AI AND THE ADMINISTRATION OF CRIMINAL JUSTICE IN ITALY

Mitja GIALUZ[1] and Serena QUATTROCOLO[2]

PART I. PREDICTIVE POLICING

1. National practices

General questions

1.1. In the Italian system, there is no official definition of "predictive policing", since there is no specific legislation on this subject[3].

1.2. Anyway, in Italy, we can see some forms of AI-based systems used for predictive policing.

The first one is XLaw, which has been designed and developed by police inspector Elia Lombardo. It was tested, first, by the Questura of Naples in 2004, and in 2013 also in Salerno, Prato, Parma, Modena and Venice.

In 2021, XLaw was acquired by XServizi, a company that, on the basis of this software, developed a new predictive policing program, Pelta Suite. The peculiarity of the latter consists in the availability of two different kinds of software, because it addresses either police offices (Pelta *Urban Security*) and commercial activities (Pelta *GDO&Retail*). Pelta *Urban Security* has been tested in towns such as Caorle, in Veneto, since 2021, and Signa, in Tuscany, since January 2022.

Another software is Delia® (Dynamic Evolving Learning Integrated Algorithm), the evolution of the former KeyCrime, invented by Mario Venturi, a former senior police officer. This system was used for the first time in 2008 by the Milan Police Department and since 2018 it has been produced by the innovative startup KeyCrime founded by the same ideator of the software, Mario Venturi.

There is also Vigilium, a software elaborated by the startup Intellegit and based on the know-how of the project eSecurity, co-funded by the European Commission under the program *Prevention of and Fight against Crime – ISEC 2011*. In particular, this project, which lasted from 2012 to 2015, is described as «one of the first projects worldwide on predictive policing and the first-ever project on "knowledge-based and predictive urban security"»[4]. It was experimented in the City of Trento, under the coordination of the eCrime research team of the Faculty of Law-University of Trento, in partnership with the Questura of Trento, the ICT Centre of Fondazione Bruno Kessler and the Municipality of Trento. So, as already noted, Vigilium comes from this experience. In particular, it has been adopted since 2019 in a specific area of Naples and since 2020-2021 in some municipalities of the Emilia-Romagna region.

With reference to predictive policing, it is also possible to mention a program which aims to help the police to identify potential criminal conducts and people linked to terrorism. More specifically, the Italian Ministry of Defence and Carabinieri adhere to DANTE project (*Detecting and Analysing Terrorist-related Online Contents and Financing Activities*), financed by the European Commission and already implemented by Carabinieri, in order to identify terrorism-related web contents[5]. In particular, based on a recent answer given by the European Commission to a Parliamentary question asking if the project results are being used and by whom[6], it is possible to specify that «so far, the platform has been made available for test runs and study cases to the law

[1] Full Professor of Criminal Procedure, University of Genoa, Italy.

[2] Full Professor of Criminal Procedure, University of Eastern Piedmont, Italy.

[3] It should not be overlooked the fact that many advocate that predictive policing is more a change in tools rather than strategy: F. Galli, Law Enforcement and Data-Driven Predictions at the National and EU Level. A Challenge to the Presumption of Innocence and Reasonable Suspicion?, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (eds), *Constitutional challenges in the algorithmic society*, CUP, 2022, p. 114.

[4] A. Di Nicola – S. Bressan, *eSecurity and the new horizon of urban security. An information system for police forces and local administrations, Guidelines*, Trento, November 2015, 2 (http://www.esecurity.trento.it/).

[5] https://cordis.europa.eu/project/id/700367/it.

[6] Question for written answer asked by Patrick Breyer (E-000025/2021) to the Commission, Parliamentary question, 5 January 2021.

enforcement authorities involved in the project»[7], including, therefore, the Carabinieri. More information, however, on the specific first year this system was used is not available.

Finally, in a broader sense, it seems also important to report other AI-based systems, not directly used by the police, but by other private or public actors.

In particular, Gianos is a software which was developed by Oasi, a company belonging to the Cedacri group, for anti-money laundering purposes: in particular, it is used by Italian banks, since 1994, in order to support the identification of suspicious operations and customer due diligence. Many bank associations contributed to the creation phase of this program. It has been constantly updated during the years; Gianos 4d is the version which has been developed in order to comply with the fourth EU anti-money laundering directive, as implemented by Legislative Decree n. 90 of 2017.

Similar programs used in Italy in this context are Discovery day, developed by Netech, and SOS, belonging to Sefin.

Lastly, in the public sector, it should be remembered the AI-based system called FROZEN, a program developed and used by the Italian Insurance body "Istituto Nazionale di Previdenza Sociale" (INPS). It was launched for the first time in 2017 to fight and prevent fraud in the area of fictitious jobs against the INPS and, in general, to the detriment of the State.

1.4. From a technological perspective, Delia® works through machine learning mechanisms; however, it should be specified that more detailed information on this point is not available.

Similarly, Xlaw – on which it was later developed Pelta Suite – is based on a heuristic kind of algorithm, which uses and elaborates data contained in denunciations and other police information, by means of machine learning mechanisms, with the aim of identifying the urban areas in which certain crimes are more likely to be committed.

As regards Vigilium, there is no particular information on its function from a technological perspective. However, concerning the pilot area of the City of Trento, we can observe that the project's results have consisted in the implementation of three products: the eSecDB geo-database, with the aim of storing data; the eSecGIS geographic information system, which, based on the data coming from eSecDB, has advanced capabilities for automatic report generation, visualization of risk maps and predictive urban security; the eSecWEB Web portal, which aims to improve the communication and the collaboration between the local administration and people on policies, initiatives and advice about preventive behaviors. In particular, the eSecGIS geographic information system «acts as a sort of "statistical engine" accessed via the web for data mining modules, algorithms for the calculation of crime indicators, and dynamic functions for map elaborations. More in detail, the database, which is relational type, is fuelled by 4 heterogeneous data flows and normalized on the basis of spatial and/or logical algorithms starting from the needs of users and analysis requested»[8].

As far as DANTE is concerned, it should be noted that it is an integrated and complex platform, that consists of more than thirty tools that have been developed during the project, «with law enforcement authorities as key practitioners»[9]. As reported on behalf of the European Commission, «the tools can be classified according to the type of functionality they offer: source management and content extraction, text analysis, image and video analysis, audio analysis, knowledge representation, mining and reasoning»[10]. In general terms, DANTE is based on advanced automated data-mining and analytical systems.

With reference to Gianos, it processes relevant data by means of the application of rules which have been established by a committee of experts, on the basis of instructions given by Banca d'Italia. Specific information concerning its functioning, however, is not available.

Lastly, FROZEN is based on a series of automated controls, structured with data mining methodologies.

[7] Answer given by Ms. Johansson on behalf of the European Commission. Question reference: E-000025/2021, 25 March 2021.

[8] A. Di Nicola – S. Bressan, *eSecurity*, cit., 14.

[9] Answer given by Ms. Johansson on behalf of the European Commission. Question reference: E-000025/2021, cit.

[10] Answer given by Ms. Johansson on behalf of the European Commission. Question reference: E-000025/2021, cit.

1.5. Concerning the kind of data used by these AI-based systems, Delia® focuses, in particular, on crime data, collected after the commission of a crime. Xlaw uses and elaborates data contained in denunciations and other police information, including – as expressly reported by, among others, the inventor of the tool – news from newspaper articles and on social networks (in particular, from Facebook, Youtube, Il Mattino.it, Napoli Today, Repubblica.it, Ottopagine.it.)[11]. Instead, as regards the more recent Pelta Suite, this algorithm processes two different layers of data. The first is composed of big data, concerning the specific features of the city context and relevant events, such as the arrival of trains and boats or demonstrations, in order to create a sort of "virtual town". The second layer consists in the information provided by the police, deriving from sources like denunciations and other criminal records, without any reference to data concerning specific individuals, but in order to identify models of criminal conducts.

As regards Vigilium, it receives, stores and organizes geo-referenced information on city security from many sources. In particular, the data used by the system consist of crime data, data about crimes, insecurity and urban degradation collected from anonymous alerts of citizens or based on people's questionnaires received through a dedicated app, data on the urban disorder, data related to the so-called "smart city", such as street lighting, traffic, weather, other data about socio-demographic variables, and data collected through intelligent video surveillance solutions (the latter are described as optional)[12]. Finally, it is important to point out that the software is also based on anonymized social network data and mobile data[13].

As regards DANTE, it elaborates data which are published online, either on the surface and in the deep web and dark nets[14].

Instead, Gianos processes data provening by the "Archivio Unico Informatico", which is the digital database used by Italian banks, containing information obtained through the identification and registration processes. Moreover, every bank can add other data, in order to make the software more suitable for its specific needs.

Finally, the inputs of FROZEN consist of predetermined risk profiles and results of the analysis of the historical data known to the Italian Insurance body INPS.

1.6. In general, these software are used in different kinds of areas, such as urban areas and suburbs, fields of terrorism, banking and financial markets.

1.7. Moreover, the criminal activities that the systems emphasize are closely linked to their purpose and function. In particular, Delia® is based on serial crimes such as robbery, sexual violence, homicide, theft and fraud. Since 2008 it has been used by the Milan police to prevent commercial robberies. In addition, in 2018 a trial of the application was also planned for thefts in the apartment. Finally, at the time of writing, there is the intention to use Delia® by the Municipality of Turin to fight sexual violence crime in public transport.

Similar to Delia®, Xlaw is focused on the prevention of "predatory crimes", such as robberies, thefts, burglaries and fraud in urban areas, because of their features, which make them foreseeable with a quite high accuracy level. In fact, they are normally serial, and their authors tend to perpetrate more than one of them within a short time, in order to gain illicit proceeds, and in similar ways in different towns. The same can be said concerning Pelta Suite, the evolution of Xlaw. In fact, the latter is used for "predatory crimes" in urban areas. Lastly, also Vigilium is mainly focused on crimes committed in urban areas and, in general, on urban disorder.

As regards Gianos and other similar programs, they are aimed at supporting the identification of operations which could involve money-laundering activities, or the financing of terrorism. Moreover, as has been mentioned above, FROZEN focuses on fraud against the INPS, in the general context of the fight against fictitious jobs. Finally, with reference to DANTE, it is aimed at identifying and analysing terrorism-related contents.

[11] See G. Di Gennaro – E. Lombardo – R. Marselli – M. Spina, *Tolleranza zero o deterrenza selettiva: quali strade intraprendere per rispondere più efficacemente alla domanda di sicurezza*, in G. Di Gennaro – R. Marselli (editors), *Criminalità e sicurezza a Napoli, Secondo rapporto*, Naples, 2017, 200.

[12] https://www.intellegit.it/soluzioni/sicurezza-urbana/.

[13] https://www.intellegit.it/soluzioni/sicurezza-urbana/.

[14] https://www.h2020-dante.eu.

1.8. Regarding the kind of organizations involved, it is no doubt that the predominant one is the police. However, as has already been noted, further actors may also be involved.

In particular, concerning more in detail Pelta *GDO&Retail*, we cannot omit to remark the recipients of this system: the private commercial activities, which could then use the private security companies. With reference to Gianos, it is currently used not only by Italian banks, but also by insurance companies and other financial intermediaries. The FROZEN program is instead conducted by the Italian Insurance body INPS.

1.9. The concrete results produced by these software are different depending on the system used.

More in detail, Delia® is able to use crime data, collected after the commission of a crime, to create a so-called "crime linking". In other words, this software elaborates and compares data to create a link between crimes that were committed by the same person. In the end, this helps investigators to predict where and when will be the future crime. Moreover, according to Delia®'s official website, this also permits to «convict perpetrators of their multiple crimes instead of just the last one for which they were caught»[15].

