Legal Considerations on Predictive Policing Based on Italian 'Algorithmic Administration' Principles

by

Stefano Rossa*

CONTENTS

Abstract

In Beck's current risk society, the State is faced with a dilemma – fail to prevent the risk from materializing, but to keep the sphere of citizens' rights intact; or not to fail, but to restrict fundamental rights? Striving for a balance turns out to be

* Assistant Professor in Tenure Track of Administrative and Public Law, University of Eastern Piedmont, Vercelli, (Italy); email: stefano.rossa@uniupo.it; ORCID: https://orcid.org/0000-0002-2037-8102.

Suggested citation: Stefano Rossa, 'Legal Considerations on Predictive Policing Based on Italian "Algorithmic Administration" Principles' (2025) 18(32) YARS.

Article received: 01.07.2025, accepted 07.09.2025.

Yearbook of Antitrust and Regulatory Studies, Vol. 18, No. 32, pp. 57–78 • ISSN 1689-9024
https://doi.org/10.7172/1689-9024.YARS.2025.18.32.1

the main issue that juridical assessment must consider when it comes to the use of predictive technology tools in the public sector. Policing is an administrative function that is mainly composed of acts of a preventive nature. By using ICT, it is possible to employ AI systems with a very high rate of certainty to 'predict' future crime scenes. But is it possible to combine the use of such predictive systems with the protection of fundamental rights? The paper will attempt to answer this question by reconstructing the Italian legal framework, focusing on its most recent laws and, above all, on the principles of algorithmic administration as set out by the Italian administrative judiciary. On this basis, the paper will investigate whether it is possible to use these tools so as to enjoy their positive effects, but reduce the risk of violating fundamental rights.

Résumé

Dans la société du risque actuelle décrite par Beck, l'État est confronté à un dilemme. Échouer face au risque mais préserver l'intégrité des droits des citoyens, ou ne pas échouer mais restreindre les droits fondamentaux ? Ce compromis s'avère être la question principale que doivent prendre en compte les réflexions juridiques sur l'utilisation des outils technologiques prédictifs dans le secteur public. Le maintien de l'ordre est une fonction administrative qui consiste principalement en des actes de nature préventive. Grâce aux TIC, il est possible d'utiliser des systèmes d'IA avec un taux de certitude très élevé pour « prédire » les futures scènes de crime. Mais est-il possible de combiner l'utilisation de ces systèmes prédictifs avec la protection des droits fondamentaux ? Cet article tentera de répondre à cette question en reconstituant le cadre juridique italien, en mettant l'accent sur ses lois les plus récentes et, surtout, sur les principes de l'administration algorithmique énoncés par le tribunal administratif italien. Et ce, afin d'étudier s'il est possible d'utiliser ces outils tout en profitant de leurs effets positifs et en réduisant le risque de violation des droits fondamentaux.

Keywords: Predictive Policing; Algorithmic Administration' Principles; AI; Algorithm; Administrative Law.

JEL: K22; K23; K29

I. Introduction. The Challenges of Technology to Current Society

From Max Weber's well-known definition of the State, according to which it constitutes the monopoly of the legitimate use of physical force[1], it is possible to deduce a central consideration in the relationship between citizens and public power: the citizens' demand (and need) for protection addressed to the State. This is a thesis supported by leading legal philosophers[2], epistemologists[3] and sociologists already.

Among the latter is Ulrich Beck[4], for whom the current social context is characterised by increasing uncertainty, where the danger of a certain event transitions into the risk of the unknown that cannot (any longer) be calculated.

In our current society, which Beck called a 'risk society' because it is characterised by uncertainty, the State is faced with a dilemma. On the one hand, failing in the face of risk, but keeping the sphere of citizens' rights intact; or, on the other hand, not failing in the face of risk, but restricting fundamental rights.

---

[1] Cf. Max Weber, *Politik als Beruf* (Duncker & Humblot 1919) 4: «*Staat ist diejenige menschliche Gemeinschaft, welche innerhalb eines bestimmten Gebietes – dies: das „Gebiet", gehört zum Merkmal – das Monopol legitimer physischer Gewaltsamkeit für sich (mit Erfolg) beansprucht*». About the figure of Max Weber, see Wolfgang Drechsler, 'Good Bureaucracy: Max Weber and Public Administration Today' (2020), *Max Weber Studies* (2), 219 ff.

[2] Such as, among others, Thomas Hobbes, *Leviathan* (Cambridge University Press 1991 [first ed. 1651]), Chapt. XVII, 117: «*The finall Cause, End, or Designe of men, (who naturally love Liberty, and Dominion over others,) in the introduction of that restraint upon themselves, (in which wee see them live in Commonwealths,) is the foresight of their own preservation, and of a more contended life thereby; that is to say, of getting themselves out from that miserable condition of Warre, which is necessarily consequent (ad hat been shewn) to the naturall Passions of men, where there is no visible Power to keep them awe, and tye them by feare of punishment to the performance of their Covenants, and observation of those Lawes of Nature*»). The thesis is also supported by John Locke, *Two Treaties of Government – The Second Treatise* (Cambridge University Press 1988 [first ed. 1689]), Chapt. III, 21, 282: «*To avoid this State of War (wherein there is no appeal but to Heaven, and wherein every least difference is apt to end, where there is no Authority to decide between the Contenders) is one great reasons of Mens putting themselves into Society, and quitting the State of Nature. For where there is an Authority, a Power on Earth, from which relief can be had by appeal, there the continuance of the State of War is excluded, and the Controversie is decided by that Power*». It is also supported by Baruch Spinoza, *Tractatus theologico-politicus* (Einaudi, 1972 [first ed. 1670]), Chapt. XVI, 379–380. For a wide reconstruction of the topic, see Norberto Bobbio, *Giusnaturalismo e positivismo giuridico* (Edizioni di Comunità 1965), in part. 163 ff. On the thoughts of Locke and Hobbes, see Wolfgang von Leyden, *Hobbes and Locke. The Politics of Freedom and Obligation* (Macmillan 1982).

[3] Cf. Karl Popper, *The Open Society and its Enemies*, I (Routledge 1962 [first ed. 1945]), Chapt. VI, 109–110: «What do we demand from a state? […] I demand protection for my own freedom and for other people's».

[4] See Ulrich Beck, *Risikogesellschaft. Auf dem Weg in eine andere Moderne* (Suhrkamp 1986).

This payoff turns out to be the main problem facing contemporary society, in a context characterised by an increasing interconnection between risks and opportunities offered by digital technology (hereinafter: ICT – Information and Communication Technology). In fact, this aspect led Beck to write about risk deriving from the technological unknown[5].

