle is thus set up, given the (possible) partiality of the information and data found by those to whom such data will return in an artificially aggregated and analysed form.

Nevertheless, although this allows considerable criticism to be advanced against artificial intelligence, it is difficult to imagine an artifice that operates otherwise. The only (im)practicable way would be to aggregate both sets of data coming from, firstly, the empirical comparison carried out in the local reality and, then, from the results of an ideal "perfect" society. It is difficult to even imagine a complete study that describes, in terms of absolute precision, the perfect social system; even if it was theorised, it would perhaps be unreliable.

In any case, as it is possible to solely use data regarding real society, a fruitful collaboration between the different professionals operating in social sciences becomes

[10] On this point, see S. Vezzadini, *Profilo geografico e crime mapping. Il contributo della criminologia ambientale allo studio del delitto*, in *Scena del crimine e profili investigativi. Quale tutela per le vittime?*, edited by R. Bisi, Franco Angeli, Milan 2006; P.J. Brantingham, P.L. Brantingham, *Environmental Criminology: from Theory to Urban Planning Practice*, in «Studies on Crime and Crime Prevention», n. 7, 1998; J. Eck, S. Chainey, J. Cameron, M. Leitner, R. Wilson, *Mapping Crime: Understanding Hot Spots*, in «National Institute of Justice», 2005, available at: <https://nij.ojp.gov/library/publications/mapping-crime-understanding-hot-spots> (accessed 02.11.2021).

[11] Data is the fulcrum on which artificial intelligence turns. Obviously, the data must firstly be captured using the so-called sensors. They could be cameras, microphones, a keyboard, an Internet site or other data entry systems, as well as sensors of physical quantities (*e.g.*, temperature, pressure, distance or force/torque sensors or tactile sensors). See F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi d'indagine*, in «Diritto Penale e Uomo», 2019, p. 6.

necessary (and favourable).[12] The world of justice is of course the first to be involved: the investigations of the Criminal Police, just like the already filed cases, are collectors of an inestimable amount of data that can be validly used. Nevertheless, other important parameter sectors, which can bring a volume of qualitatively and quantitatively different data, must not be undervalued.

Think, for example, of the world of health in its broad sense, which also includes the multiform area of the social services. These are the sectors which, also thanks to the implementation of information technology, deal on a daily basis with information regarding criminal or socially dangerous people. In some ways, the health world data can be a *quid pluris* compared to the information collected by the Criminal Police, for different sets of reasons. Firstly, at a quantitative level, entry into a further branch of social activities inevitably allows the exponential increase of data. Secondly, the type of information collected, *e.g.*, from the social service, is by far different and certainly complementary to what was found by the Criminal Police.

Given that there are data – or rather, big data – at the basis of the whole artificial intelligence process, it is maybe appropriate to wonder about the very concept of "intelligence," which is often put to the test by the methodology applied.

In this regard, the authoritative definition of artificial intelligence provided by the independent group of high-level experts appointed by the European Commission for carrying out the consultative function must be remembered.[13] For the EU experts, «artificial intelligence (AI) systems are software (and possibly also hardware[14]) systems

[12] This hope is shared by J.H. Ratcliffe, *Intelligence-Led Policing*, Routledge, Oxfordshire 2016.

[13] Information on the expert group appointed by the European Commission can be found on the institutional website, at: <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence> (accessed 02.11.2021).

[14] The systems based on artificial intelligence can be considered both software and hardware. More specifically, vocal assistants, programs for the analysis of images, search engines and biometric recognition systems are well-known examples of software. On the other hand, the implementation of such programs in peripherals that act outside the digital world makes it that artificial intelligence is also present in hardware. Think, for example, of driverless cars, drones, robots and the various applications of the *Internet of Things*. In this regard, see *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe*, 2018, 2, available in the full version at: <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe> (accessed 02.11.2021).

designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).»