Instead, XLaw is based on the concept of "situational prevention", which aims at identifying the situations and conditions which can facilitate the commission of crimes. The main idea under this software is the strong link existing between the characteristics of urban areas and the commission of the "predatory crimes", such as robberies, thefts, burglaries and fraud: the latter are aimed to be influenced by objective and subjective factors, consisting, respectively, in the presence of suitable targets and in the availability of escape routes and hiding places, or, more widely, on conditions which could ease the author's flee. Another fundamental element consists in the identification of certain phases of city life, with special reference to the opening times of post offices, banks, shops and other commercial activities, as well as to the hour in which most people go out to reach their offices or schools, and also to train and bus schedules, because they are thought to influence the commission of crimes, too. Consequently, the system elaborates different layers of data, concerning, first of all, the features of urban areas and, then, the characteristics of the crimes committed daily within them, with reference to the authors, *modus operandi,* victims and proceeds; lastly, it takes into consideration the city life phases, as described above.

After the processing of this information, the software is capable of identifying models of criminal conducts which are perpetrated, in a regular manner, within a certain territory, as well as their time and space distribution. Consequently, it provides the police with an alert concerning the probable commission of a certain crime, in a specific area and at a given time, even foreseeing the kind of author and target. Alerts are updated every thirty minutes and are communicated to police officers on their phones and tablets, through a specific app.

Similarly, as regards Pelta Suite, the software output consists in the determination of the areas in which the crimes are more likely to be committed: these places are signaled with specific colors on a virtual map. Risk analysis is updated every thirty-sixty minutes, but an assessment of its evolution in the following seven days is also available, with the scope of ensuring a better organization of preventive activities. The program is even capable of quantifying a measure of "criminal pressure" concerning a specific area.

Vigilium produces real-time statistics, risk maps, and analyses, including predictive ones, to help police and local administrations to make more informed, rapid, and effective decisions on problems of crime, insecurity, and urban disorder.

DANTE is based on an effective data mining system, able to detect, monitor, collect and analyse huge amounts of «multimedia and multi-language terrorist-related contents»[16], either on the surface and in the deep web and dark nets. In particular, the DANTE platform is capable, by means of specific algorithms, of translating and summarizing quickly multi-language contents, as well as elaborating images, in such a way to recognize people and symbols. Thus, the system permits the fast identification of terrorist online groups and the storing of relevant data for further forensic analysis. Moreover, with regard to the financing of terrorism, it is projected to identify suspicious operations.

[15] https://keycrime.com/delia/.

[16] https://www.h2020-dante.eu/.

In the end, with reference to Gianos, it is used to make the customer due diligence and the notification of suspicious operations more effective. On the other hand, FROZEN identifies cases with risk profiles, allowing the INPS to carry out accurate controls on such situations. Depending on the outcome of these controls, the competent judicial authority may be informed.

1.10. Based on those results, it can be said that there are cases where AI-based systems have been used to improve policing through better allocation of resources and the adoption of more effective strategies[17]. In these situations, it seems that even a change in policing methods can be observed since the same use of predictive policing mechanisms transforms the traditional *modus operandi*.

1.11. In general, in Italy, the political or socio-economic incentives for using AI-based systems are principally based on safety and security promises[18] and focused on the need to reduce policing costs[19]. In addition, as already explained during the analyses, it should be pointed out that the eSecurity project, on which Vigilium has been built, was developed co-funded by a European program.

Moreover, in Italy, other projects aiming at using artificial intelligence for crime prevention purposes have been financed by the European Union.

In particular, beyond what we have already described about the DANTE project (see **1.2.**), it is possible to mention another predictive policing project, with crime-prevention objectives, called *Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies (AIDA)* and financed by the European Union in the context of Horizon 2020 program[20].

But that is not all. At the local level, it can be also seen that the recent use of Vigilium in some Italian municipalities has been partly financed by the Emilia-Romagna region. Lastly, it is worth noting to highlight the recent Italian Strategic Program on Artificial Intelligence 2022-2024. Although the AI-based systems connected to predictive policing are not expressly mentioned, this strategic program is important because it is focused on the development of AI in the Italian system, through European and national funding.

1.12. Finally, it seems that the concrete objectives pursued by using AI-based systems are in line with the stated objectives. More especially, the aim is mainly focused on preventing crime, reducing them, improving urban security and having positive repercussions in the socio-economic field.

1.13. In Italy, a public debate concerning the use of predictive policing has not really developed, yet. However, the media have spread information concerning the use of these algorithms, with special reference to XLaw and KeyCrime, and have enlightened their ability to make the prevention of crimes more effective, contributing to increase the security of urban areas.

Police officers tend to appreciate the reliability of the programs at issue; some of them are even involved in their design and development.

Academics have also dealt with this topic and some universities validated or contributed to create the programs: for example, XLaw obtained the validation of two Neapolitan universities and Vigilium was tested under the supervision of the research team eCrime of the University of Trento.

Generally speaking, however, the academic approach to the matter is quite more critical.

In fact, law professors, even if they recognized the advantages of these techniques, in terms of better allocation of resources and effectiveness of police activities and of the prevention of crime, also enlightened the risks deriving from predictive policing, with reference to the respect of fundamental rights. As it will be better

[17] See, in particular, the interview made by R. Juvara, *Il Questore di Milano: durante l'EXPO più sicurezza anche in città*, in https://www.securindex.com/downloads/25f5cb77b28be2746a8c167d5707db45.pdf, March-April 2015.

[18] See e.g. Delibera di Giunta dell'Unione pedemontana parmense, Act n. 24, 9.3.2021, in https://www.unionepedemontana.pr.it/upload/unioneparmense_2019/gestionedocumentale/PianodellaPerformance2021_784_65207.pdf ; Procura della Repubblica presso il Tribunale di Milano, Bilancio di responsabilità sociale 2018, in https://www.procura.milano.giustizia.it/files/brs-procura-milano-2018.pdf.

[19] See e.g. R. Juvara, *Il Questore di Milano*, cit.; or, again, Delibera di Giunta dell'Unione pedemontana parmense, Act n. 24, cit.

[20] In Italy, the project is guided by Engineering Ingegneria Informatica; Pluribus One, a company based in Cagliari, leads the Work Package on the creation of AI systems aimed at the collection of information and the analysis of criminal models.

explained in the following paragraphs (see **3**), the legal doctrine observed that these programs place at risk the privacy of individuals, because of the use of big data and of the massive storage of personal information[21]. The problem is made even more serious by a certain lack of transparency with regard to the sources of data which represent the algorithm input; some authors envisaged the possibility of a self-acquisition of information by the algorithm[22]. Another critical aspect is identified with the risk of discriminations and biases, deriving from the selection of information and from the way in which the program is designed in order to process them, and of "self-fulfilling prophecies"[23].

Assessment of reliability, transparency and effectiveness

1.14., 1.16. With reference to AI-based systems used for predictive policing in Italy, some information about their effectiveness and reliability is available.

In particular, the effectiveness of using KeyCrime – then evolved into the current software Delia® – has been evaluated both by the authorities using the system and by third parties.

Especially, concerning the first profile, based on the data available on Delia®' s official website[24], the use of the software has produced a reduction in retail robberies of about 58% from 2008 to 2017 in Milan and a reduction in bank robberies of about 89% from 2009 to 2017 in the province of Milan. Moreover, a constant increase in solved retail robberies – meaning the identification of the offender – has been recorded from 2008 (47%) to 2017 (63%). Similarly, as regards bank robberies, the percentage of crimes solved has increased from 2009 (38%) to 2017 (60%). Finally, following the use of this AI system, the number of robberies dropped much more compared to other cities.

On the other side, concerning the evaluation made by third parties, the software has been analyzed by a research conducted by the Professor of Economics Giovanni Mastrobuoni[25]. The analysis has been based on commercial robberies in Milan, comparing two police forces, the Polizia di Stato, using KeyCrime, and the Carabinieri, acting traditionally.

The research highlights that, «while there is no evidence of a productivity differential between Polizia and Carabinieri for the very first robbery of a sequence, subsequent robberies that fall in the Polizia sector as opposed to the Carabinieri sector are 8 percentage points more likely to be solved»[26]. In addition, it is observed that «when there is a Polizia Intervention the likelihood of clearing a case increases by 0.9 percentage points (more than 10 percent) for each additional robbery (Number of the sequence) the predictive policing software can analyze»[27].

In this context, it should also be pointed out that, after 2010, once the Carabinieri have access to the AI-based system reports, the gap's productivity between the two forces became smaller[28]. Moreover, based on the evidence illustrated by the research, after the implementation of the AI-based system during the period 2008-2011, the bank robberies rates fell from about 1.4 to about 0.5[29]. Finally, according to the evaluation, there are also significant economic advantages derived from using the predictive software[30].

[21] L. Algeri, *Intelligenza artificiale e polizia predittiva,* in *Diritto penale e processo,* 2021, 724 ff.

[22] C. Parodi – V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo*, 2019, 52.

[23] L. Algeri, *Intelligenza artificiale*, cit., 724 ff.; M.B. Armiento, *La polizia predittiva come strumento di attuazione amministrativa delle regole*, in *Diritto amministrativo*, 2020, 983; A. Bonfanti, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *Media Laws*, 24 ottobre 2018, 206 ff.; G. Contissa – G. Lasagni – G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet*, 2019, 619 ff.

[24] https://keycrime.com/.

[25] G. Mastrobuoni, *Crime is Terribly Revealing: Information Technology and Police Productivity*, in *Review of Economic Studies*, 2020, 87, 2727.

[26] G. Mastrobuoni, *Crime is Terribly Revealing*, cit., 2729; see also 2746.

[27] G. Mastrobuoni, *Crime is Terribly Revealing*, cit., 2746.

[28] G. Mastrobuoni, *Crime is Terribly Revealing*, cit., 2748.

[29] G. Mastrobuoni, *Crime is Terribly Revealing*, cit., 2734

[30] G. Mastrobuoni, *Crime is Terribly Revealing*, cit., 2750.

In addition to the foregoing, we can't overlook that Delia®'s official website reports that all the documentation connected to the use of KeyCrime in the Milan area «was evaluated by the Italian Ministry of Justice»[31]. However, this is an unclear issue, since more information can't be found on this point.

Instead, concerning Vigilium, we can observe that the reliability of the eSecGIS geographic information system – one of the eSecurity's products on which Vigilium was developed – has been evaluated by the inventor of the system. The software has been tested concerning domestic burglaries in the municipality of Trento by the district during 2014[32]. In particular, as regards the system's predictive power, the study affirms «the good performance of the model»[33], without omitting to specify that this performance «can only be further improved by the use of explanatory variables with more precise spatial and temporal details»[34].

In addition, the reliability and effectiveness of XLaw and Pelta Suite have been evaluated by their creators and by the authorities who have used them, but XLaw, as said above, obtained also an academic validation in 2019.

With reference to XLaw, its estimated accuracy level amounts to 87-93% in Naples, to 92-93% in Venice and to approximately 94% in Prato; in Parma, the police central stations registered a percentage between 87 and 97%[35].

Moreover, concrete results in a crime reduction perspective have been observed.

According to data provided by the Questura of Parma, published in March 2019, a decrease of "predatory crimes" was registered in the cities in which the program has been used: the reduction is equal to 27.9%, from February 2013, in Naples, to 39.9.%, from December 2016, in Venice, to 37%, in Parma, and to 24.3% in Modena, from January 2019. In the same cities and with reference to the same periods, an increase of arrests *in flagrante delicto* was observed: this percentage is equal to 29% in Naples, to 22% in Venice, to 26% in Parma and to 19% in Modena[36].