This contrast between the protection of security and the protection of fundamental rights is further emphasised by those technological tools that can offer predictive results to police activity.

II. The Administrative Police Function and the Importance of Preventive Activities

The Italian legal literature of the past century studied police activity in depth[6], with the aim of analysing and framing it within public (and administrative) legal categories[7].

Without reconstructing here the development of these relevant studies, it is necessary to point out the important distinction between 'judicial police activity' and 'security police activity'[8].

In fact, judicial police activity is an investigative process aimed at searching for, and discovering crimes and offenders. Conversely, security police activity is an activity aimed at the protection of rights that takes the form of maintaining public order. Therefore, the former is instrumental to the exercise of criminal prosecution, and presupposes that the criminal act has already occurred. By contrast, the latter is the expression of an administrative function, and is aimed at preventing the criminal act from being committed.

Thus, in the Italian legal system, these two types of police activities are constitutionally distinct from each other[9]. But it is precisely its preventive

---

[5] *Ibidem*.

[6] As in other European countries, such as France: f.i. see Maurice Hauriou, *Précis èlementaire de Droit administratif* (Recueil Sirey 1938) 326 ff.

[7] *Ex multis* Oreste Ranelletti, 'Concetto della polizia di sicurezza' (1898), *Arch. Giur. Fil. Serafini*, n.s., Vol. I, fasc. 3, Vol. II, fasc. 1 ff. [also in Oreste Ranelletti, 'La polizia di sicurezza', in Vittorio Emanuele Orlando (cur.), *Primo trattato completo di Diritto amministrativo italiano*, Vol. IV, parte I (Società Editrice Libraria 1904) 207 ff.]; Santi Romano, *Principi di diritto amministrativo italiano* (Società editrice libraria 1901) 193 ff.; Guido Zanobini, *Corso di diritto amministrativo*, Vol. V, (Giuffrè 1950).

[8] Distinction considered to be valid today.

[9] Cf. Article 109 Italian Constitution: «Criminal police shall be at the service of the Judiciary» (the English official translation of the Italian Constitution is available at <https://s.uniupo.it/hzi2v> accessed 21st October 2025). On this argument see in general, in Italian, Salvatore

nature that, on closer inspection, lies at the heart of the security function of the police[10]. Furthermore, as already stated by Cesare Beccaria in *Dei delitti e delle pene*, it is precisely preventive activities that are the most functional in avoiding the criminal act from occurring, since repressive activity must be understood as an exceptional measure[11].

Summarising the above, public security policing (hereinafter: police activity) is therefore that administrative function of the police, which is aimed primarily at the prevention of future criminal behaviour. Criminal prevention, as is well known, takes the form of prevention measures, personal or patrimonial sanctioning measures[12] based on clues or suspicions, and imposed on specific categories of individuals considered socially dangerous[13], regardless of the verification and commission of the fact[14]. As regards prevention measures, which are not to be confused with security measures[15], the present discussion will not focus on.

Raimondi, *La sicurezza pubblica* (Giappichelli 2023); Tommaso Francesco Giupponi, *ad vocem* 'Sicurezza e potere' (2023), *Enc. dir.*, I, tematici, V, *Potere costituzione*, 1149 ff.; Riccardo Ursi, *La sicurezza pubblica* (Il Mulino 2022); Carlo Mosca, *La sicurezza. Valori, modelli e prassi istituzionali* (Editoriale Scientifica 2021); Edoardo Chiti, 'Le sfide alla sicurezza e gli assetti nazionali ed europei delle forze di sicurezza e di difesa' (2016), *Dir. amm.*, n. 4, 511 ff.; Alessandro Pace, 'La sicurezza pubblica nella legalità costituzionale' (2015), *Rivista AIC*, n. 1, 1 ff.; Tommaso Francesco Giupponi, *Le dimensioni costituzionali della sicurezza* (Bonomo 2010); Ginevra Cerrina Feroni, Giuseppe Morbidelli, 'La sicurezza: un valore superprimario' (2008), *Perc. cost.*, n. 1, 31 ff.; Giuseppe Caia, 'Ordine pubblico e sicurezza', in Sabino Cassese (a cura di), *Trattato di diritto amministrativo*, *Diritto amministrativo speciale*, I (Giuffrè 2003), 281 ff.; Sergio Foà, *ad vocem* 'Sicurezza pubblica' (1999), *Dig. disc. Pubbl.*, XIV, 127 ff.; Marco Mazzamutto, 'Poteri di polizia e ordine pubblico' (1998), *Dir. amm.*, n. 3–4, 441 ff.; Guido Corso, *L'ordine pubblico* (Il Mulino 1979); Paolo Barile (a cura di), *La sicurezza pubblica* (Neri Pozza 1967).

[10] As underlined by Pietro Virga, *La potestà di polizia* (Giuffrè 1954) 10; and by Aldo Mazzini Sandulli, *Manuale di diritto amministrativo* (Giuffrè 1954) 381.

[11] See Cesare Beccaria, *Dei delitti e delle pene*, XLI (Livorno 1764). On Beccaria's significance for modern legal culture, see Giovanni Tarello, *Storia della cultura giuridica moderna* (Il Mulino 1976), 462 ff.

[12] In the Italian legal order personal preventive measures may include: a mandatory travel order, an oral warning, a special surveillance, a prohibition to access sporting events (in Italian: DASPO), a warning for persecutory acts, a warning for acts of domestic violence; a removal order and a prohibition to enter specific urban areas. On this issue, see Letizia Mandaglio, Giuseppe Pullara (cur.), *Linee guida in materia di misure di prevenzioni personali* (Direzione Anticrimine della Polizia di Stato 2020).

[13] Cf. Italian Supreme Court of Cassation, Criminal Section, No. 54119/2017. As established by Italian Supreme Court of Cassation, Criminal Section, No. 23641/2014, the social dangerousness must be verified in facts.

[14] Cf. Italian Supreme Court of Cassation, Criminal Section, No. 3886/2012.

[15] Security measures are imposed in cases of a proved dangerousness of individuals who have committed an act provided for by law as a criminal offence. About the differences between

III. The Technological Improvement of Police Activity: the Centrality of Algorithms and their Use

What has been written above must necessarily be read in correlation with the progress that ICT is bringing about, both in society and in the public administration itself.

Digital technology is an instrument used to improve administrative actions and organisation. On the one hand, data analysis is employed as a tool to optimise the knowledge gathering activities of public administration[16]. On the other hand, digital technology is used to enforce the law at the administrative level (potentially achieving important results in terms of preventing its non-implementation)[17].