Without prejudice to the definition proposed, it is appropriate to make the following clarifications.[15] Firstly, artificial intelligence, because it was created by human beings, does not fully correspond to the "naturalness" of the latter's reasoning. Secondly, and not for importance, the expression "artificial intelligence" is far from the operation of the human mind, whose "intelligence" remains to this day an undetermined concept. It seems that very little connects today's work in the AI field to the mysterious mechanisms of the human mind. At least at this stage, we are dealing with an engineering discipline with relations with biological organisms that are more metaphorical and "inspirational" than anything else.[16] For this reason, one often prefers to replace the expression "intelligence" with "rationality," where rationality means the capacity to choose the best action in order to achieve a certain objective in light of some criteria for the optimisation of the available resources.[17]

[15] The clarification that follows has been advanced by authoritative doctrine. See Basile, *Intelligenza artificiale e diritto penale*, cit., p. 5; C. Trevisi, *La regolamentazione in materia di Intelligenza artificiale*, *robot, automazione: a che punto siamo*, in «MediaLaws», 2018, p. 1 et seq.

[16] J. Kaplan, *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, Rome 2018, p. 81 et seq.

[17] Basile, *Intelligenza artificiale e diritto penale*, cit., p. 5.

4. Innovative Crime Prevention Strategies

If we examine the dynamics of predictive policing in more detail, in the already-mentioned double meaning of prediction and investigation, we can analyse the different strategies for preventing crime and the functional tools for analysing the facts of an already committed crime or one that is in progress.

Based on the models drawn up at a theoretical level, it would be possible to predict when, where and how the crimes will be committed, so that an attempt can be made to anticipate the causal mechanism of the crime.[18] The ultimate aim of the predictive policing method is a concatenation of elements that, together, make the investigation stage more efficient. The increase in resources to safeguard public safety in the areas at greatest risk allows us to identify the areas where the criminal risk factors are concentrated and, consequently, channel the intervention of the police force in order to conduct targeted operations.

It is possible to distinguish the continuous interaction between the following elements: data collection, analysis, police operations and criminal response. It is complex to imagine the operational efficiency of predictive policing without one of the mentioned components.

Data collection, suitably aggregated (fusion), is functional for their analysis. The latter is prefixed with the objective of preventing future crime, which inevitably guides the police operations. As a consequence of these interventions, the criminals react in a diverse manner, resulting overall in two fronts: on one hand, the reactions of the people in question solicit the requirement for new assessment and consequently new operating actions; on the other, they create an altered environment. In the latter case, the circle is closed because the new information found on the so-called altered environment [*i.e.*, the data on the criminal (re)actions] return to be collected and aggregated.

The use of similar predictive models, therefore, allows police force to organise the resources they have so that they can repress, thwart and, if possible, anticipate

[18] See A. Di Nicola, G. Espa, S. Bressan, M.M. Dickson, A. Nicolamarino, *Metodi statistici per la predizione della criminalità. Rassegna della letteratura su predictive policing e moduli di data mining*, in «eCrime Working Papers», n. 2, 2014, p. 5 et seq.

criminal conducts.

The interventions carried out by the police force achieve a fairly high specificity and concreteness rate and finish up by being remarkably targeted. The crime in certain areas could therefore be considerably reduced, which would allow us to assess the operation of artificial intelligence positively.

The current state of the art seems to allow the classification of the predictive policing strategies into four macro-categories.[19]

[19] *Ivi*, p. 6.

4.1 Methods for Predicting Crime

A first subset of predictive policing is represented by the methods for predicting crime (see *Table 1*). All the types of strategy aimed at predicting the place and time a crime will most likely be committed can be attributed to it. It seems that this category has been widely experimented with, particularly in the Anglo-Saxon countries, where the final objective ends up by coinciding, in a certain sense, with general prevention. In fact, as we will see, these operating models, which benefit from the collection and processing of large quantities of data usually from previously committed crimes, are prefixed with the purpose of anticipating (*i.e.*, preventing) the criminal event. On the other hand, different methods aspire to anticipate, and even prevent, its repeat or the repeat of a different crime by certain individuals.