Similarly, the developers of Pelta Suite report an accuracy level between 87 and 93%[37].

A possible negative effect deriving from the use of this kind of program had been identified with the movement of the authors of crime to new areas, subjected to fewer police interventions. However, the developers of the software denied this, declaring that no similar consequence had been actually observed.

In conclusion, with reference to Gianos and other similar instruments used for anti-money laundering purposes, according to data provided by the Italian Financial Information Unit in 2020, 26% of reports of suspicious operations derives from automated systems, and 37,9% of notifications attributed to bank branches concerns transactions identified by IT tools[38].

1.15. Contrary to what has been just seen about reliability and effectiveness, the impartiality of AI-based systems used for predictive policing in Italy doesn't appear to have been analyzed.

1.17. In the end, to our knowledge, there aren't public authorities, which have experimented with using AI-based systems for predictive policing, that have decided not to use them in the future.

2. Normative framework

Law and soft law

[31] https://keycrime.com/.

[32] A. Di Nicola – S. Bressan, *eSecurity*, cit., 28 ff.

[33] A. Di Nicola – S. Bressan, eSecurity, cit., 31.

[34] A. Di Nicola – S. Bressan, *eSecurity*, cit., 31.

[35]https://www.cnr.it/sites/default/files/public/media/attivita/editoria/VOLUME%20FULL%2014%20digital%20LIGHT.pdf.

[36] https://www.parmateneo.it/?p=49150.

[37] https://www.pelta.it/.

[38] F. Berghella, *I vincoli per lo sviluppo degli algoritmi e dell'intelligenza artificiale nell'antiriciclaggio*, in *https://www.cedacri.it/cedacri/downloads/rassegna_stampa_2014/Bancaria-n.6-2020-Berghella-Algoritmi-e-IA.PDF.*

2.1., 2.2., 2.3. In Italy, specific legislation concerning predictive policing is absent and, at the moment, Italy is not considering adopting such legislation. Similar considerations can be done for the normative instruments produced by executive authorities.

Nevertheless, considering that these instruments involve a massive collection of personal data, legal rules regarding data protection must be considered in this field.

Legislative decree n. 51 of 2018 implements EU Directive 2016/680, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. In particular, Article 16 of this national normative source establishes the principles of privacy by design and privacy by default, imposing the adoption of technical and organisational measures, including pseudonymization, aimed at protecting either personal data and individual rights. Moreover, it provides for a limitation of the processing of personal data, by default, only to the ones which are necessary for each specific purpose pursued.

Article 8, implementing Article 11 of the Directive, prohibits decisions based solely on automated processing, including profiling, which produce an adverse legal effect concerning the data subject, unless authorised by European Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject.

From the same perspective, it is useful to mention the Decree of the President of the Republic n. 15 of 2018, regarding the processing of personal data for prevention, security and police purposes. It establishes, under Article 10, the maximum periods in which data retention is allowed, with reference to the different kinds of information which may be processed; according to Article 10, the new IT systems should be designed in such a way that, after the expiring of this term, data are cancelled or made anonymous, and that all authorized people's operations are registered. Moreover, the controller and the processor must adopt measures aimed at guaranteeing the security of personal data and at avoiding their loss or damaging, as well as any kind of illegal access.

In addition, the use of automated instruments and IT technology to support the analysis of transactions for anti-money laundering purposes is established by Article 36 of Legislative Decree n. 231 of 2007. With reference to the assessment of the risk of money-laundering or terrorism financing activities associated to transactions, Banca d'Italia also adopted dispositions which recommend the use of IT tools[39].

Concerning the internal administrative acts, it is necessary to recall the circular adopted by the Italian Insurance body INPS. We refer in particular to Circular n. 93 of 2017, which is entirely dedicated to the FROZEN system. Especially, the act aims to introduce this system, describing its function and objectives.

Finally, to our knowledge, no specific soft law source concerning predictive policing has been published, yet. Anyway, even in this case, it is important to mention the recent Italian White Paper on Artificial Intelligence (*Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*), adopted in 2018 by the Italian public agency AgID (Agenzia per l'Italia digitale). More in detail, it is a document addressed to public administrations, which contains recommendations and guidelines on sustainable and responsible use of artificial intelligence, without omitting to consider the problematic aspects connected to AI.

2.4. International normative instruments concerning the use of AI-based systems are also important for the national criminal justice system. As explained above, the Italian legislator has implemented the EU Directive 2016/680, which is relevant with regard to the processing of personal data for police and prevention purposes. In the same context, particular attention should also be drawn to Article 8 ECHR and, above all, to Article 8 CFREU, which expressly guarantees the right to the protection of personal data. Moreover, it is necessary to recall the right to privacy protected by Article 8 ECHR and Article 7 CFREU.

[39] See, in particular, Banca d'Italia, *Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo*, in G.U., Serie Generale, n. 83, 8th April 2019.

Case law

2.5. To our knowledge, the judicial authorities[40] or regulators haven't issued decisions in cases in which AI-based systems were used for predictive policing. However, in this context, we cannot omit to indicate that in Delia®'s official website it is explicitly affirmed that thanks to this software «prosecutors benefit as well as delia®'s documentation helps them prosecute criminals for multiple crimes and not just the one for which they were caught»[41]. Anyway, as already noted, there is no direct evidence about it.

2.6. As regards eventual decisions issued by the criminal courts on the subject, the answer is partly different.

First of all, according to the Milan Police Department's official website, a preventive measure has been adopted, founded, among other things, on the serial character of the robberies committed by the recipient, which has been analyzed through the software KeyCrime[42]. Nevertheless, it is not possible to find more information on this point.

Moreover, it seems also important to signal one judgement of the Italian Court of Cassation which dealt with a case concerning the Gianos system. In particular, this decision, in endorsing the judgement given by the court of the second instance, inferred the conscious participation of the accused person in a money-laundering operation from, among others, the failure to report a suspicious transaction, despite the alert made by Gianos[43].

2.7. Finally, there are no decisions given in cases in which AI-based systems were used for predictive policing by the civil, administrative, constitutional courts or other independent authorities.

Substantive guarantees

2.8. The reliability, impartiality and effectiveness of the AI-based systems used for predictive policing are not addressed by specific legislative provisions in Italy and there are no mechanisms that allow the victim to be compensated. However, in administrative matters, there are interesting decisions issued by the Council of State (Consiglio di Stato) that establish the need to respect the fundamental principles of the Italian legal system concerning AI-based systems. So, this case law may also include those systems regarding predictive policing. In particular, among the principles mentioned, there is the prohibition of algorithmic discrimination. This means that mathematical procedures or appropriate statistics must be used for profiling, taking appropriate technical and organizational measures to rectify the factors causing data misstatements and to reduce the risk of mistakes. The aim should be also to ensure the security of personal data, in order to prevent the discriminatory effect[44].

2.9. Because of the lack of a normative framework, in Italy there is no legal obligation for AI-based systems to be certified or labelled before they can be used for predictive policing. However, as we said before, XLaw was validated by the *Direzione centrale anticrimine* of the Public Security Department, Minister of Domestic Affairs, and by Federico II and Parthenope Universities. Moreover, Vigilium was tested under the coordination of the research team eCrime of the University of Trento.

To our knowledge, no public information or report is available, with reference to the details of the validation process and to the criteria applied.

2.10. There is no legal obligation, for the authorities using AI-based systems for predictive policing, to continuously monitor and adjust them.

2.11. With reference to transparency about the technological functioning of AI-based systems, it is not really guaranteed[45]: only information concerning the general features of the programs is provided by their creators. Moreover, a complete transparency is not guaranteed even with reference to the way of collecting data which

[40] E.g. prosecution services, tribunal deciding on investigation measures.

[41] https://keycrime.com/.

[42] See, in particular, https://questure.poliziadistato.it/it/Milano/articolo/11945ca751d7e9cfc751322501.

[43] Cass., sez. IV, 18 February 2016, n. 10709.

[44] Council of State, sez. IV, 4 February 2020, n. 881.

[45] There are no peer reviews, auditing systems, etc.

represent the input of the algorithms, with particular reference to the ones different from the content of denunciations and police records, such as information from social networks.

However, more significant transparency is guaranteed with reference to the eSecurity project of the University of Trento, which represents the basis of Vigilium. Infact, in the guidelines published on the website of the project, it is possible to find information concerning the algorithm input: anonymous data concerning reported offences, collected in the SDI ("Sistema di Indagine" - Investigation System) database of the Italian Ministry of Domestic Affairs; data collected through a survey on objective and subjective security in the municipality of Trento; geo-referenced data on urban disorder collected by the Questura of Trento through a specific device; smart city data and other socio-demographic and environmental variables. Technical indications concerning eSecGIS geographic information system, an ICT prototype able to process data and to automatically generate reports and maps of both risk and predictive urban security, through the use of specific algorithms, are even provided.

2.12. We should also like to emphasize that there is no specific legal framework on the accountability of the companies producing AI-based systems for the results they provide. Nevertheless, they may be held responsible in civil matters pursuant to the general rules on civil liability.

2.13. In general, it should be specified that there are no precise modalities through which organizations that use software for predictive policing guarantee transparency about their practices. It is visible, for example, some limited information about it on the official website of the Italian police force Polizia di Stato (https://www.poliziadistato.it/) or on journalist interviews (e.g. see an interview given by the Superintendent of Milan in 2015)[46]. Instead, more detailed information on this issue has been ensured within the eSecurity project (see http://www.esecurity.trento.it/). Finally, it is necessary also to recall the case concerning the FROZEN system. In this situation, the abovementioned administrative act, issued by the Italian Insurance body INPS, outlines the operation and the objectives of the new program adopted.

2.14. In addition to the above, these organizations are not accountable for the actions they undertake based on indications provided by AI. Anyway, if, for instance, a person is arrested on the basis of an incorrect AI-based system calculation, it will apply the general legislation guaranteed by the Italian code of criminal procedure. In particular, that person can be entitled to claim compensation under Article 314 c.p.p. due to the unlawful detention.

2.15. Finally, as has been described above, the police authorities that use AI-based systems must act in accordance with the right to privacy and data protection. In particular, they must respect the obligations and the guarantees prescribed by Legislative decree n. 51 of 2018, which implements EU Directive 2016/680, and by Decree of the President of the Republic n. 15 of 2018, regarding the processing of personal data for prevention, security and police purposes (see **2.1, 2.2., 2.3**).

3. General principles of law

3.1. In Italy, there is a discussion about protecting the right to equality or the right to non-discrimination with respect to AI-based systems used for predictive policing[47]. This also particularly concerns the observation that processing methods may reproduce or aggravate human discrimination[48]. According to the legal commentators, the problem arises especially where such systems are based on factors of dangerousness related to ethnic, religious and social characteristics[49] or, more generally, focused on data affected by bias[50].

[46] R. Juvara, *Il Questore di Milano*, cit.

[47] See among the other, L. Algeri, *Intelligenza artificiale*, cit., 733; M.B. Armiento, *La polizia predittiva*, cit., 993 ff.; A. Bonfanti, *L'efficacia orizzontale*, cit., 206 ff.; R. Patscot – M. Bisogni, *Intelligenza artificiale e dati giudiziari: verso una "iurisfera" digitale del procedimento penale (telematico)?*, in *ilProcessotelematico*, 17 March 2022; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milan, 2021, 19. More in general, V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (editor), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milan, 2020, 541.

[48] P. Severino, *Intelligenza artificiale e diritto penale*, in U. Ruffolo (editor), *Intelligenza artificiale*, cit., 541.