In this technological context, algorithms play an indisputable central role, influencing the legal field[18].

Without anticipating what will be analysed in detail below, algorithms can basically be classified into two categories. On one side are (quite) simple algorithms, so-called conditional (or rule-based) ones[19]. On the other side (more) are complex algorithms, which we could define as machine learning (hereinafter: ML) algorithms[20] for simplicity's sake.

Conditional algorithms operate on a programming rule that requires human intervention by the programmer to input data to obtain a particular output. In this way, the programmer can match a logical rule with a computer rule: if it is applied in a legal context, then it can correspond to a legal rule. This may occur in all those cases where the administration acts without discretion.

---

prevention and security measures see *ex multis*, in Italian, Tullio Padovani, *Misure di sicurezza e misure di prevenzione* (Pisa University Press 2014).

[16] See Italian recent literature, as Roberto Cavallo Perin, Isabella Alberti, 'Atti e procedimenti amministrativi digitali', in Roberto Cavallo Perin, Diana-Urania Galetta, *Il Diritto dell'Amministrazione Pubblica digitale* (Giappichelli 2025), 138 ff.; Isabella Alberti, *L'istruttoria nel procedimento amministrativo. Prospettive di acquisizione digitale della conoscenza* (Giappichelli 2024); and Matteo Falcone, *Ripensare il potere conoscitivo tra algoritmi e big data* (Editoriale Scientifica 2023). On this topic may I refer also to Stefano Rossa, *Contributo allo studio delle funzioni amministrative digitali* (Wolters Kluwer 2021).

[17] Cf. *ex multis* John F. Schnelle, E. Scott Geller, Mark A. Davis, 'Law Enforcement and Crime Prevention', in Edward K. Morris, Curtis J. Braukmann (Eds.), *Behavioral Approaches to Crime and Delinquency* (Springer 1987) 225 ff.; Nicoletta Rangone, 'Making law effective: behavioural insights into compliance' (2018), *European Journal of Risk Regulation*, 3, 484 ff.

[18] About it see Edward J. Walters, *Data-Driven Law: Data Analytics and the New Legal Services* (CRC Press 2018).

[19] On this topic, see Mark J. Johnson, *A concise introduction to Programming in Python* (CRC Press 2018).

[20] *Ex multis* François Chollet, *Deep Learning with Python* (Manning 2017).

Instead, machine learning algorithms are algorithms composed of a source code (as well as conditional algorithms), but they work by applying their own autonomous learning process[21]. By training the machine, which is 'fed' a dataset, a complex algorithm is programmed to independently develop its own model in the learning phase. This learning model is different from a source code because the latter is known and can be consulted by individuals with technical knowledge, whereas the model is created by the machine itself, in progressive and temporally distinct stages, and is, in principle, not discernible[22]. In this case, therefore, the action of the programmer is minimal[23].

IV. The Issue of Algorithmic Transparency: between the EU AI Act and 'New' Jurisprudential Principles

In this context, the issue of an algorithm's transparency becomes evident.

The European Union, as is well known, can proudly claim to be the first international organisation to adopt a positive regulatory framework on AI, thanks to the recent approval of the so-called EU AI Act (EU Regulation 2024/1689)[24].

The paper does not intend to analyse the rules of this Act, referring readers to studies of the literature instead[25]. What is necessary to highlight,

[21] Cf. Gherardo Carullo, 'Large Language Models for Transparent and Intelligible AI-Assisted Public Decision-Making' (2023), *CERIDAP*, 3, 1 ff.

[22] In this way, see in Italian Gherardo Carullo, 'Decisione amministrativa e intelligenza artificiale', *Il diritto dell'informazione e dell'informatica* (2021), 3, 439.

[23] As pointed out by the Italian Council of State, III sect., 25/11//2021 No. 7891 (available in Italian at <https://s.uniupo.it/begju> accessed 21st October 2025), with the use of machine learning algorithms there would be a real substitution of civil servants by machines.

[24] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (available at <https://s.uniupo.it/ytajd> accessed 21st October 2025).

[25] About the EU AI Act see Lorenzo Cotino Hueso, Diana-Urania Galetta (Eds.), *The European Union Artificial Intelligence Act. A Systematic Commentary* (Editoriale Scientifica 2025); Ceyhun Necati Pehlivan, Nikolaus Forgó, Peggy Valcke (Eds.), *The EU Artificial Intelligence (AI) Act: A Commentary* (Wolters Kluwer 2024). In general, on the broader topic of the use of artificial intelligence systems by public authorities, see Markku Suksi (Ed.), *The Rule of Law and Automated Decision-Making Exploring Fundamentals of Algorithmic Governance* (Springer 2023); Simona Demková, *Automated Decision-Making and Effective Remedies. The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Elgar 2023); Stefan Schäferling, *Governmental Automated Decision-Making and Human Rights. Reconciling Law and Intelligent Systems* (Springer 2023). In particular, in relation to Public Administration aspects,

however, is the general approach to the topic of Artificial Intelligence that the European legislator wanted to provide with the EU AI Act. It is based on a risk assessment approach[26], whereby AI systems are classified into three 'risk classes' relating to the impact of their use on the fundamental rights of individuals, health and safety. In this context, risks can be described as: unacceptable, high, or low/minimal.

According to the precautionary approach, which can be summarised in the motto 'higher the risk, stricter the rules', the higher the class of risk, the greater the guarantees for the protection of rights and, conversely, the stricter the applicable rules[27]. One example of this is the regulation of transparency obligations for AI systems, in particular for those considered high-risk[28], and for those designed and developed to interact with individuals[29]. In fact, in the case of high-risk automated systems, specific strengthened transparency obligations have been imposed, which require their manufacturers to draw up and communicate the specific technical documentation of the system to the deployers, and to the public control authority[30].

It is precisely the obligation to provide the technical documentation of the system to deployers that aims to put them in a position where they can understand the technical functioning of the algorithm and, ultimately, to use it in the correct way. The transparency obligation (understood as the duty to

---

see Diana-Urania Galetta, *Artificial Intelligence and Public Administration. A Journey* (Editoriale Scientifica 2025); Sophie Weerts, 'Generative AI in public administration in light of the regulatory awakening in the US and EU' (2025), *Cambridge Forum on AI: Law and Governance*, Vol. 1, 1 ff.; Frank Pasquale, Gianclaudio Malgieri, 'Generative AI, explainability, and score-based natural language processing in benefits administration' (2024), *Journal of Cross-Disciplinary Research in Computational Law*, 2(2). For a comparative perspective see Francesco Decarolis, Barbara Marchetti, Luisa Torchia (Eds.), *The EU Digital Regulation and Its Impact on Member States* (Springer 2025); Roberto Scarciglia, 'Artificial Intelligence and the State from a Comparative Perspective' (2025), *Italian Journal of Public Law*, Vol. 17, Issue 2, 474 ff.; Herwig Christian Hellmut Hofmann, Felix Pflücke (Eds.), *Governance of Automated Decision-Making and EU Law* (Oxford University Press 2024); Herwig Christian Hellmut Hofmann, 'Comparative Law of Public Automated Decision-Making. An Outline' (2023), *CERIDAP*, n. 1, 1 ss.