Problem	**Conventional Crime Analysis (low to moderate data demand and complexity)**	**Predictive Analytics (large data demand and high complexity)**
Identify areas at increased risk		
Using historical crime data	Crime mapping (hot spot identification)	Advanced hot spot identification models; risk terrain analysis
Using a range of additional data (e.g., 911 calls, economics)	Basic regression models created in a spreadsheet program	Regression, classification, and clustering models
Accounting for increased risk from a recent crime	Assumption of increased risk in areas immediately surrounding a recent crime	Near-repeat modeling
Determine when areas will be most at risk of crime	Graphing/mapping the frequency of crimes in a given area by time/date (or specific events)	Spatiotemporal analysis methods
Identify geographic features that increase the risk of crime	Finding locations with the greatest frequency of crime incidents and drawing inferences	Risk terrain analysis

Table 1 – Methods for predicting crime. Source: *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, in *RAND. Safety and Justice Program*, 2013, p. 10.

4.2 Methods for Predicting the Future Offender

The second category of the predictive methods consists of the methods for predicting the future offender (see *Table 2*). Groups of individuals most exposed to the risk of delinquency are identified through the strategies under analysis. However, in order to do this, it is necessary to collect, analyse and aggregate the data coming from the already committed crimes, though combined with the data concerning each offender. One of the main objectives of the methods falling under this category is the reduction of recidivism. Although theoretically there is not an exact correspondence between committing a crime and its reiteration (in the more or less distant future), in practice a high percentage of specific reoffending has been found.

Problem	**Conventional Crime Analysis (low to moderate data demand and complexity)**	**Predictive Analytics (large data demand and high complexity)**
Find a high risk of a violent outbreak between criminal groups	Manual review of incoming gang/criminal intelligence reports	Near-repeat modeling (on recent intergroup violence)
Identify individuals who may become offenders:	Clinical tools that summarize known risk factors	Regression and classification models using the risk factors
probationers and parolees at greatest risk of reoffending		
domestic violence cases with a high risk of injury or death		
dental health patients at greatest risk of future criminal behavior or violence		

Table 2 – Methods for predicting the future offender. Source: *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, in *RAND. Safety and Justice Program*, 2013, p. 10.

4.3 Methods for Drawing Up a Criminal Identikit

The third category includes the methods for drawing up a criminal identikit (see *Table 3*). In a certain sense, these models come under the nuance of the term "predictive" which concerns the merely investigative stage for already committed crimes. The objective of this type of strategies is the processing of data for suspects using a multi-level database. These databases contain an indefinite plurality of information that is completely diverse (biometric data, records for the ownership of assets, tax information, etc.), whose aggregation, by using delegated algorithms if necessary, provides the operators with brilliant leads during the investigations.

Problem	**Conventional Crime Analysis (low to moderate data demand and complexity)**	**Predictive Analytics (large data demand and high complexity)**
Identify suspects using a victim's criminal history or other partial data (e.g., plate number)	Manually reviewing criminal intelligence reports and drawing inferences	Computer-assisted queries and analysis of intelligence and other databases
Determine which crimes are part of a series (i.e., most likely committed by the same perpetrator)	Crime linking (use a table to compare the attributes of crimes known to be in a series with other crimes)	Statistical modeling to perform crime linking
Find a perpetrator's most likely anchor point	Locating areas both near and between crimes in a series	Geographic profiling tools (to statistically infer most likely points)
Find suspects using sensor information around a crime scene (GPS tracking, license plate reader)	Manual requests and review of sensor data	Computer-assisted queries and analysis of sensor databases

Table 3 – Methods for predicting the future offender. Source: *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, in *RAND. Safety and Justice Program*, 2013, p. 11.

4.4 Methods for Predicting the Future Victim

Finally, the last category is an interesting "synthesis" of the methods expounded so far (see *Table 4*). In fact, the methods for predicting the future victim use the tools in the previous categories with the objective, this time, of identifying the groups or individuals at risk of victimisation.