[49] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto penale e uomo*, 29 September 2019, 13.

[50] P. Severino, *Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in P. Severino (editor), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, Rome, 2022, 96-97.

This may be, in particular, the case of Delia®. As noted by a newspaper article[51], in turn quoted by a study conducted by the international human rights NGO Fair Trials[52], Delia® uses ethnicity data, unlike other systems that have abandoned the use of ethnicity data as a result of controversy related to problems of discrimination against the weakest members of society. The system's developer expressly affirms that «in terms of investigation, information on the ethnicity of those who committed the crimes is essential; if developers of other software have decided not to collect this data, I have serious doubts about the effectiveness of their software»[53].

Critical remarks rise even as far as the AI-based systems crime hotspots are concerned (as may be the case of XLaw, Pelta Suite or Vigilium). In this situation, scholars observe that police activity increases in the hotspots identified by the software. Thus, this may create vicious cycles. Going more in detail, in this way, the number of crimes detected in relation to an area or certain persons will rise. In turn, the crime prediction algorithms concerning those areas or persons will increase, causing discriminatory effects[54] and, at the same time, determining the risk of a reduction in law enforcement activities in other areas[55].

3.2. A debate concerning right to privacy and data protection has developed in Italy, because of the use of big data and of the massive storage of personal information involved in predictive policing tools[56]. Emphasis has been placed on the need to minimize the risk of violation of the right to privacy arising from mass surveillance as well as safeguarding the protection of personal data. Moreover, it is precisely in the field of predictive policing that scholars have recently pointed out the important European Parliament resolution of 6 October 2021[57], emphasizing the fact that it has requested a moratorium from the Member States for each type of activity leading to a form of mass surveillance[58].

As has already been mentioned, Italy has adopted Legislative decree n. 51 of 2018 to implement the EU Directive 2016/680, which, together with the general rules contained in Regulation (EU) 2016/679 (GDPR), represents the so-called data protection reform package. However, this legal framework may not provide satisfactory protection concerning the right to data protection. In particular, it is necessary to report a recent study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. It examines the impact on fundamental rights of Artificial Intelligence in the field of law enforcement and criminal justice, even regarding predictive policing[59]. Well, this research expressly points out that «the current EU data protection legal framework shall not be assumed to offer enough solid safeguards for individuals in light of the increased uses of automated decision-making profiling for law enforcement and criminal justice purposes»[60].

Legal commentators have raised similar concerns, generally affirming that data protection rules «may not be of much assistance to those whose fate is determined by predictive policing technologies»[61].

[51] A.D. Signorelli, *Il software italiano che ha cambiato il mondo della polizia predittiva*, 18 May 2019, in Wired. This article is also translated into English by KeyCrime in https://www.keycrime.com/stampa1.

[52] Fair Trials, *Automating Injustice: the use of artificial intelligence & automated decision-making systems in criminal justice in Europe*, 9 September 2021, in https://www.fairtrials.org/articles/publications/automating-injustice/.

[53] See, again, A.D. Signorelli, *Il software italiano*, cit., translated into English in https://www.keycrime.com/stampa1.

[54] C. Parodi – V. Sellaroli, *Sistema penale e intelligenza artificiale*, cit., 58 e 70. See also A. Ziroldi, *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in *Questione giustizia*, 18 October 2019.

[55] F. Basile, *Intelligenza artificiale*, cit., 13; P. Severino, *Intelligenza artificiale*, cit., 541-542.

[56] See among the other, L. Algeri, *Intelligenza artificiale*, cit., 724 ff.; G.M. Baccari – C. Conti, *La corsa tecnologica tra costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Diritto penale e processo*, 2021, 711 ff.

[57] See European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

[58] P. Severino, *Le implicazioni*, cit., 96.

[59] *Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights*, Study requested by the LIBE committee, July 2020, in https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)656295.

[60] See the executive summary of *Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights*, Study requested by the LIBE committee, July 2020, 2.

[61] O. Lynskey, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing*, in *International Journal of Law in Context*, 2019, 175.

Some authors, with reference to pseudonymization of personal data, have observed that the risk of identification of the individual is not absent, as an effect of the possible combination of different kinds of anonymised data[62].

Moreover, with regard to the ban on decisions based solely on automated processing, including profiling, which produce an adverse legal effect concerning the data subject – established by Article 11 of EU Directive and by Article 8 of Legislative Decree n. 51 of 2018 – a reflection has been made with reference to the real ability of a natural person to adopt a critical approach towards the algorithm output[63].

Some doubts about the adequacy of the discipline of this matter are also connected to the processing of data by algorithms belonging to private subjects, in the absence of real control by public authorities[64].

In the end, it has also been observed that the possible violation of privacy and data protection rules will probably not produce significant consequences in the criminal proceedings, because of the traditional case law according to which this kind of violation does not determine the invalidity of procedural acts[65].

There are ways to challenge unlawful access to and use of personal data. In particular, Article 12 Legislative decree n. 51 of 2018 (in line with Article 16 EU Directive 2016/680) prescribes the data subject's right to obtain from the controller without undue delay the rectification of inaccurate personal data. Moreover, the controller erasures personal data without undue delay where processing is contrary to the law. The data subject has the right to be informed in writing by the controller of the refusal of rectification, cancellation or restriction of processing, with the reasons for the refusal, and of the right to lodge a complaint with the Italian Data Protection Authority or to seek a judicial remedy. In addition, the Italian Data Protection Authority has the task of checking the lawfulness of processing, conforming to Article 13 Legislative decree n. 51 of 2018. More generally, Article 39 Legislative decree n. 51 of 2018 (in line with Articles 52 and 54 EU Directive 2016/680) also guarantees the data subject's right to lodge a complaint with the Italian Data Protection Authority and to seek a judicial remedy if the data subject considers that the processing of personal data infringes provisions established by the Legislative decree[66].

Finally, under Article 41 Legislative decree n. 51 of 2018 (implementing Article 56 EU Directive 2016/680) the data subject has the right to receive compensation for the damage suffered from the controller, in case of an unlawful processing operation or of any act infringing the Legislative decree.

3.4. A debate concerning the proportionality requirement involves, more in general, the use of Artificial Intelligence and new technologies in criminal proceedings. As some authors observed, in Italy the lack of a specific statutory discipline concerning these instruments determined the urgency of an intervention of case law, implementing the principle in this field: in fact, proportionality aims at safeguarding the essence of individual rights, but in such a way to limit their restriction to what is necessary to satisfy other particularly relevant interests, such as the prevention and prosecution of serious crimes[67]. However, as far as data protection is concerned, the principle of proportionality is expressly established by Article 3 of Legislative Decree n. 51 of 2018.

In this context, the influence of European Courts on national discussion on the matter has been particularly relevant. In fact, when an interference with the rights to respect for private life and to data protection, guaranteed by Article 8 of the European Convention on Human Rights and by Articles 7 and 8 of the European Charter of Fundamental Human Rights, comes at issue, proportionality is a central requirement in the assessment of the legitimacy of technological measures involving a limitation of individual rights.

[62] A. Bonfanti, *L'efficacia orizzontale*, cit., 211.

[63] G. Contissa – G. Lasagni – G. Sartor, *Quando a decidere in materia penale*, cit., 629.

[64] A. Giraldi, *Intelligenza artificiale e predictive policing nella rinnovata fase d'indagine,* in A. Massaro (ed.), *Intelligenza artificiale e diritto penale,* 2020, 96.

[65] M. Pisati, *Indagini preliminari e intelligenza artificiale: efficienza e rischi per i diritti fondamentali,* in *Processo penale e giustizia,* 2020, 966.

[66] On the right to challenge unlawful access to and use of personal data, see also Articles 26-28 Decree of the President of the Republic n. 15 of 2018.

[67] C. Conti, *Sicurezza e riservatezza*, in *Diritto penale e processo*, 2019, 1576. See also D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Rivista italiana di diritto e procedura penale*, 2020, 3 ff.; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Diritto penale e processo*, 2021, 1043.

In particular, the Court of Strasbourg, with reference to measures of secret surveillance, has constantly affirmed that any interference can only be justified under Article 8, § 2, of the Convention if it is in accordance with the law, pursues one or more of the legitimate aims established by the norm and is necessary in a democratic society in order to achieve any such aim, establishing the principles of necessity and proportionality[68].

Moreover, a fundamental role, also for the evolution of the Italian legal system, has to be recognized to the case law of the European Court of Justice, with regard to data retention. Starting from the judgement on the *Digital Rights Ireland* case[69], the Court denied the compliance with EU primary law of rules allowing a massive collection and retention of personal data, without limitations regarding the kind of information collected, or the involvement of the persons concerned in investigations on serious crimes, and in the absence of adequate procedural safeguards, such as the need of an authorization of a judge or of an independent authority in order to access traffic data[70]. Especially in the latest judgement on this topic, a strong link has been established between the seriousness of the interference with individual rights and the seriousness of crimes which are prosecuted, as well as the need for the authorization of an impartial authority[71]. As previously observed, some predictive policing programs, with particular reference to Vigilium, use mobile data as a part of its input (see **1.5**).

However, even if the law regulating specifically data retention has evolved in such a way to comply with European prescriptions, other sectors do not seem to have really changed in a similar way. With particular regard to the analysis of big data by public authorities, it has been observed that it seems, per se, incoherent with the principle of proportionality[72].

3.3., 3.5. Instead, there is no debate in Italy on the rights to liberty and security of persons subject to the predictive policing tools and procedural legality, that is to say the requirement that enforcement authorities base their investigation on a suspicion (and not vice-versa).

3.6. Finally, there is a discussion about principles of constitutional law with regard to using AI-based systems for predictive policing and, more generally, concerning the use of AI in criminal matters.

First of all, it is worth noting to emphasize the need to protect the right to equality, when using predictive policing tools, which is expressly guaranteed by Article 3 of the Italian Constitution (see **3.1.**). It is also necessary to recall the right to privacy under Article 8 ECHR and Article 7 CFREU as well as the right to data protection, derived from Article 8 ECHR by the Strasbourg judges and, instead, expressly affirmed by Article 8 CFREU. In addition, it is again crucial to highlight the right not to be subject to decisions based solely on automated processing, established by Article 8 Legislative decree n. 51 of 2018 (implementing Article 11 EU Directive 2016/680) and, similarly, by Article 22 GDPR (see **3.2.**).

Furthermore, and more generally, reference has been made to Articles 14 and 15 of the Italian Constitution, protecting the inviolability of the home and correspondence and every other form of communication[73]. Article 13 of the Italian Constitution, ensuring the right to personal liberty, has been enhanced too, in the face of developments in digital innovation. In particular, some legal commentators stress the need for an

[68] ECtHR 25th May 2021, Big Brother Watch and others v. U.K.; ECtHR, 4th December 2015, Roman Zakharov v. Russia; ECtHR, 2nd August 1984, Malone v. U.K.; ECtHR, 6th September 1978, Klass and Others v. Germany; see also, on the surveillance via GPS, ECtHR, 8th February 2018, Ben Faiza v. France, and ECtHR, 2nd September 2009, Uzun v. Germany, in *hudoc.echr.coe.int*.

[69] ECJ, G.S., 8th April 2014, C-293/12 and C-594/12, Digital Rights Ireland Ltd.