[26] Cf. Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' (2024), *Computer Law & Security Review*, Vol. 54, 1 ff.; Jonas Schuett, 'Risk Management in the Artificial Intelligence Act' (2023), *Eur. Journ. Risk Reg.*, 1 ff.; Giovanni De Gregorio, Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022), *Common Market Law Review*, 59-2; Francesca Palmiotto, 'The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation' (2025), *Eur. Journ. Risk Reg.*, 16, 770 ff.

[27] Cf. Article No. 6 Regulation (EU) 2024/1689.

[28] Cf. Article No. 13 Regulation (EU) 2024/1689.

[29] Cfr. Article No. 50 Regulation (EU) 2024/1689.

[30] See respectively Article No. 13 and No. 11 Regulation (EU) 2024/1689.

provide the end user with all information on AI systems), is reinforced by the manufacturer's obligation to design and develop these AI systems to ensure that their functioning is «sufficiently transparent» to enable the deployer to interpret the result generated, thus ensuring «an appropriate type and degree of transparency»[31].

The AI Act requires manufacturers to include all documentation and information on the functioning of their automation systems in the EU's public database for AI systems[32]. This aspect allows the interpreter to link the principle of transparency to that of public awareness, placing a strong emphasis on widespread social control granted to citizens. However, this link is weak, above all because it presupposes that access to technical data implies automatic and widespread knowledge of the algorithm's functioning mechanism for those consulting it. This turns into a substantial vulnerability if such AI systems are used to make public decisions.

In the context of increasing public digitisation, the issue of algorithm transparency assumes central importance, being indispensable in all cases where public administration employs automated systems to achieve its institutional purpose[33].

The reconstruction that the Italian administrative judiciary outlined a few years ago highlights this point: an administrative act generated by digital devices (and thus by algorithms) is an «electronically processed administrative act»[34] that must comply with the same rules as analogue 'non-electronic' administrative acts[35].

It is therefore essential to know the logical process that led the administration to its adoption, in particular through the obligation to provide the reasoning of the decision[36], the right of access to administrative documents[37], and procedural participation[38]. There are three legal instruments that the Italian legislator has foreseen to ensure maximum transparency of administrative actions. From this

[31] Cf. Article No. 13 para. 1 Regulation (EU) 2024/1689.

[32] Cf. Article No. 71 Regulation (EU) 2024/1689.

[33] Aspect, moreover, highlighted by Enrico Carloni, 'Transparency within the artificial administration principles, paths, perspectives and problems' (2024), *Italian Journal of Public Law*, Vol. 16, 1, 8 ff.

[34] Author's translation. Cf. Regional Administrative Cour of Lazio, Rome, III-*bis*, decision 22/03/2017, No. 3769 (available in Italian at <https://s.uniupo.it/o3d1g> accessed 21st October 2025).

[35] Cf. Italian Law on the Administrative Action and the Right of Access to Administrative Documents (Law No. 241/1990). This law is available in Italian at <https://s.uniupo.it/oz2c3> accessed 21st October 2025. About it see Giorgio Pastori, 'The Origins of Law No 241/1990 and Foreign Models' (2010), *Italian Journal of Public Law*, 2, 259 ff.

[36] Cf. Article No. 3 Italian Law No. 241/1990.

[37] Cf. Article No. 22 ff. Italian Law No. 241/1990.

[38] Cf. Article No. 13 Italian Law No. 241/1990.

perspective, the link between transparency and the algorithm is in line with the right to good administration established by Article 41 of the EU Charter of Fundamental Rights[39].

A categorical consideration of the nature of algorithms is necessary at this point. Recalling the aforementioned distinction made by Italian doctrine[40], we can distinguish between (simple) conditional (or rule-based) algorithms, and (more) complex algorithms (or machine learning (ML) or, in a broader sense, those based on Artificial Intelligence).

Conditional algorithms operate based on an 'if-else' type of programming rule where human intervention is required, by the programmer, to input data to obtain a given output. In this way the programmer is able to make a logical rule coincide with a programming rule, which, if applied in a legal context, can linearly correspond to a legal rule. This is what generally happens when public administration acts in the context of a binding activity. In fact, if the administration is called upon to implement the rule at the administrative level, in the absence of a margin of discretion, it will be faced with a binding activity. Therefore, it is not important whether or not technology is used to carry out the public activity in question, since the choice of 'medium' is incorporated into the binding nature of the action[41].

More relevant is the event when the administration employs algorithms in an activity characterised by discretionary power – a situation, moreover, drawn into the scope of the operation of the second type of algorithms, those based on machine learning. They are algorithms composed of a source code (like conditional algorithms), but possess the particularity of functioning through a process of authentic learning. By training the software to which a dataset is 'fed', a complex algorithm is programmed to independently develop its own model in the learning phase (the so-called 'black box issue')[42].

---

[39] On this topic see Paul Craig, 'The Right to Good Administration', in Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (Eds.), *The EU Charter of Fundamental Rights. A Commentary* (Bloomsbury 2021) 1125 ff.; in Italian instead Diana-Urania Galetta, 'Digitalizzazione e diritto ad una buona amministrazione (Il procedimento amministrativo, fra diritto UE nuove tecnologie dell'informazione e della comunicazione)', in Roberto Cavallo Perin, Diana-Urania Galetta, *Il Diritto dell'Amministrazione Pubblica digitale*, *cit.*, 79 ff.

[40] Distinction used, in Italian, by Gherardo Carullo, 'Decisione amministrativa e intelligenza artificiale', *cit.*, 431 ff., and to whose technical bibliographical references we address for further details.

[41] In this way, see G. Carullo, 'Decisione amministrativa e intelligenza artificiale', *cit.*, 441.