Problem	**Conventional Crime Analysis (low to moderate data demand and complexity)**	**Predictive Analytics (large data demand and high complexity)**
Identify groups likely to be victims of various types of crime (vulnerable populations)	Crime mapping (identifying crime type hot spots)	Advanced models to identify crime types by hot spot; risk terrain analysis
Identify people directly affected by at-risk locations	Manually graphing or mapping most frequent crime sites and identifying people most likely to be at these locations	Advanced crime-mapping tools to generate crime locations and identify workers, residents, and others who frequent these locations
Identify people at risk for victimization (e.g., people engaged in high-risk criminal behavior)	Review of criminal records of individuals known to be engaged in repeated criminal activity	Advanced data mining techniques used on local and other accessible crime databases to identify repeat offenders at risk
Identify people at risk of domestic violence	Manual review of domestic disturbance incidents; people involved in such incidents are, by definition, at risk	Computer-assisted database queries of multiple databases to identify domestic and other disturbances involving local residents when in other jurisdictions

Table 4 – Methods for predicting the future offender. Source: *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, in *RAND. Safety and Justice Program*, 2013, p. 12.

5. The Development of Predicting Software in Anglo-Saxon Countries

The greatest development of artificial intelligence in this field, with specific regard to predictive policing techniques, has taken place in the Anglo-Saxon countries and, in particular, in the United States. The latter has developed several predictive policing systems which, unlike the European experience, are used for a wide range of crimes.

These predictive methods are designed to predict future crimes in a perspective of general prevention. In fact, the American software is not only based on the characteristics of specific crimes, capable of providing the algorithms with the right data to predict future actions (so-called crime linking), but, more generally, tends to analyse the area and spreads the police force efficiently. With this, they try to dissuade criminals, also thanks to the deterrence generated in the community, which is well aware of the operating efficiency of artificial intelligence systems.

One of the more renowned software in the U.S. is *PredPol* (abbreviation of Predictive Policing), developed by some researchers of two Californian Universities, in collaboration with the Local Police Department.[20]

This software, still in use in the U.S., consists of an operating diagram aimed at analysing property crimes, in particular, burglary, vehicle theft and theft from vehicles. The information on past crimes committed in the area under analysis acts as input to the program, which already has a huge database. This input is crossed with the software's own algorithm, which allows the "hottest" spots to be predicted. The heat map which is traced is functional to the organisation of the police operations, which, promptly and precisely, provide the system with new data records, on the basis of which the analysts continue to process trends and criminal models. It should be specified that the police officers are not acquainted with the methods used to create the maps: they are only required to use their professional skills and experience to identify the interventions to be taken.

One of the first models of predictive policing was born in 2005 in another area of the United States, more specifically in Memphis (Tennessee). The software, innovative at that time, is developed by IBM with the name of *Blue C.R.U.S.H.* (*Crime Reduction*

[20] Z. Friend, *Predictive Policing: Using Technology to Reduce Crime*, in «FBI Law Enforcement Bulletin», 2013.

Utilizing Statistical History). Memphis, the first most populous city in Tennessee, had seen a huge rise in the crime rate, in such a way that it had significant effects on the population and the local economy.

It is for this reason that the local authorities tried to draw up a new methodology to combat and manage crime.[21] The software project took into consideration a set of variables, such as the geographical data regarding the crimes committed and being committed, as well as environmental, social and demographic factors. The crossing of the analysed data allows hot-spot maps to be created. The results obtained using this software were considerable and led directly to a reduction of 25% in property crimes.[22]

A similar experience in Europe is the one made in the United Kingdom by some researchers from the Jill Dando Institute of Security and Crime Science in London. The experiment took place in Trafford with the aim of drastically reducing the incidence of burglaries and was Europe's link with the experiences in the United States.

The project started from the assumption that repeat victimization and near repeat victimization are reiterated over time and space. This is why it was necessary to spread police forces over the areas where burglaries had been committed in the (not distant) past. The operation of the experiments included an initial phase aimed at mapping, on one hand, the buildings in which the thefts had occurred and, on the other, the buffer zones, highlighted with different colours according to the near repeat victimization rate. The organisation of the police, based on the data resulting from the experiment, allowed an important reduction in burglaries to be achieved.

6. The Experience of Predictive Policing in Europe

In Italy, the experience of artificial intelligence applied to predictive policing is quite significant and is concentrated on the prevention of specific crimes and the search for criminal profiles which, sometimes, hide mandates that can be traced back to

[21] T. Armstrong, *Managing for 21st Century Crime Prevention in Memphis*, available at: <http://www.managementexchange.com> (accessed 02.11.2021).