[70] See also ECJ, G.S., 21th December 2016, C-203/15 and C-698/15, Tele2 Sverige AB and Watson; ECJ, G.S., 6th October 2020, C-623/17, Privacy International; ECJ, G.S., 6th October 2020, C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, in *curia.europa.eu*. On the Court's judgements, *ex multis*, C.M. Cascione, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di giustizia e gli echi del* datagate, in *Nuova giurisprudenza civile commentata*, 2014, 1045 ff.; R. Flor, *Data retention ed art. 132 cod. privacy: vexata quaestio (?)*, in *Diritto penale contemporaneo*, 29th March 2017; M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Diritto dell'Unione Europea* (II), 2014, 803; T. Rafaraci, *Verso una* law of evidence *dei dati*, in *Diritto penale e processo*, 2021, 853 ff.; F. Ruggieri, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cassazione penale*, 2017, 2483 ff.

[71] ECJ, G.S., 2nd March 2021, C-746/18, H. K., in *curia.europa.eu*.

[72] M. Pisati, *Indagini preliminari e intelligenza artificiale*, cit., 967.

[73] M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in *Giurisdizione penale*, cit., 56-57.

interpretation of the inviolability of personal liberty able to ensure integral protection of the individual not only in the physical dimension but also in the electronic dimension[74].

Another crucial aspect to be taken into account as far as principles of constitutional law are concerned is the possible use of the output of the predictive policing tools in criminal proceedings. Scholars have reported the issue[75], calling for the attention of the interpreter on it, since there is no regulatory coverage on the legitimate use of predictive policing systems[76]. This has been pointed out especially concerning the tools based on crime linking. In this case, as legal commentator noted, the outputs may be used not only in relation to the last crime committed by the accused (for which he has been identified) but also in relation to previous crimes constituting the criminal series reconstructed by the storage and processing of data, for investigative purposes[77]. Moreover, as already mentioned, it is the same Delia®'s official website that reports it (see **1.9**. and **2.5.**).

Thus, in this context, it is necessary to recall the problems traditionally related to the AI-based systems: their opacity and the concern related to the so-called black box[78]. On the basis of this, procedural guarantees under Articles 24, § 2, 111, §§ 2, 3, 4, Italian Constitution and under Article 6 ECHR[79], regarding the need to protect the right of defence, the right to confrontation and the equality of arms, are at stake. Moreover, in relation to that, it is also necessary to report the importance of the right to an effective remedy, protected by Article 13 ECHR and Article 47, § 1, CFREU[80].

Finally, in general terms, it also seems crucial to recall the case law developed by the Council of State, although it refers to administrative matters. As already explained, the Council of State has affirmed that AI cannot violate the principles of the Italian legal system[81]. Thus, the judges have established some fundamental principles that must be taken into account[82]. First of all, there are the principles of accessibility and transparency; moreover, according to the Council of State, private companies cannot object to the disclosure of the information concerning the AI-based systems. In addition, the Court has highlighted the prohibition of decisions based solely on the automated processing of data and, as already mentioned (see **2.8.**), the prohibition of algorithmic discrimination.

PART II PREDICTIVE JUSTICE

1. National practices

[74] M. Gialuz, *Intelligenza artificiale*, cit., 58. See also L. Parlato, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Processo penale e giustizia*, 2020, 297 ff.; M. Torre, *Nuove tecnologie e trattamento dei dati personali*, cit., 1056.

[75] G. Padua, *Intelligenza artificiale e giudizio penale: scenari, limiti e prospettive*, in *Processo penale e giustizia*, 2021, 1492; C. Parodi – V. Sellaroli, *Sistema penale e intelligenza artificiale*, cit., 58 ff.; M. Pisati, *Indagini preliminari*, cit., 958.

[76] P. Severino, *Le implicazioni*, cit., 97.

[77] F. Basile, *Intelligenza artificiale*, cit., 13; G. Ubertis, *Intelligenza artificiale*, cit., 19.

[78] P. Severino, *Le implicazioni*, cit., 97.

[79] S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham, 2020, 91 ff.

[80] G. Contissa – G. Lasagni – G. Sartor, *Quando a decidere in materia penale*, cit., 624 ff.

[81] Council of State, sez. IV, 4 February 2020, n. 881.

[82] See, more in detail, J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Rivista di diritto processuale*, 2021, 713 ff.; M. Gialuz, *Intelligenza artificiale*, cit., 66 ff.

1.1. In the Italian legal system there is not a normative definition of 'predictive justice', nor it is under discussion, in terms of drafts or proposals.

1.2. As a consequence, there is no software officially used at the moment for predictive purposes. Nor there are trials or experiments set forth on behalf of the Ministry of Justice. It is likely that research groups, in the academic context, are testing and experimenting computational models for specific purposes of 'predictive justice', but the Ministry has not ordered, endorsed or engaged in possible researches of the kind.

1.3. This does not depend on a specific and explicit decision about the reliability and desirability of 'Quantitative Legal Prediction' methods (like it happened in France), rather on the delay in the discussion about the matter. However[83], one important reference to recidivism risk assessment is necessary here. In Italy, according to art. 220 § 2 of the Code of Criminal Procedure, the psycho-criminological expertise on the defendant's character is allowed only after sentencing, in the correctional phase: it cannot be used either for adjudicating on guilt, or for sentencing. Traditionally, a persisting mistrust in psychology is said to be the main rationale of the norm. However, it seems that the strongest reason for it is, rather, the reluctance to value character in the decision of the case, as the defendant's personal attitudes have no evidentiary value as to the facts of the file. Based on the assumption reported above, an Italian court could not make use of any risk-assessment tool, such as COMPAS or SAVRY, in the guilt and sentencing phase, given the prohibition of art. 220 § 2 ItCCP, as risk assessment reports should be considered and treated as psycho-criminological expert testimonies. Only the judge presiding over the correctional phase could rely on a risk-assessment tool, in order to decide, e.g. on parole or other prison benefits. Incorporated into a file, a digital risk assessment tool delivers reports that are the result of the application of a specific scientific theory, elaborated by scholars or clinicians, tested, verified and criticised by a community of peers. Although a digital tool does not imply the expert's personal presence in court, it delivers a result that is based on a scientific theory, according to the traditional paradigm of expert testimony: the adjudication on a matter of the case entails the application of technical or scientific knowledge, of which the judge is deprived.

1.4. (to 1.14) Given this legal restriction, the psycho-criminological research on judicial risk assessment tools has been limited to the correctional area and the digital turn did not change the situation, due to the absence of a tradition in the field (see however, G. Zara…) and the unlikeliness of a change in the normative framework.

As to the other component of predictive justice, it is to say quantitative legal prediction and tools foreseeing judicial decision, the Italian institutional scheme does not encourage the research. Strongly rooted in the roman tradition, the jurisdiction is not based on stare decisis, and consistency – even in the Supreme Court's decision – is difficult to achieve, due to the wide range of means of appeal provided by the system, in opposition to the most important consequence of the rule of *stare decisis*, i.e. the binding commitment for the courts to respect the precedent, even if it appears wrong or unjust. A diffused organisation of the higher courts is a distinctive feature of many continental systems, such as e.g. in France, Italy and Germany. Usually deprived of the power of *certiorari*, or to select the cases to be reviewed, these courts decide cases in thousands each, per year, and deploy greater numbers of judges, organised in different sections or chambers, adjudicating independently from each other. This hampers the possibility of such courts to focus on their original mission, granting the uniformity of the law. For these reasons, quantitative legal prediction, based on retrieval of precedent decisions, may turn out to be less attractive than in common law countries. By attractive, we mean less useful, due to the scarce binding role of the precedent and also to the reduced reference that the Italian supreme court (and the whole continental tradition) owe to the merits of the fact, rather than to the principle of law. This has an impact on the capability of a predictive software to establish useful and accurate correlations. When referring to a precedent, either in common law or in civil law, the judge

[83] QLP, Quantitative Legal Prediction, is a computational approach. Based on data-driven AI, it implies the use of computational modelling to predict many different aspects of legal cases, or potential legal cases, moving from whole collections of existing data. According to the scholar who largely promoted it «QLP-based are designed to remedy or supplement the shortcomings of human reasoners» (D.M. Katz, Quantitative legal prediction or how I learned to stop worrying and start preparing for the data-driven future of the legal services industry, in Emory Law Journal, 2013, p. 928). When referring to predictive justice, literature usually encompasses software to specifically predict the outcome of case or, in criminal law, the risk of recidivism.

applies a form of analogy, comparing a certain number of variables, on the basis of which a precedent can prove relevant for the solution of the pending case. Within a computational model, the number of factors, variables, involved in the decision-making process is crucial: it can be established *ex ante*, and once for all, e.g. in expert systems; or, in machine learning, it can be left to the training set, during which the system will be fed with a sufficient number of decisions, to allow it to recognise the relevant variables: the factors selected during the training set, will be applied in the predicting set. In criminal case, variables are many, both substantive and procedural (with specific regard to evidence admission and evaluation) and this hardly affect the possibility to release 'predictive software'. AI solutions are used in the most popular case-law data base, such as the Supreme court one (Centro Elaborazione Dati Corte suprema di cassazione [www.italgiureweb.it]) and DeJure, by the publisher Giuffré, which are, however, traditional – although sophisticated – data base retrieved with different set of keywords. Quantitative legal prediction tools are unavailable in criminal justice both to the judiciary and the public, so there are no trends of alternative dispute resolution in this context.

1.15 The attention of both scientific literature and media to quantitative legal prediction, or predictive justice is scarce. As to the literature, the topic has recently (last two years) started to be treated as a matter of academic research. As to media, they tend to ignore this aspect, given the absence of a practical application, while they tend to highlight any possible achievement in predictive policing.

Assessment of reliability, impartiality, equality, adaptability

1.16-1.23 Given the framework above, the answer to this sub-session is generally negative. At the time being, there is a huge on-going reform of criminal justice. The process started in Spring 2021, in relation with the Next Generation EU fund. The Government's engagement in a profound reform of the Italian justice system has been crucial in the negotiations. In particular, with regard to criminal justice, one main endeavour is the strong reduction of the length of proceedings, especially appeals. The Ministry of Justice appointed an expert committee to draft a 'delegation law' (piece of secondary law, passed by the Parliament, delegating the Government to implement the principles established by the law itself), and a second committee, in charge of drafting the implementation. Both rapporteurs were appointed in both committees and worked at the implementation draft, which was fialised by the Ministry of Justice and entered into force on December 30th 2022.

One point in the reform (D.lgs. 150/2022) is 'digitalisation of criminal justice'[84]. However, in the principles established by the delegation law, there was no specific reference to predictive justice, rather to a more basic profile of digitalization. This means, in first instance, transforming the file into a digital one, something that has not happened yet, in Italy. It will imply using digital resources for summoning parts and depositing acts in the file, at any stage of the proceeding, transforming notifications and deposits into a system of on-line, certified, exchanges. Although other countries may have experienced such transition years ago, this will be a huge challenge for the Italian system. Firstly, such transition underpins effective and reliable digital infrastructures, allowing both judiciary and private parties to access and take advantage of the digital systems. Italy did not invest enough in digital infrastructures in the past decades and does not deploy the same effective resources in every part of the country: there are areas which are not covered by reliable, fast and regular digital services 24/7. Secondly. A digital file implies secure IT systems, guaranteeing both authenticity and privacy of communications: adequate subsidiaries must be provided for, in case of misfunctioning of IT systems, not to jeopardise the chain of acts of the proceedings. This is the basic level of engagement at which the commission is working at the moment, with no attention with further, specific aspects of predictive justice. However, it is possible that, in the future, there will be an engagement of the Ministry of Justice into the endeavour of predictive justice. It is our opinion that the topic will be studied and analysed at a governmental level. As the topic is gaining momentum in public funded research[85] calls, it is likely that, in the future, the Ministry of Justice will monitor the research process in order to understand the effective qualities of quantitative legal prediction (in terms of consistency, neutrality, equality, as mentioned by this section of the questionnaire) and the advantages, if

[84] B. Galgani, *Forme e garanzie nel prisma della innovazione tecnologica*, WKI, 2022.