[42] On this argument, *ex multis*, see Vasiliki Papadopuli, 'Artificial Intellingece's Black Box: Posing New Ethical and Legal Challenges on Modern Societies', in Angelos Kornilakis, Georgios Nouskalis, Vassilis Pergantis, Themistoklis Tzimas (Eds.), *Artificial Intelligence and Normative Challenges* (Springer 2023), 39 ff.

As is evident, in the case of machine learning algorithms the intervention of the programmer is minimal and could potentially represent a case of AI replacing the relevant civil servant. In these circumstances, one could wonder whether the nexus allowing the liability of the civil servant for the (mainly) discretionary exercise of administrative action, arising from their liability on the basis of the relationship of 'organic identification' (which allows the actions of an official to be considered as direct actions of the body to which he or she belongs) is still valid.

Similarly, one could question the real effectiveness of 'traditional' instruments of safeguarding the individual legal positions of those involved in algorithm-based administrative procedures – namely the obligation to provide reasoning and the right of access. Ultimately, one might wonder where the transparency is in these situations.

1. The Italian Principles of 'Algorithmic Administration'

Precisely to answer these questions, the Italian administrative judiciary delivered several relevant decisions, whose reasoning is based on the interpretation of the transparency of the so-called 'algorithmic administration'. These rulings laid the foundations for an important interpretative strand[43].

In a famous decision of the Council of State[44], the Italian judiciary first highlighted a logical and legal equation: if an algorithm is transparent then it is comprehensible; if it is comprehensible then it is questionable; if an algorithm is questionable, then it is subject to judicial review.

The transparency of the algorithm, therefore, turns out to be imperative and represents the parameter towards which to orient the use of traditional legal tools (the obligation to motivate the decision and the right of access), reinterpreting them, however, in an 'algorithmic' key.

---

[43] *Ex multis* about it see Diana-Urania. Galetta, Giulia Pinotti, 'Automation and Algorithmic Decision-Making Systems in the Italian Public Administration' (2023), *CERIDAP*, 1, 13 ff. In Italian see Luisa Torchia, *Lo Stato digitale. Una introduzione* (Il Mulino 2025), 129 ff. In general, on the broader topic of the use of automation systems in Italian public administration, see, in Italian, Maria Bianca Armiento, *Pubbliche Amministrazioni e Intelligenza Artificiale* (Editoriale Scientifica 2025); Alessandro Di Martino, *Tecnica e potere nell'amministrazione per algoritmi*, (Editoriale Scientifica 2023); Luigi Previti, *La decisione amministrativa robotica* (Editoriale Scientifica 2022); Giovanni Pesce, *Funzione amministrativa, intelligenza artificiale e blockchain* (Editoriale Scientifica 2021).

[44] Italian Council of State, VI sect., decision 08/04/2019, No. 2270 (available in Italian at <https://s.uniupo.it/f367m> accessed 21st October 2025).

With reference to the aforementioned decision on the equivalence of an 'electronic administrative act' to an analogical administrative act[45], the Italian administrative judiciary affirmed that there is a need for the discernability of the logical process (*recte*: *iter*), on which the administration adopted the final act[46].

The need for transparency and the contextual obligation to justify a digital administrative act arise in relation to both conditional, and machine learning algorithms.

In the case of conditional algorithms, the administration has the duty to guarantee the interested party access to the source code, because, as pointed out above, computer rules correspond to logical rules and legal rules – the verification of programming rules, therefore, leads to the verification of legal rules. Access to the source code thus corresponds to the right of documentary access, understood as the individual's claim to view and extract a copy of the source code (or part of it)[47].

More problematic is the question of transparency in relation to machine learning algorithms, because as previously mentioned they 'learn' autonomously on the basis of a continuously self-evolving training model. Nevertheless, even for machine learning algorithms, access must be granted not only to the source code, but, above all, to the learning dataset with which the machine is trained – as training the machine based on data increases the risk of creating decision bias.

The Italian administrative courts have set out this interpretative approach, establishing the so-called 'principles of algorithmic administration'[48]:

i) 'principle of algorithmic transparency' – according to which Public Administration has the obligation to make the source code and the learning dataset effectively accessible to the person involved, putting him or her in a situation where the algorithm is actually knowable;

---

[45] See footnote No. 34.

[46] Italian Council of State, VI sect., decision 13/12/2019, No. 8472 (available in Italian at <https://s.uniupo.it/qhtqj> accessed 21st October 2025).

[47] In this way, see Carullo G., 'Decisione amministrativa e intelligenza artificiale', *cit.*, 449. Of course, in addition to this access, transparency must also be guaranteed by the absence of pathologies in the administrative act (of electronic processing).

[48] Cf. Council of State, VI sect., decision 13/12/2019, No. 8472-8473-8474 del 2019; Council of State, VI sect., decision 04/02/2020, No. 881; Council of State, VI sect., decision 09/02/2021, No. 1206. More recently also Regional Administrative Cour of Campania, Naples, III sect., 14/11/2022, No. 7003. On this last decision, see Alessandro Di Martino, 'More on Algorithms and Public Administration' (2023), *European Review of Digital Administration & Law – Erdal*, Vol. 4 Issue 1, 307 ff. The mentioned decisions are available in Italian at <https://s.uniupo.it/ca6vp> accessed 21st October 2025.

ii) 'principle of algorithmic non-discrimination', which requires that its use must not be formulated – intentionally or not – so as to discriminate against specific individuals or groups of individuals[49];
iii) 'principle of non-exclusivity' of the use of automated systems, which prohibits the addressee of an administrative act from being subject to a decision taken by fully automated systems (principle that *ad contrarium* imposes that there must always be a civil servant to monitor the decision and take responsibility for it[50]).

In the Italian legal order, the principles of the so-called 'Algorithmic Administration' have recently been adopted by the national legislator – before the entry into force of the EU AI Act. In fact, the latter introduced into the Italian Public Procurement Code[51] a rule expressly dedicated to the use of automated procedures in the life cycle of public contracts, thus transposing the aforementioned approach of the Italian administrative judiciary[52].

In addition to this law, the Italian Parliament recently approved the Italian Law on Artificial Intelligence (Law No. 132/2025)[53], with the explicit aim of «[p]romoting a correct, transparent and responsible use, in an anthropocentric dimension, of artificial intelligence, in order to seize its opportunities»[54] (in accordance with the EU AI Act)[55].

The use of AI tools has generated relevant legal issues, especially in relation to the activities of public administration, which the interpretative actions of the judiciary have tried to regulate 'by principles'. As a result, it is not surprising

[49] This circumstance recalls the issue, mentioned above, of the need to reduce the bias that the machine training model can produce from the data stored in the dataset.