[22] J. Vlahos, *Come anticipare il crimine*, in «Le scienze», 2012.

structured criminal organisations capable of repeating (or have repeated) a considerable quantity of crimes.

Besides the pioneering *KeyCrime*,[23] the experience of other Italian IT programmes is worthy of being mentioned, albeit briefly, because it has led to satisfying results in the territorial areas of interest.

A type of software that handles predictive policing through a heuristic algorithm, on a probability basis, is *XLAW*. This instrument, created by the Police Inspector Elia Lombardo, is based on the idea that urban crimes are committed in precise places and a relatively short space of time, which allows the maximum profit to be drawn from the seriality. The places where crimes are concentrated are chosen by people acting on the basis of an objective (*e.g.*, presence of potential victims) and a subjective element (*e.g.*, presence of shelters, suitability of the area in terms of accessibility and escape routes). The software intelligence crosses the "appetising" places in a single map and superimposes their socio-economic and environmental characteristics, as well as information on past crimes, on it. This way, the system allows the re-creation of criminal models that can be potentially applied to an indefinite series of crimes. The risk map drawn up by the software is supplied to the operator, who, even two hours in advance, can intercept the places and times where, at a probability level, a crime will be committed.

Another predictive policing system, in the experimental stage, is *S.O.Cr.A.TE.S.*, software that is being researched by the Italian Ministry of Defence and the Department of Equal Opportunities, in collaboration with the Department of Prison Administration, in order to carry out the scientific research with the support of inmates. The purpose of the project is to construct an effective criminal profiling that represents the behaviours of various types of crime against the individual (violent crimes, apparently motiveless and with a sexual background).

On the other hand, a computer program capable of receiving anomalies that can be traced back to episodes of money-laundering is being used in financial matters.

[23] For an in-depth analysis of this software, see L. Grossi, *Software predittivi e diritto penale*, in *Intelligenza artificiale e giustizia penale*, edited by A. Massaro, Paruzzo Editore, Caltanissetta 2020, p. 155 et seq.

Gianos is the software used by the majority of Italian banking institutions. It is based on the constant comparison of databases held by the various entities involved, which allows a somewhat efficient cross-check to be carried out.

Predictive policing systems are also constantly used in Spain.[24] Already in 2006, following a series of forest fires in Galicia, the *Guardia Civil*, in collaboration with the *Fiscalía Coordinadora de Medio Ambiente y Urbanismo de la Fiscalía General del Estado*, started a study on the psychological profile of the so-called *incendiarios forestales*. Police officers filled in an online questionnaire of a psycho-social nature whenever they arrested a pyromaniac.[25] Thanks to the information obtained via the questionnaire instrument, predictive policing tools were implemented. These allowed a search for the most frequent characteristics in the pyromaniacs so as to facilitate the police operators to localise and identify the criminal. The experiment was of great use because it placed the methodological bases to be made use of in other criminal dynamics.

The development and application of predictive policing in Spain are of particular significance in two specific sectors, which are strictly connected to each other: on one hand, in gender violence and management of the safety of the victims, and, on the other, in cases of homicide, when the algorithms allow to make a probability estimate for the personal characteristics of the potential authors.

To date, the most developed predictive policing methodology in Spain is the one regarding the creation and validation of a protocol for assessing the risk of re-offending with regard to gender violence using the *Sistema de Seguimiento Integral de los Casos de Violencia de Género* ("Full Monitoring System for Cases of Gender Violence"), which is called *VioGén* and was developed by the *Secretaría de Estado de Seguridad* of the Spanish Ministry of the Interior. This protocol allows the officers to assess the risk that a woman who reports a violent crime runs of being a victim of the same crime from the same or another partner. To do this, a specific computer procedure

[24] See J.L. González Álvarez, J. Santos Hermoso, M. Camacho Collados, *Policía predictiva en España. Aplicación y retos futuros*, in «Behavior & Law Journal», n. 6, 2020, p. 26 et seq.