[85] See, e.g., G. Lasagni; G. Contissa, M. Caianiello, G, Sartor, *Effective Protection of the Rights of the Accused in the EU Directives. A Computable Approach to Criminal Procedure Law*, Brill, 2022.

any, that this may bring to the Italian justice system. In these terms, a full public engagement in the discussion is desirable: not only public funded research, but public monitored research, because of the dramatic impact of digitalised judicial decision-making process on the basic features of society. A massive usage of automated decision-making process in criminal matters may affect every aspect of the institutional structure of justice, from independence of judiciary to the concept of predictability and certainty of criminal law: for these reasons, there should be no room for private investments and research in this field, rather a publicly regulated and monitored system. In this sense, the limited experience in other fields of public administration (see 2.6), suggests the need for transparent process of commitment, development and application of AI solutions in public administration, in order to fully realise the purposes of a good and fair public administration, which is enshrined in art. 97 of the Italian Constitution.

2. Normative framework

Law and soft law

2.1.-2.4. As it has already been said (see 1.16.-1.23.), at the moment, in Italy, there is no legislation or normative instrument produced by executive authorities on predictive justice, nor its introduction is really under discussion, even in the context of the current efforts towards digitalisation.

However, from a general perspective, legal rules concerning right to privacy and data protection are relevant in this field, due to the fact that the systems at issue involve a massive treatment of personal information. For this reason, Legislative decree n. 51 of 2018, implementing EU Directive 2016/680, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, comes into consideration.

As far as the legal principles established by these sources are concerned, it is possible to recall what has been observed with reference to predictive policing (see I, 2.1.-2.3.). Nevertheless, in this context, the ban on decisions based solely on automatic processing – already mentioned in the first section – is particularly important. As said above (Section I, 2.1-2.3.), Article 8 of Legislative decree n. 51 of 2018, implementing Article 11 of the Directive, prohibits this kind of completely automated decisions, including profiling, which produce an adverse legal effect concerning the data subject, unless authorised by European Union or Member State law to which the controller is subject and which provides for appropriate safeguards for the rights and freedoms of the data subject. According to a strict way of interpreting the norm, it requires not only a human contribution to the decision, intended as an effective and significant control on the machine output, but also the imposition, to a human judge, of the evaluation of further evidence, different from the machine output, as a basis of any decision[86].

The «user under control» principle and the need for a critical approach towards the algorithm output, at the European level, in also expressed by the European Commission for the Efficiency of Justice (CEPEJ)'s European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, as well as by Article 14 of the European Commission's proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence.

Moreover, Article 8 of the mentioned Legislative decree prohibits automated decisions based on the sensitive personal data listed in Article 9 of GDPR, unless specific measures aimed at protecting the individual's rights and liberties are adopted. In any case, according to the same disposition, a discrimination of persons by the use of profiling based on this kind of information can never be admitted.

Finally, even if, to our knowledge, no specific soft law source concerning predictive justice has been published yet, it is possible to mention, even in this field, the already cited AgID's White Paper on Artificial Intelligence (Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino), of 2018 (see Section I, 2.1.-2.3.).

Regarding the implementation of international sources, for the reasons explained above, it is important to recall the implementation of EU Directive n. 680/2016; moreover, it is necessary to mention Articles 7

[86] M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Diritto penale contemporaneo*, 29th May 2019, 16-18.

CFREU and 8 ECHR, concerning the right to respect for private life, and Article 8 CFREU, on the right to data protection.

Moreover, as it will be said below, other supranational principles come into play regarding predictive justice, as specific profiles of the fundamental guarantee of the access to a human judge, implicit in the provisions of Article 6 ECHR and of Article 111 of Italian Constitution, on fair trial (see 3.3.).

With specific reference to risk assessment tools in the field of personal liberty, Article 5 ECHR establishes two significant aspects of this right: first, the right to be conducted promptly before a human judge; secondly, the right to an effective control on the legitimacy of the restriction of personal liberty, within an adversarial procedure, which should involve the defence's access to the functioning of the algorithm[87].

Moreover, as it will be explained below, either supranational and internal sources establish the principle of foreseeability of law, provided for by Articles 7 ECHR, 49 CFREU and 25 of the Italian Constitution (see 3.9.).

Case law

2.5. Criminal tribunals or courts haven't been confronted with AI-based systems used for predictive justice.

2.6. To our knowledge, the same can be said about the civil and the constitutional courts, or about other independent authorities: none of them has issued decisions concerning this subject. However, the conclusion is partly different as regards the administrative courts. In fact, it is worth noting to recall the case law of the Italian administrative supreme court, the Council of State, which emphasizes the need for AI-based systems to respect the fundamental principles of the Italian legal system (see Section I, 2.8. and 3.6.). Despite the fact that these judgements specifically refer to administrative decisions, they seem relevant due to the general scope of their assertions. According to the Italian judges, a procedure involving AI should not be stigmatized, but rather, in principle, encouraged: it has many advantages, such as, for example, the significant reduction in the time frame for purely repetitive and discretionary operations; the exclusion of interference due to negligence of the competent person and the consequent greater guarantee of impartiality of the automated decision[88]. However, recalling what has been said in the first part of this report regarding predictive policing (see Section I, 3.6.), the Council of State establishes that using artificial intelligence must be in line with certain fundamental principles: the principles of accessibility and transparency, the prohibition of decisions based solely on the automated processing of data and the prohibition of algorithmic discrimination (see also, *infra*, 3.8.). Thus, an important conclusion can be drawn from this position. If the Italian legislator decided to introduce risk assessment tools in the criminal area, these principles would prevent him from adopting tools similar, for example, to the well-known AI-based system COMPAS, which is clearly in contrast with the principle of transparency. Finally, the statements of the Italian administrative supreme court have been warmly welcomed by legal commentators, arguing for the extension of these *dicta* to criminal matters as well[89].

Substantive guarantees

2.7. In light of what we reported above, in Italy specific legislation about the reliability, impartiality, equality, and adaptability of AI-based systems used for predictive justice is absent. Anyway, it is important to once again draw attention to the case law of the Italian administrative supreme court about using AI in the decisions adopted by public administrations in administrative matters. As already observed, the guarantees elaborated by the Council of State may constitute a significant barrier to the use of AI-based systems used for predictive justice that contrast with the above-mentioned fundamental principles. This conclusion appears relevant even concerning criminal proceedings.

2.8-2.18. Given that there are no tools officially used for predictive justice in the Italian legal system at the moment, the answers to the other questions related to this sub-session are negative or not relevant.

3. General principles of law.

[87] See M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale,* cit., 14-15.

[88] Council of State, sez. IV, 4 February 2020, n. 881.

[89] See J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *Rivista di diritto processuale*, 2021, 724 ff.; M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milan, 2021, 66 ff.

3.1. At the time being, the Italian society is not ravaged, like others, by issues of discrimination. Due to many social factors, public opinion's complaint about justice do not focus on discriminatory aspects, rather on the time-consuming process of it, inducing a strong feeling of ineffectiveness. However, if there is an aspect of predictive justice that has captured the interest of a small part of the literature, that is exactly the risk of discriminatory practices hidden behind the black box of predictive software. Against the backdrop of several, serious problems in the functioning of our criminal justice system, what is certainly accepted and widely recognised is that the current code of criminal procedure offers wide room for discussion and confrontation between the parties, based on a strongly rooted adversarial scheme, especially with regard to the first instance decision. For these reasons, reading about the Loomis case, ruled by the Supreme Court of Wisconsin some years ago, set the spotlight of a part of the literature on the unprecedented risk of importing implicitly discriminatory software and practices to be used in criminal proceedings. The topic of risk assessment immediately echoed the season of the Lombroso's theories, also based on discriminatory beliefs, enhancing a strong reaction of mistrust. However, for the many reasons explained above, the feeling is that of observing a phenomenon which goes on abroad, with no serious repercussions on our legal system.

3.2. A burgeoning case-law of the ECtHR established that the fundamental guarantee of judicial independence is multifaceted. It implies different layers of action, both external and internal to the judiciary, objective and subjective. As also the Italian contemporary history demonstrates, the most dangerous external incursion into judicial independence is represented by other public powers and authorities. Nevertheless, also private interference in the function may be detrimental and thus, contrary to the Convention. In fact, social constraint is a negative factor impinging on judicial independence, regardless of the form that it holds: a large-scale access to 'prediction' can be a serious risk for constraint over the judge, who would feel 'encouraged' to follow the normative force of numbers… And this would have an impact also on the internal side of independence, even in legal systems which are not based on the *stare decisis* rule. The ECtHR has stressed the importance that the organisation of each judicial office allows each individual to perform her task without being influenced by other judges, from higher courts or from the same court: in particular, the Court endorsed the freedom of a judge from her peers' influence (ECtHR, Findlay v. UK, 25.2.1997). Pushing judges to use and follow the 'prediction' would mean to constraining them into the respect of the decisions taken by other judges, that – due to the public opinion's expectations - they should feel forced to comply with. The intensity of the constraint could vary, according to the position taken by each institutional context: from a bare moral-suasion to a precise disciplinary duty to follow the prediction, clearly impinging on the independence of each single judge, in case a legal order should recognise in case-law consistency a superior interest in the administration of justice.

3.3. The right to access to a human judge has not been formalised yet because it can be considered an implicit premise of the whole range of guarantees of the fair trial. Moving either from art. 6§1 ECHR and art. 111 §§ 1-3 of the Italian Constitution, the whole theory of the prerogatives of the fair judge is implicitly based on a human judge. All notions of 'tribunal', 'independence', 'impartiality' have been elaborated by the ECtHR (and by national constitutional courts) on the basis of a function performed by humans. Even the most recent analysis of the Strasbourg case-law demonstrates that the court takes it for granted that such prerogatives play their crucial role in a context in which judiciary is human. Probability, doubt, conviction, are all processed by the human intuition, the human comprehension of the facts, and the reasoning of the decision grants accessibility to that process. As a consequence, the centre of the discussion should be whether a non-human decision is a judicial decision at all. I personally doubt. While it is important to study if and how automated decision systems may improve the real problems of criminal justice, it is crucial to recognise that, although assisted by a sufficient range of guarantees, automated decisions will not be judicial decisions, leaving room for an appeal to human courts.

3.4. Given the general ban of psycho-criminological expertise in the judgement upon the merits, digital risk assessment tools could be used in Italy only in the correctional phase, it is to say after the conviction became final and the presumption of innocence has been defeated for good.