[50] Or, to use the expression coined by Judge Gallone, there is a 'reserve of humanity'. Cf. Giovanni Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo* (Wolters Kluwer 2023).

[51] Legislative Decree 31/03/2023, No. 36 (available in Italian at <https://s.uniupo.it/alxxf> accessed 21st October 2025).

[52] Cf. in particular Article No. 30 para. 3 Italian Legislative Decree 31/03/2023, No. 36: «3. Decisions made by automation shall comply with the principles of: (a) knowability and comprehensibility, whereby every economic operator has the right to know the existence of automated decision-making processes concerning him and, if so, to receive meaningful information on the logic used; b) non-exclusivity of the algorithmic decision, whereby in any case there exists in the decision-making process a human contribution capable of checking, validating or refuting the automated decision; (c) algorithmic non-discrimination, whereby the owner implements appropriate technical and organizational measures to prevent discriminatory effects against economic operators» (Author's translation). On this argument, see Anna Maria Chiariello, 'The Digitisation Principles in the New Italian Public Contracts Code' (2024), *European Review of Digital Administration & Law – Erdal*, Vol. 5, Issue 2, in part. 180 ff.

[53] Law 23/09/2025, No. 132 (available in Italian at <https://s.uniupo.it/1ffp6> accessed 21st October 2025).

[54] Article No. 1 para. 1 Law 23/09/2025, No. 132 (Author's translation).

[55] Cf. Article No. 1 para. 2 Law 23/09/2025, No. 132.

that the Italian AI Law also regulates the use of these automation tools, especially with reference to administrative action. In fact, this law establishes that public administration may use AI systems only «in an instrumental and supporting function to the provvedimental activity [i.e. the activity aimed at adopting administrative acts], respecting the autonomy and decision-making power of the person who remains solely liable for the administrative acts and procedures in which artificial intelligence has been used»[56].

V. Digital Technologies and Police Activity: from Prevention to Prediction

Just as algorithmic technologies can be employed to optimise administrative activity, it is possible to employ them to optimise police activity too, with the aim of preventing the commitment of criminal acts. However, thanks to algorithms, it is possible to develop technological tools capable of preventing the perpetration of a crime with a very high rate of probability, which may, in this sense, 'forecast' or 'predict' the future. Tools of a predictive nature – is precisely where predictive police activity comes in[57].

---

[56] Article No. 14 para. 2 Law 23/09/2025, No. 132 (Author's translation).

[57] On this general topic, see *ex multis* Elizabeth E. Joh, 'Policing by numbers. Big data and the fourth amendment' (2014), *Washington University Law Review*, 89; Andrew D. Selbst, 'Disparate Impact in Big Data Policing' (2017), *Georgia Law Review*, 52; Andrew G. Ferguson, 'Policing predictive policing' (2017), *Washington University Law Review*, 94; Lyria Bennett Moses, Janet Chan, 'Algorithmic prediction in policing. Assumptions, evaluation, and accountability' (2018), *Policing and Society*, 28:7, 806 ff.; Andrew G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2018); Rashida Richardson, Jason M. Schultz, Kate Crawford, 'Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice' (2019), *New York University Law Review Online*, Vol. 94, 15 ff.; Will Douglas Heaven, 'Predictive policing algorithms are racist. They need to be dismantled' (2020), *MIT Technology Review*, July 17; Daniel Susser, 'Predictive Policing and the Ethics of Preemption', in Ben Jones, Eduardo Mendieta (Eds.), *The Ethics of Policing: New Perspectives on Law Enforcement* (New York University Press 2021); Matthias Kuppler, Christoph Kern, Ruben L. Bach, Frauke Kreuter, 'From fair predictions to just decisions? Conceptualizing algorithmic fairness and distributive justice in the context of data-driven decision-making' (2022), *Frontiers in Sociology*, Vol. 7; Youngsub Lee, Ben Bradford, Krisztian Posch, 'The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review' (2024), *Justice Evaluation Journal*, 7(2), 127 ff.; Klaus Behnam Shad, 'Artificial intelligence-related anomies and predictive policing: normative (dis)orders in liberal democracies' (2025), *AI & Society*, Vol. 40, 891 ff.; Ahmed S. Almasoud, Jamiu Adekunle Idowu, *Algorithmic fairness in predictive policing* (Springer 2025); Vasilis Galis, Helene O.I. Gundhus, Antonis Vradis (Eds.), *Critical Perspectives on Predictive Policing. Anticipating Proof?* (Elgar 2025).

Predictive policing tools[58] can be distinguished from those of traditional investigations primarily by their approach: the former follow a deductive logic, while the latter employ a probabilistic approach[59].

There are two types of predictive policing software.

The first concerns 'crime hotspot' software, focused on place-based algorithms that identify places that may be a potential scene of specific crimes, and that can be identified as 'future' crime scenes of specific crimes[60]. This is because, with the combination of particular factors (e.g. space, time, convergence of offenders, targets, victims) in specific contexts, it is possible to foresee the commission of serial offences[61] (e.g. robbery), thus enabling the police to allocate their forces across their coverage territory in the best possible way.

---

[58] This paper does not aim to conduct a comparative study on predictive policing. Nevertheless, for further information on the use of predictive policing tools in some EU Countries, see about Germany: Johanna Sprenger, Dominik Brodowski, "Predictive Policing', 'Predictive Justice', and the Use of 'Artificial Intelligence' in the Administration of Criminal Justice in Germany' (2023), *e-Revue internationale de droit penal*, 5 ff.; Simon Egbert, 'About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany' (2018), *European Journal for Security Research*, 3, 95 ff.; Kai Seidensticker, Felix Bode, Florian Stoffel, *Predictive Policing in Germany* (Konstanzer Online-Publikations-System, 2018); see, about France, instead, Cécile Godé, Sébastien Brion, 'The Affordance-Actualization Process of Predictive Analytics: Towards a Configurational Framework of a Predictive Policing System' (2024), *Technological Forecasting and Social Change*, Vol. 204; Edlira Nano, Félix Tréguer, *La police prédictive en France : contre l'opacité et les discriminations, la nécessité d'une interdiction* (La Quadrature du Net 2024); Cécile Godé, Sébastien Brion, Amélie Bohas, 'The Affordance-Actualization process in a Predictive Policing Context: insights from the French Military Police (2020), *European Conference on Information Systems (ECIS)*, Jun 2020. Lastly, about the Netherlands, see Marc Schuilenburg, Melvin Soudijn, 'Big data policing: The use of big data and algorithms by the Netherlands Police' (2023), *Policing: A Journal of Policy and Practice*, Vol. 17, 1 ff.; Albert Meijer, Lukas Lorenz, Martijn Wessels, 'Algorithmization of Bureaucratic Organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems' (2021), *Public Administration Review*, Vol. 81, Issue 5, 837 ff.; Gerwin van Schie, Serena Oosterloo, 'Predictive Policing in the Netherlands: A Critical Data Studies Approach', in Veronika Nagy, Klára Kerezsi (Eds.), *A Critical Approach to Police Science: New Perspectives in Post-Transitional Policing Studies* (Eleven Int. Publ. 2020), 169 ff.