[25] J.L. González, V. Muñoz, M.L. Calcerrada, A. Sotoca, *Perfil psicosocial del incendiario forestal español privado de libertad*, in «Behavior & Law Journal», n. 3, 2017, p. 26 et seq.

called *Valoración Policial del Riesgo* (VPR, *i.e.*, Police Risk Assessment) is used.[26] Depending on the level of risk obtained using the VPR, preventive strategies aimed at anticipating the repeat criminal action are drawn up, with the final aim of safeguarding the passive subject against the repeat victimization that he or she would be subject to.[27]

In the context of the fight against gender violence, actively combated by the Spanish system (see *Ley Orgánica* no. 1/2004 on global protective measures against gender violence), one should note that the cases of so-called femicide in Spain reach absolute values that cannot be ignored. It is for this reason that the *Equipo Nacional de Revisión Pormenorizada de Homicidios en el contexto de la Violencia de Género* (EHVdG) was set up in 2018, with the aim of examining the case histories of femicide at an international level, as well as the best practices of similar teams set up in other countries.[28] The work group was also in charge of planning and promoting the monitoring of the cases of femicide in Spain, facilitating the organisation of experts at district level, which consisted of professionals from a large number of universities and research institutes. These technicians, on the basis of collaboration agreements with the Ministry of the Interior, undertook the analysis work in the field, after receiving suitable training from the national team.

One of the most significant results of the detailed study of the femicides was the construction of a prediction scale for the risk of a lethal outcome following the reporting of gender violence. An analytical tracing of the crime facts was followed to create the scale, called H. The final sample consisted of over two thousand criminal episodes. Of these, just under 10% resulted in femicides and the remaining 90%

[26] J.J. López Ossorio, J.L. González, S. Buquerín, L.F. García, G. Buela Casal, *Risk Factors Related to Intimate Partner Violence Police Recidivism in Spain*, in «International Journal of Clinical and Health Psychology», 2017, p. 107 et seq.

[27] J.J. López Ossorio, J.L. González Álvarez, J.M. Muñoz Vicente, C. Urruela, A. Andrés Pueyo, *Validation and Calibration of the Spanish Police Intimate Partner Violence Risk Assessment System (VioGén)*, in «Journal of Police and Criminal Psychology», 2019.

[28] J.L. González, M.J. Garrido, J.J. López Ossorio, J.M. Muñoz, A. Arribas, P. Carbajosa, E. Ballano, *Revisión pormenorizada de homicidios de mujeres en las relaciones de pareja en España*, in «Anuario de Psicología Jurídica», 2018, p. 28 et seq.

consisted of non-mortal cases which had to be constantly monitored.[29]

The VPRs of all the episodes of crime about which there was information were needed to complete the study, as the aim was to understand whether the indicators for predicting a repeat of the violence were capable of also predicting a fatal episode.

To make the public safety operators' decisions easier, with regard to the protection of the victims, it was also decided to program a dual algorithmic mechanism that was transparent and shared with the officers. This way, when a report of violence is received, the police officers fill in the information card for the VPR. At this point, without showing any type of result, the *VioGén* system applies the first algorithm and calculates the risk of the specific episode being repeated on the basis of the elements available at that time. Then, with maximum speed, the program calculates, using the second algorithm, the risk that episode could constitute only a part of the criminal plan that will culminate in femicide.

If the second algorithm gives a positive result (*i.e.*, high risk of a mortal event), the risk of re-offending as of the first algorithm is raised a level. Only at this point the result of the analysis using artificial intelligence is shown to the officers, with the warning that the above-mentioned case is of particular interest. This takes place so that the measures adopted by the police bodies can be adequate for the characteristics and circumstances of the specific case.

One element of particular interest is that the report made to the police officers is also recorded in special minutes, to be sent immediately to the competent Court and the public prosecutor's office. The latter, while ascertaining the characteristics of the case, can adopt suitable measures to safeguard the victim and, if necessary, provide that the persons concerned are promptly assessed by psychologists or medical staff capable of going in depth into the factual circumstances and proposing new or different measures to protect and safeguard the victim.