3.5 As to the right to a fair trial, it is suitable to move from one specific feature of quantitative legal prediction, or predictive justice. In my book I tried to demonstrate that quantitative law predictions (QLP) works on the basis of correlations established between a pending case and previous decisions in similar cases. Setting aside the traditional discussion, in the common law, about the concept of similarity between two cases, I tried to list a very general list of variables that are imping on a decision in criminal cases. The relevant variables can be divided into: i) ***substantive*** and ii) ***procedural***. The substantive variables can be distinguished into: a) *material* and b) *legal*. The material variables refer to: a1) factual (*actus reus*) and a2) subjective (*mens rea*) elements.

i) Substantive; a) *material*; a1) factual variables:

-the conduct
- the subsequent natural event
- causality
- the circumstances of the case, aggravating or mitigating
- in case of attempt (or other forms of inchoate offence), the stage of development in the action

i) Substantive; a) *material*; a2) subjective variables:

- *Mens rea* (bearing in mind that different legal systems provide for different classifications of *mens rea*)
- Liability
- Complicity (in some jurisdiction, like the Italian e.g., complicity refers to the material aspect and not the subjective one)
- Propensity towards crime

i) Substantive, b) *legal* variables:

- *Nomen iuris*
- Any legal condition impinging on the sentence, such as recidivism and other forms of habitualness in re-offending
- Statute of limitation (usually depending on *nomen iuris*: e.g. classifying the facts under a different *nomen iuris*, the statute of limitation may not occur)
- Continued or concurrent offences.

ii) Procedural variables are much more complicated to list. Although not the only relevant aspect, the evidence process is the factor that most affects the possibility to establish relevant variables, to build up useful correlations. All the elements listed above must be appreciated on the basis of evidence provided by the parties (although many European legal orders recognise the judges *ex officio* power of introducing decisive evidence): based on such evidence, the judge must reach conviction beyond any reasonable doubt, on each of the listed points. However, the whole evidence process relies on discretional judicial evaluations. It is highly debatable that a quantitative computational model can grasp useful correlations in the realm of assessing reliability beyond any reasonable doubt, not only because of an intrinsic limitation of AI techniques. In fact, in this field, establishing similarities between different cases is particularly complicated, because the factors listed above are discretionally weighted by the judge, in each case. For instance, comparing two cases from the standpoint of the judicial evaluation of mitigating and aggravating circumstances may prove pointless: given the same circumstances, judge 1 may consider the aggravating circumstances predominant, while judge 2 may reach the opposite conclusion. And, although a machine learning system is trained to learn from previous errors, there are no right or wrong decisions, but only decisions giving different, discretional interpretation of the same factor.

As to the procedural aspects, selection and admission of evidence is the first step of a crucial process that will bring the judge to 'establish the truth', in the adjudication of the case. Every legal order provides for different criteria to admit evidence, and it is difficult to generalise. However, it is possible to argue that, all over the world, the courts' activities must orient the fact-find towards the truth, encouraged to pursue these basic goals through admitting and taking into consideration any evidence that appears to be factually relevant for the disposition of the case. 'Relevance' is a multi-fold concept that not only undergoes the typical process of a discretional evaluation, but can vary significantly, depending on the stage of the procedure in which it is applied.

Moreover, criminal evidence evaluation is a factor that seriously impinges on the effectiveness of a computation model. In fact, evidence in criminal proceedings is still mostly oral. Documents are valuable and frequently used as evidence, of course; however, witnesses and expert-witnesses are key evidence in the majority of the cases. The evaluation of the accuracy, reliability and relevance of each piece of evidence is crucial in the decision of a case and cannot be standardised into a computational model. Based on very similar factual elements and evidence, two cases can be decided in different ways, because of a different evaluation of reliability and accuracy of a witness or expert witness.

For these reasons, the whole discussion about the risk of jeopardising the right to a fair trial must rather concentrate on the question whether a QLP process is a trial at all. In fact, as demonstrated, a trial needs to take into account a long list of variables. **A reliable automated decision-making process based on QLP can be conceived exclusively in relation to simple cases, in which the number of the variables at stake, both material and procedural, are extremely limited**. Outside these boundaries, there cannot be the illusion of accomplishing the task of a trial, nor fair, neither unfair: the number of variables and the subjectivity in the evaluation of such variables exclude that QLP can perform the same task and functions of the trial. If the number of variables is extremely reduced and the consistency of the case law is extremely high, QLP may possibly perform a coincident function, delivering a result which may satisfy the parties, but that, according, to 3.3., is not a judicial decision and should be likely to be submitted to a court for a human review.

3.6. Given the absence of currently used QLP systems, the effectiveness of the right to defence has not been discussed in practical terms, so far. However, the most basic idea of right to defence implies the defendant's right to give arguments upon each of the variables that have been listed in 3.5. The basic idea of equality of arms elaborated by the ECtHR (see Martinie v. France) implies that every part of the trial must be in the condition to convince the judge upon her reconstruction of the facts. It is arguable whethe predictive systems may comply at all with this basic principle.

3.7 The matter does not change in terms of appeals. Appeals are meant to be solutions against judicial errors and, insofar, they must allow the parties to convince the court of their reconstruction of facts, against a first instance decision that came to wrong conclusions. In this sense, the right to appeal, as a refined aspect of the most general right to defence, would be totally illusory in a process in which a real second instance judgment would not be allowed, like in the case mentioned by the question, of using the same AI system.

3.8 Without lingering over aspects that will be analysed in Section III, it is crucial to reflect on whether and how it is possible to assess the reliability of data and the correctness of a calculation generated by a digital system. The Italian administrative supreme court (Consiglio di Stato) has recently recognised the right of those who suffer the effects of an algorithmic public decision to get a review on how the algorithm works and what the datasets used are (Consiglio di Stato: Sez. VI, 8.4.2019, n. 2270; Sez. VI, Sent., 13.12.2019, n. 8472; Sez. VI, 2.1.2020, n. 30; Sez. VI, 4.2.2020, n. 881). Although this position is not referred to judicial decisions, it appears to be a paradigm for algorithmic decision taken, at any level, by the public administration. With more specific regard to criminal proceedings, given that the minimum standard of the equality of arms is the chance to "effectively influence the court's decision", what if the defendant claims that the impossibility to assess the reliability of an automatedly generated piece of evidence deprived her of the chance to "effectively influence the court's decision"? In my opinion, it seems compliant with the principle of the equality of arms that the court discharges such automated calculations. Given that, in many cases, technology can provide sufficient validation of automated process, when *ex post* validation is not available, the court should exclude the results of that process from the adjudication on the defendant's guilt, in order not to violate the basic expression of the fair trial, the equality of arms.

3.9. As said above, predictive justice is arguably compatible with several constitutional principles and, in particular, independence and impartiality of judiciary, but also, in my opinion with the foreseeability of criminal law, which is provided for by art. 25 of the Italian constitution, art. 7 ECHR, and art. 49 CFREU. With specific regard to this aspect, the guarantee of foreseeability acknowledges that if the individual is not in the position of understanding what the criminal law imposes or bans, her compliance with the law cannot be expected. Actually, inconsistency in the judicial interpretation of a criminal command can affect the foreseeability of what is legitimate and what is not. It was said that the foreseeability of the legal consequences of our actions is one of the dimensions of legal certainty. More precisely, certainty guarantees that individuals, before acting, can foresee these three aspects: whether their conduct will be considered legitimate; if illegitimate, whether it will amount to a crime; what punishment they may undergo. Insofar, predictive justice seems to improve and foster certainty and foreseeability of criminal law, reducing the risk of inconsistency in the case-law. However, even under a semantic aspect, the distinction between fore-*see* (pre-vedere, in Italian) and fore-*tell*, (i.e. to pre-dict, based on etymology, pre-dire, in Italian) is based on the same difference between 'foreseeability of the criminal law' and 'predictive justice'. The fundamental right of legal certainty, established by the main bills of human rights in the world, is a guarantee of accessibility, comprehensibility, awareness that people must have of the penal consequences of their behaviours. The interpretation by the Strasbourg Court reiterates that it is a matter of cognitive comprehension, the complexity of which implies the suitable intervention of a counsel. On the contrary, 'predictive justice' is not aimed to clarify the meaning and the comprehension of legal precepts, but to predict the outcome of a potential litigation. It is a prediction of the success rate of an action and not an instrument to clarify the interpretation of the law. In this sense, such instruments are not supposed to foster the principle of legality and the accessibility of the criminal precept. Rather, they are about the personal expectation about the decision in each specific case, and this is much different from the core guarantee protected by the principle of legal certainty. Far from enhancing legal certainty, predictive justice appears to reduce or exclude the individualisation of the judicial response: individualisation is crucial not only in sentencing but throughout the whole criminal proceedings. The result of a judgment *must* depend on the peculiar circumstances of each case, otherwise other fundamental rights would be violated, such as art. 6 ECHR, as said above. Predictive justice can seriously jeopardise such right.

3.10 Some have argued that applying a computational model based on precedent decisions of a court means to *predict* the decision in a new case. In fact, what QLP can do is to provide accurate calculation of how a court or a judge decided in previous cases on a similar claim. Looking at the achievement in AI from the legal point of view, it has been said that the best that the modelling of judicial decision can do, so far, is to give a model of the possible different solutions to a legal problem, as it has been observed. As a consequence, such programs can express probabilities, even high probabilities, that the court will stick to the precedent (especially in a common law jurisdiction), refusing to distinguish or to overrule, or that it will follow the mainstream interpretation, rejecting the more eccentric one (in a civil law jurisdiction). Thus, it is undisputed that the first step to address the matter of 'predictive justice' is to abandon the (dystopic) idea of a machine being able to predict the outcome of a future decision, that is to say, being able to decide: such a process delivers probabilities, based on what has occurred in the past and no serious scientific approach can use past events to build previsions of the future. As said, it is still the case of a law machine 'to inform', rather than a law machine 'to decide'. Given the undisputed value of statistics in hard science, it has been said that the application of probabilities to human activity is non-sensical, as it is governed by uncertain rules and factors, constantly changing over the time. These remarks seriously impinge on how the purported 'accurate numbers' of QLP can be used. As an example, in many legal orders prosecutors have discretional power to drop cases they are not interested in. Within such a framework, the judicial statistics completely overlook the cases dropped by the prosecutor, either because of an 'immunity bargain', based on a deal between the suspect and the prosecutor, or other discretional evaluations. Such cases escape a complete review of precedents, as they do not even reach the trial stage. For these cases there is no judicial decision and thus they are completely overlooked by the software. This has a great impact on the reliability of the results of 'predictive justice tools'. Moreover, the case outcome depends, in the reality, on how the parties express their arguments, on the evidence they bring, on the application of procedural rules based on incidental conditions. Although modern techniques of natural language processing have reduced the gap between human and digital processing in the realm of semantics, the distinction between syntactic and semantic elaboration is still crucial. Traditionally, data is syntactically processed, while information is semantically processed: digital agents outperform human agents in syntactic analysis; humans excel in semantics, while digital technologies are not able to process data with a semantic function. Given that natural language processing has been at the centre of AI and law research, since the very initial stages and the achievements in such a field have been great, it is still really hard to establish similarities between different cases, due to the hindrance of such a semantic gap, provided that, in law, there is no 'application', rather 'interpretation'. For these reasons, the epistemological discussion has still to reach its higher level: the most recent literature opened the floor for such discussion, which will be enlarged and enriched, also in Italy, in the next decade.

3.11 Against the backdrop of the current situation, in Italy there is no discussion about the risk of privatisation of criminal justice. Given the large space devoted by the Italian constitution to Justice (under the point of view of judiciary recruitment and organisation but also of the basic guarantees of the jurisdiction), I do not see real risks in this sense.

3.12 For several reasons, income impair is in many countries a divide between effective and ineffective defence and in Italy as well. Predictive justice seems to be able to rephrase this axiom into expensive and inexpensive justice, forcing those unwealthy to accept the consequences of automated and possibly unfair justice, while wealthy ones may have the chance to access to more expensive human justice. The risks have been listed above and it is certainly not desirable to leave the floor for such a scenario. This remark reinforces the wish that: 1) predictive justice is narrowed down to few offences, in which: a) the number of variables to be examined is extremely limited; b) cases are repetitive and the judge's individual intuition does not play a relevant role in the decision; 2) predictive justice is used only with the purpose to tackle the backlog of cases: in this sense, given the defendant's right to appeal to a human judge, the automated solution of the case is acceptable as an alternative to the relinquishment of the file, that would consist of a patent denial of justice.