[59] Some examples are certain software used by the Italian police, including the 'X-Law' software, adopted by the Naples Police Headquarters, the 'Key-crime' software, adopted by the Milan Police Headquarters, and the 'Giove' software, used by the Ministry of the Interior. On this topic, see Maria Bianca Armiento, 'La polizia predittiva come strumento di attuazione amministrativa delle regole' (2022), *Diritto amministrativo*, 4, 990 ff.

[60] In this way, in Italian, see Lorenzo Algeri, 'Intelligenza artificiale e polizia predittiva' (2021), *Diritto penale e processo*, 6, 730 ff. On this topic, from a criminal law perspective, see also Giulia Barone, *Giustizia predittiva e certezza del diritto* (Pacini 2024).

[61] Cf. Paul J. Brantingham, Patricia L. Brantingham, 'Crime generators and crime attractors' (1995), *European Journal on Criminal Policy and Research*, 3, 5 ff.

The other type of software is 'crime linking' in nature, relying on person-based algorithms, which study the seriality of criminals (rather than crimes) to forecast where and when these offenders will commit serial offences[62].

By extending this discourse into different contexts, predictive (non-police) systems are in fact already applied in everyday life. For example, the calculation of car insurance premiums varies according to the city of residence of the person signing the insurance contract. The larger and more populous the city of residence, the greater the risk of traffic accidents. Consequently, the risk of traffic accidents is larger. This is why car insurance premiums are usually higher in the city than in the countryside.

However, the issue addressed in this paper is different and critical, because the use of predictive policing software has a clear impact on the fundamental rights and freedoms of individuals.

1. The Persisting Relevance of the Contrast Between Public Security and the Guarantee of Individual Rights

Therefore, Ulrich Beck's theorisation about the conflict between the protection of citizens' fundamental rights and the protection of public security (in some cases national security) till appears relevant.

Based on the aforementioned points, there are essentially five reasons why predictive policing software could harm the fundamental rights of individuals.

Firstly, there is the issue of the misperception of the algorithm's neutrality[63]. One of the major limitations related to the need for algorithm transparency, particularly regarding complex machine learning algorithms, stems from the intrinsic functioning of the algorithm (the mentioned black box issue). In brief, if the source code and the learning dataset are known, it is instead difficult to understand the functioning model of the algorithm developed because of machine learning. This aspect is linked to the fact that the algorithm reflects biases (i.e. distortions in the evaluation of facts or events) that are the result of the social context in relation to which the data used to develop the algorithm was taken. The effects of this distortion of reality are thus amplified by the lack of knowledge of how the algorithm learns, precisely from data that reflect pre-existing biases: such as, for instance, the risk of overestimating the social danger linked to the perceived ethnicity of offenders[64].

---

[62] Lorenzo Algeri, 'Intelligenza artificiale e polizia predittiva', *cit.*, 730.

[63] Cf. Maria Bianca Armiento, 'La polizia predittiva come strumento di attuazione amministrativa delle regole', *cit.*, 993.

[64] The current level of development of AI image generation software is greatly affected by bias. This is witnessed, for example, by Federico Bianchi, Pratyusha Kalluri, Esin Durmus, Faisal

The second problem (which, from a certain point of view, can be considered a different facet of the first) stems instead from the degree of accuracy of the algorithm, especially in relation to machine learning algorithms[65]. Given that such complex algorithms are based on datasets, on the basis of which they develop their learning model, there is a strong necessity to have an accurate and non-redundant dataset. A lack of accuracy in the dataset results in a lack of accuracy within programming activity, which also affects the accuracy of the algorithm's learning model and results[66].

A third category of problems concerns the risk of a distorted use of the algorithm in relation to its purpose – such as for political reasons, but not only. A situation that may occur, for instance, in the use of such predictive tools to prepare dossiers, or directly target individuals deemed 'unfriendly' (e.g. judges, political opponents, etc.)[67]. A further distorting effect, which is outside the focus of this paper, is related to the violation of privacy in the face of the use of digital surveillance systems, which are the basis of predictive policing tools[68].

A further critical issue is linked to the risk of an incorrect functionality of administrative power, which could result in the ineffectiveness of control in the face of system effects. Considering, for example, the case of places considered dangerous, where the police would logically be led to intensify controls. However, this leaves other areas that are considered safe with fewer patrols; and precisely because they are considered safe, they could be targeted

---

Ladhak, Myra Cheng, Debora Nozza, Tatsunori Hashimoto, Dan Jurafsky, James Zou, Aylin Caliskan, 'Easily Accessible Text-to-Image Generation Amplifies Demographic Stereotypes at Large Scale' (2023), *FAccT '23*, June 12–15, 1493 ff., <https://s.uniupo.it/s51k4> accessed 21st October 2025, that points out that the outputs of AI-generated images based on specific queries (e.g. 'a thug', 'a happy family') show racist results. The risk of overestimation based on ethnicity leads to real situations of inequality. For instance, in the US people of Afro-American ethnicity are 2.5 times more likely to be killed during a police arrest than people of Caucasian ethnicity: cf. Frank Edwards, Hedwig Lee, Michael Esposito, 'Risk of being killed by police use of force in the United States by age, race–ethnicity, and sex' (2019), *Proceedings of the National Academy of Sciences of the United States of America*, <https://s.uniupo.it/81qkn> accessed 21st October 2025.

[65] In this way, even more in general, see Gherardo Carullo, 'Large Language Models for Transparent and Intelligible AI-Assisted Public Decision-Making', *cit*, 11.

[66] On these links, see Mehryar Mohri, Afshin Rostamizadeh, Ameet Talwalkar, *Foundations of Machine Learning* (MIT Press 2018).

[67] This risk tends to exist in the use of many tools and in various fields. Nevertheless, the exponential potential of predictive policing tools could merely increase the negative consequences of such misuse.

[68] Cf. Lorenzo Algeri, 'Intelligenza artificiale e polizia predittiva', *cit.*, 732.

by criminals, who would be less likely to encountering the police there and, consequently, would be attracted by the opportunity to commit crimes there[69].