This dual mechanism is put forward to reduce the rate of femicide in cases where a report has been made, clearly within the area where the *VioGén* system is used. The real efficacy of this dual protocol cannot be ascertained at the moment: in fact, in order

[29] González Álvarez, Santos Hermoso, Camacho Collados, *Policía predictiva en España*, cit., p. 33.

to monitor the work of the algorithms and formulate a judgement on their work, it is necessary to analyse the evolution of the various crimes of violence over a significant time scale.

7. Towards a "Criminal" Groupware: Bridging the Gap Between Benefits and Legal Concerns

Artificial intelligence, now at the height of its evolution and at the centre of social and legal debate,[30] is an undoubtedly important innovation which must, nevertheless, face its structural criticisms and the limits set by the current legal system.

Firstly, it has been highlighted several times that the operation of artificial intelligence (or rather, rationality) systems is based on the collection and processing of big data. The quantity of information and data collected is nothing but the fruit of reprocessing by the human being, who, as such, incorporates various partiality factors. At an instrumental level, this circumstance represents an effective limit to the operations of the algorithms: in fact, they only produce effective results if the input supplied is of quality and corresponds to the factual reality.

In order to achieve satisfactory results, it would perhaps be opportune to share and approve a *numerus clausus* of indispensable variables to be considered so as to make the algorithmic procedure much more objective. This closed number would only represent the starting point for data collection. In fact, it is evident that, given the specific circumstances of every case and the personal and professional qualities of the operators, every datum collected could hide aspects which escape the imperativeness of an *a priori* list.

A further problem encountered with data exploited by algorithms regards their quantitative aspect. Algorithms struggle to operate with the same efficiency in large and

[30] On this point, see *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment*, adopted by the European Commission for the Efficiency of Justice (CEPEJ) during its 31st plenary meeting (Strasbourg, 3-4th December 2018), 35, § 7, available at: < https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (accessed 02.11.2021).

small situations. The volume of data held by the operators, even if it were nothing but the different crime rate (from which the information "useful" for predicting the future is taken), diverges in a manner that cannot be ignored, depending on whether the reference territory is a medium-large size or medium-small size area.

Finally, with reference to the data, two more strictly legal questions are worth raising, one on privacy and the other on the ownership and control of the databases and the respective algorithms.

The implications that concern the right of privacy, with reference to the data used by artificial intelligence algorithms, come under the more general framework of the socio-technological development of contemporary society, which has led, in a short time, to a significant and sharp growth in the daily exchange of information, both at a domestic and an international level. However, such as in the case of the big data supplied to the software in question, personal data, and particularly sensitive data, is circulated in remote-controlled mode and, consequently, does not stop at the threshold of the State boundaries. Therefore, a regulatory intervention directly at a supranational level became necessary.

Personal data are thus widely protected both by domestic regulations and European ones. All the characteristics of the crimes, which, for one reason or another, concern individuals (criminals, victims or third parties) and are analysed by operators who feed the artificial intelligence, come into this category. The European legislator, with the General Data Protection Regulation (Regulation EU no. 2016/679), has also intended to prepare a special statute for particular categories of personal data, among which genetic and biometric data and data "regarding health" stand out. In the perspective of the configuration of the aforesaid statute, the range of the expression, designed to be broad, "data regarding health" is of particular importance. This locution, like a broad genus, includes the both the following species of data: firstly, the so-called immediately sensitive data (or sensitive in the strict sense) and, secondly, the so-called indirectly sensitive data (or sensitive in the broad sense).

Personal data which, by their nature, are born and exhausted in the phenomenological description of the individual's state of health come into the first category. The genetic characteristics of the individual, the blood group and audiometric results are, for example, immediately sensitive information. On the other hand, personal

data which, though appearing generic, hide intimate profiles are defined as indirectly sensitive, and are in any case worthy of particular protection. For example, the occasional or habitual use of substances that create addiction (*e.g.*, tobacco, alcohol and drugs) and the common prescription for glasses are information which, once acquired, reveal obvious clues on the state of health of the data subject.

Article 9 of the GDPR prohibits every type of processing for some sensitive data, except if «processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity» (letter f) and «processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject» (letter g).