PART III. EVIDENCE LAW

1. Evidence gathering through AI-based systems

1.1. Italian law enforcement agencies (LEAs)[90] use AI based tools to retrieve large data sets. There is no specific normative regulation of such tools, nor explicit description of their features. Newspapers often report this kind of news, with no specific description of the technical features of software. E.g. Molecola, is a software used by Guardia di Finanza (LEA depending on the Ministry of economic and finance, performing duties of judicial police).

1.2. Performing their investigating duties (both independently or under the guidelines of the prosecutor), LEAs can extract data from mobile devices and decode and analyse that data in their own laboratories or, rather, appoint computer scientist in digital forensic to extract data.

1.3. Moreover, LEAs use wide range of malware (malicious software) which may be based on AI applications, mainly to intercept images, conversations, screen shot and other row data. This turned out to be a very fruitful system of investigation, which is only in part regulated by the code of criminal procedure, leaving much room for 'free application'…

1.4. In fact, the only regulation is currently provided for the use of malware in cases of interceptions. The criminal procedure code has been recently amended, introducing a procedure which is similar to the traditional interceptions (art. 266 ff. Code of criminal procedure). The use of malware is mainly located during pre-trial investigations for a list of specific crimes (mainly organised crime and some white-collar crimes) and is based on the prosecutor's duty to ask for authorisation by the judge for preliminary investigations. The judge must set the specific reasons and conditions for using the malware: in particular, the judge must establish in advance the period of time and the locations in which the malware can be activated. The legal framework does not authorize or rule out the use of AI to operate the malware.

[90] The activity of investigative police are carried out, in Italy, by three main different corps: Polizia di Stato, non-military, depending on the Ministry of Home Affairs; Arma dei Carabinieri, military, depending on the Ministry of the Defence; Guardia di Finanza, military, depending on the Ministry of Economics), but there is no specific regulation or procedure, based on the specificity of the AI tool used.

1.5. Against this backdrop, unfortunately, there are no specific provisions to let the defendant understand the technical features of the digital tool used in the investigations.

1.6. The topic has not been addressed comprehensively yet, nor by the literature, neither by courts. To our knowledge, as to criminal cases, there are not leading cases at the moment.

1.7. Scholars are certainly in favour of regulating this area. On the one hand, specific criticism was deployed against the recent reform about the use of malware for interceptions. As explained above, the regulation establishes unrealistic duties upon the judge, who should be able to establish, in advance, when and where the malware can be activated: not only this provision is difficult to realise but it implies that a human follows 24/7 the location of the device intruded by the malware, activating and de-activating it, on the basis of the judicial decision. The literature about the use of malware is huge, with a certain number of monographs dedicated to the topic[91].

On the other hand, as to the literature more specifically dedicated to AI-based systems, there have been some comprehensive overviews on the matter, with both a book and several articles.

2. Evidence produced by AI-based systems

2.1. As in the majority of the countries, in Italy LEAs use facial recognition systems for investigations. From 2017, the Italian Scientific Police Department has acquired SARI, "Automatic Image Recognition System", an automated face-based human recognition software, for the purposes of the prevention, investigation, detection and prosecution of criminal offences or the enforcement of criminal sanctions. The technical specifications of the contract presents two operating scenarios, "Enterprise" and "Real-Time". The first is one in which an operator needs to search for the identity of a face in an image, using one or more facial recognition algorithms, within a large database. For the "Real-Time" scenario, the system is able to analyse in real-time the faces of subjects captured by the cameras installed there, comparing them with a watch-list whose size is 'in the order of hundreds of thousands of subjects. After the negative opinion by the Italian Data Protection Agency on the use of "real-time" modality by law enforcement authorities(https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842), currently Italian Police uses only SARI Enterprise system. Facial images are stored in AFIS-SSA System (Automated Fingerprint Identification
System and the subsystem of the investigative activities).

Very recently, with law no. 205/2021, the Italian Parliament adopted a controversial approach for the regulation of the use of automated facial recognition systems by law enforcement authorities, showing a clear lack of awareness about the different levels of complexity in this matter[92].

With regard to the voice recognition, the Italian Scientific Police Department uses automated and semi-automated systems, allowing a faster analysis of the physical characteristics of the voiceprint. The technical analysis is divided into three different operational phases. First of all, the operator must choose the phonic material. Secondly, special programmes - IDEM and SMART, in Italy – isolate some parameters for the characterization of the voice. The final phase consists in a statistical interpretation of the data and a comparison made between the measurements obtained, in order to establish the compatibility between the anonymous voice and that of the known subject. At the current state of knowledge, there is no system capable of capturing, simultaneously, all the characteristics of a voice. A voice database does not yet exist, although Italy is currently collaborating in the Interpol 'Speaker identification integrated project' to create a large database of voice tracks.

[91] See at least F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria*, WKI-CEDAM, 2020; M. Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017.

[92] In particular, the bill introduced a "moratorium on the use of facial recognition systems in public places or places open to the public [...] until legislation is adopted which ensures full respect for citizens' constitutional rights, in accordance with the indications of the national and European authorities for the protection of personal data. However, such moratorium does not apply to «public authorities» (which an extremely broad definition), operating under the purpose of preventing or prosecutions crimes or applying final convictions. Moreover, an explicit exclusion of the moratorium is provided for the judicial use of face recognition systems, regardless they are 'real time' or not.

2.2. The extensive use of digital devices (often incorporating AI systems) in the everyday life of the whole world's population, has created a completely new range of data that can have decisive impact on criminal investigations and trials. In addition to 'digital evidence' (i.e. sources of information being specifically regulated for trial purposes), non-specifically regulated sources can convey crucial knowledge for criminal proceedings. Such knowledge is not based on secure protocols, because it is not conceived, unlike digital criminal evidence, with the specific purpose of being used in trial. Such knowledge usually derives from data processed for generic or commercial use, such as home assistants, IoT, or other AI devices, used for a variety of human activities. This second kind of information poses major challenges, as it can make its way to the courtroom, mainly as a document.

2.3. Based on the Budapest convention, digital evidence has gradually conquered its own autonomous standing, thanks also to the contributions of the doctrine, which has tried to elaborate a specific statute.
Without being able to go into detail on this issue, it can certainly be said that by 'digital evidence' we mean the cognitive data extracted from an immaterial substrate that derives from the application of specific methods of extraction and conservation, designed and established by the legislator to guarantee authenticity, inalterability, reliability. The digital evidence, therefore, is a cognitive datum, made available to the judge, due to its specific and controlled origin: it exists in as much as it derives from the application of a 'probative procedure' provided for by law, with the aim to guarantee its reliability. On the contrary, automated generated evidence are pieces of information deriving from digital devices which are not generated with the specific purpose of being used with probative effect in criminal proceedings. Currently they are generated by devices which have mainly commercial usage. Insofar, their access to trial is not regulated by Italian law. My personal proposal is to distinguish between digital evidence and automatedly generated evidence and to apply a double test: first, of their specific demonstrative potential; second, of the transparency and explainability of their genesis.

2.4. So far, there is no specific regulation of automatedly generated evidence. Usage in court is submitted to the application of traditional evidence rules. In particular, art. 189 c.p.p. deploys a useful test, measuring the effective demonstrative potential of an automatedly generated evidence. In advocating such demonstrative potential, parties are forced to elaborate upon the transparency and the explainability of the automated process that generated the information that they want to use as evidence. Thus, an adversarial debate can arise between defense and prosecution.

2.5. Challenging the automated generated evidence depends upon the effective possibility to have an adversarial debate upon the process that generated the information itself. For this purpose, two elements are crucial: transparency, which is a feature of software, enabling a technical access to the coding of software; explainability, which is a feature allowing for an (even) non-technical representation of the process leading from input to output.

2.6. As to the distinction between digital evidence and automated generated evidence, see under 2.3.

2.7. Given the backdrop of the current evidentiary law in Italy, daily usage of commercial devices based on AI solutions is a main source of information that may be considered and used as evidence in court.

2.8. Based on the previous remarks, it seems to me that, being 'non-typical pieces of evidence' (meaning non-specifically regulated by the law, see under 2.4) automated generated evidence must undergo the test of art. 189 c.p.p. As said, such test is meant to assess the intrinsic demonstrative reliability of a piece of evidence. Generally speaking, such assessment is done, once for all, by the legislator for the typical pieces of evidence (listed and regulated by the law): for 'non-typical' pieces of evidence, such assessment must be repeated in each proceeding, with regard to the specific context of the case.

2.9. As a consequence of the previous remarks, automated generated evidence should be excluded if it does not meet the requirements of art. 189 c.p.p.

2.10. As to digital evidence (in the sense specified above) Italy is of course party to the Budapest convention on Cybercrime and to Convention 108+ both by the Council of Europe. However, it is worth underlining that such documents do not affect the area of admissibility of evidence. Currently Italy is involved, through the ministry of foreign affairs in the feasibility of a framework regulation of AI, held by CAHAI.

2.11. It does not seem that, at the moment, there have been decisions upon the usage of AI generated evidence (in the sense specified here above) in criminal matters.
Face recognition systems represent a specific area in which the Supreme Court delivered some interesting decisions: Cass. pen., sez. IV, 18 June 2019, n. 39731; Cass. pen., sez. I, 21 July 2020, n. 21823, applying the 'sole or decisive evidence' test: the Court excluded that facial recognition can be the sole or decisive piece of evidence to apply pre-trial coercive measures.

2.12. The academic debate is gradually growing around the different issues at stake. For instance, the concerns about facial recognition have been (and are being) thoroughly investigated[93]. Other scholars are focusing on the quality of information produced by AI-based wearable devices.
More general approaches to the category of AI-generated evidence have also produced interesting results, which have been published both in books and papers[94].

3. Evidence assessed through AI-based systems

3.1. As to the admission of evidence, art. 188 c.p.p. establishes a limitation, excluding methods and techniques which may impinge on the individual's free will and memory. Polygraphs, hypnosis, and similar techniques have been banned from the system, as a consequence of this provision. Thus, the application of digital tools meant to assess reliability, trustworthiness and other qualities may incur into the same limit. However, it is worth noting that there have been some isolated applications of IAT tests, meant to assess witnesses' reliability and of fMRI, meant to measure, based on neuroscientific theories, *mens rea*. While fMRI is a common diagnostic instrument, showing the areas of human brain activated during common daily tasks, IAT, also based on recent neuroscientific research, is an instrument tailored to assess the personal trustworthiness: is a reaction time-based categorization task that measures the differential associative strength between bipolar targets and evaluative attribute concepts as an approach to indexing implicit beliefs or biases.

3.2. As said under 3.1., reporting of instruments which are not necessarily based on AI, the assessment covers only one specific piece of evidence, in particular testimony.

3.3. As to the evaluation of evidence, the Italian code of criminal procedure establishes the judge's full freedom of evaluating evidence according to her own conviction, given the duty to give reasons explaining why the inculpatory evidence prevailed over exculpatory one. In this sense, digital tools for the evaluation of evidence may seriously hamper the ability of providing full reasoning and explanation of the evidence assessment, due to their nature of black boxes.

3.4. As a consequence of the reported scenario, in Italy, at the moment there are no rules (or drafts of normative instruments) on using AI-based systems for assessing pieces of evidence or for assessing the culpability of a person during a criminal trial.

[93] See ftn. 92.

[94] For further references, please see S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, 2020.

3.5. As said under 2.11, the cases decided by the Courts are related to biometric recognition. As to the concept of 'AI-based system', the terms seems to be too general, as far as AI solutions may be integrated into traditional digital tools, such as search tools.