Even if it may seem taken for granted, the algorithm organism is fed with every type of data (sensitive or not), even the most intimate (*e.g.,* concerning health and criminal convictions) or apparently useless data. To date, the current regulations on privacy applied to computer databases could be inadequate or, in any case, non-exhaustive whilst the ownership of the personal data, the subject of the processing, remains in the hands of private entities, with a heavy limitation of public control.

The artificial intelligence algorithms studied so far and the software in use are, indeed, under the almost total hegemony of private entities. The companies or organisations which create and own the algorithms exploit, just about freely, the personal data of a very high number of individuals.

On this point, it is interesting to note that these algorithmic codes seem inaccessible to the citizenry: a lack of transparency is hidden behind this context, which, normally, belongs to the action of the Public Administration.[31] In this regard, it is interesting to mention the recent ruling of the Lazio T.A.R. (Regional Administrative Court), sect. III *bis*, n. 3769/2017, which, although in a different sector and in different circumstances, recognised the right of the petitioner, as involved party, to access the algorithm used by the public administration in managing the proceedings under its remit,

[31] On the problem of the transparency of the algorithms, see E. Gabellini, *La «comodità nel giudicare»: la decisione robotica*, in «Rivista trimestrale di diritto e procedura civile», n. 4, 2019, p. 1305 et seq.

based on the fact that the very algorithm, all in all, gives life to the administrative act.[32]

In conclusion, no critical issues seem to arise relating to the usability of the evidence as far as artificial intelligence systems applied to predictive policing are concerned. With the exception of the privacy problem, the whole process of "predicting the future" does not seem to present any significant problems as long as the computer systems are solely an aid to the operators so that they can have a more efficient organisation, as happens in the case of preparing heat maps.

However, if the "artificial" systems are functional to the constitution of the evidence to be used in trial, the permissiveness of the current system is less clear and leaves space for wide profiles of uncertainty.[33]

In the context of possible co-ordination between predictive policing and predictive justice artificial intelligences, it would seem desirable to create an algorithmic system – one for each macro-category of crimes – that allows you to reconstruct the elements of the offence, both from an objective and a subjective perspective. If the investigators could enter all the elements available into a computer system and this system could manage to "pre-analyse" them in the framework of an informal "pretrial," the course of the trial would benefit from it and would meet less obstacles, both in qualitative terms and with regard to the procedural economy required by the due process.

In conclusion of this analysis, one cannot omit the hope that, in the perspective of an implementation of artificial intelligence tools in the near future, a law proposal is put forward, even directly from the European Union (with the collaboration of the bodies involved, such as Europol and EPPO). With the aim to regulate the automated crime prevention (in the broad sense) processes uniformly, on behalf of a shared

[32] The sentence under analysis recognized the right of the petitioner because the algorithm, though being pre-set to execute the duties established by legal regulations, finished up by deciding *de facto* what should be the working place of the teacher. On this point, see I. Forgione, *Il caso dell'accesso al software MIUR per l'assegnazione dei docenti – T.A.R. Lazio Sez. III* bis*, 14 February 2017, n. 3769*, in «Giornale di diritto amministrativo», 2018, p. 647 et seq.; L. Viola, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in «Foro amministrativo», 2018, p. 1598 et seq..; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in «BioLaw Journal», n. 1, 2019, p. 73 et seq.

[33] On the subject of the legal limits to the usability of the evidence, see L. Notaro, *Intelligenza artificiale e giustizia penale*, in *Intelligenza artificiale e giustizia penale*, cit., p. 93 et seq.

exigence, such law proposal could lay the foundations for a brand new "criminal" groupware.

In order to do this, it undoubtedly becomes necessary to share knowledge, as the knowledge required to meet the transition from traditional systems to "artificial" ones, so to speak, involve a diverse multitude of disciplinary sectors, ranging from mathematics, computer science and statistics to law.[34]

[34] On the opening of law to other sciences and the need to share knowledge, see P. GARBOLINO, *Nuovi strumenti logici e informatici per il ragionamento giudiziario: le reti bayesiane*, in «Cassazione penale», n. 1, 2007, p. 326 et seq.