Finally, the fifth reasons why predictive policing software could infringe on individuals' fundamental rights is linked to a possible (dystopian) de-responsibility of civil servants, if the decisions were solely and exclusively taken by the algorithm[70] – the latter aspect that could be prevented precisely by the already mentioned principle of non-exclusivity of automated systems[71].

Beyond these critical aspects, and leaving aside for a moment the issue of fundamental rights, it is undeniable that the high level of digital processing of data and the large amounts of data available (big data analysis) could bring enormous advantages in terms of functionality and effectiveness of the analytical activity. Which leads one to consider the recourse to digital tools of predictive policing as effective on a technical level (with the limitations just underlined) as dangerous for the guarantee of the fundamental rights of individuals.

VI. Concluding Reflections. 'It's not worth the risk'

As a result of the technology's potential, there is a clear need to utilise it by reducing (as much as possible) the highlighted key problems.

An initial solution might be to ensure the transparency of algorithms, based on jurisprudential principles of algorithmic administration. Such a reconstruction, however, could contradict the rationale of predictive policing, i.e. ensuring public safety and national security.

Central in this context is Directive (EU) 2016/680 on the protection of individuals with regard to the processing of personal data by law enforcement authorities[72].

---

[69] This example is reported by Maria Bianca Armiento, 'La polizia predittiva come strumento di attuazione amministrativa delle regole', *cit.*, 995.

[70] This is an expression of defensive bureaucracy, also known as 'fear of signing'. On this topic, in general, see Jef De Mot, Michael G. Faure, 'Discretion and the economics of defensive behaviour by public bodies' (2016), *Maastricht Journal of European and Comparative Law*, 23:4, 595 ff.

[71] See Council of State, VI sect., decision 04/02/2020, No. 881.

[72] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, 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, and repealing Council Framework Decision 2008/977/JHA, <https://s.uniupo.it/cy1vm> accessed 21st October 2025.

Given that the Directive provides for the protection of personal data both at the phase of processing by default (privacy by default), but also at the programming phase of the processing system (privacy by design)[73], its framework requires a data protection impact assessment in relation to the processing[74]. It provides that if the processing of personal data poses a high risk to the rights and freedoms of individuals, then the controller (i.e. the police officer) must conduct an impact assessment of the data processing on those rights.

This impact assessment must contain a general description of the processing, an assessment of the risks to the individual rights concerned, specific measures to avoid risks of harm, and mechanisms to protect the data. In any case, pseudonymisation of personal data must always be ensured for each processing operation. Moreover, the storage of these personal data may not exceed twenty-five years.

Predictive policing cannot, therefore, disregard a related impact assessment of the specific risk posed by personal data processing to the fundamental rights of the individuals involved.

This perspective is also mirrored in the approach followed by the EU AI Act. In fact, as previously highlighted, this Act is built precisely on a risk-based approach of such systems on individuals' fundamental rights. Considered a sphere of unacceptable risk (the third, most severe level of risk), it is, for instance, forbidden to use AI tools and machine learning algorithms to classify individuals based on sensitive characteristics, to carry out social scoring, and to carry out remote biometric identification.

Although the EU AI Act includes real-time remote biometric identification systems among prohibited AI practices[75] – thus establishing the prohibition of its use as a *general* rule[76] – it does not prohibit the use of biometric identification systems carried out *ex post*[77]. Consequently, the Act provides for the possibility of using remote biometric identification of a non-preventive nature, in order to prosecute serious crimes that have already been committed, subject to authorisation by a judge. In this way, it would currently be possible to use predictive policing systems with post-crime features and for reasons justified by the protection of national security. Therefore, the choice of the European legislator is to prohibit only the use of pre-crime, predictive policing algorithmic tools, while allowing other types.

---

[73] Cf. Article No. 20 Directive (EU) 2016/680.

[74] Cf. Article No. 27 Directive (EU) 2016/680.

[75] Cf. Article No. 5 Regulation (EU) 2024/1689.

[76] The Regulation does, however, make some exceptions to this general rule. See in particular Article No. 5 para. 2–7 Regulation (EU) 2024/1689.

[77] Cf. Article No. 26 Regulation (EU) 2024/1689, that includes these AI systems among the high-risk ones.

From the regulatory framework, it thus emerges that the institutions aim, on the one hand, to prevent mass surveillance and, on the other hand, to protect the fundamental rights of individuals. To this purpose, the rules allow the use of remote biometric identification only in very limited and strictly regulated circumstances, in particular as regards real-time use in public spaces by the police.

Considering this, if we wish to conduct a purely theoretical exercise disregarding the regulatory framework, it is worth asking whether it is conceivable to seize the opportunities offered by predictive systems while minimising the associated risks, thereby allowing the use of such predictive policing tools. It is also worth asking whether there are areas in which the use of such tools could also be beneficial for the protection of individuals' fundamental rights.

On the one hand, it is evident that human intervention by public officials would seem indispensable, precisely because of the pervasiveness of these technological tools; this would be in line with the Italian judicial interpretation of the aforementioned principle of the non-exclusivity of automated procedures. However, this aspect would negatively affect the effectiveness of predictive tools, for which *ex post* control by a human would be pointless, to say the least.

On the other hand, it would be necessary for police forces to use predictive tools as one of the many investigative tools at their disposal, without relying exclusively on predictive results.

In fact, it would be necessary to be aware of the practical limitations of using these technological instruments, and not to rely on them blindly and 'passively' (suffering their indirect effects). A case in point was the October 2023 attack by the terrorist group Hamas against Israel, in which rudimentary aerial raid systems (hang gliders) were used to avoid being intercepted and shot down by defence systems designed for more technologically advanced weapons and aircraft.

The national security issue, especially in the context of warfare, has demonstrated the use of pseudo-predictive and automated (military) policing tools. In fact, in the first months of the war in Ukraine, some Russian mercenaries of the Wagner Brigade were portrayed in a photo that they later posted on social networks. Apart from the Russian mercenaries, some buildings also appeared in the image. Automatic online image recognition and comparison systems (so-called OSINT[78]) employed by the Ukrainians allowed them to identify the precise area where the photo was taken. This area was

[78] OSINT is the acronym of 'Open-Source Intelligence', i.e. the use of freely accessible information for intelligence and espionage activities. About this topic, see *ex multis* Ludo Block, 'The long history of OSINT' (2023), *Journal of Intelligence History*, Vol. 23, 2, 95 ff.

subsequently bombed with precision, killing Russian soldiers without hitting civilians[79].

This example shows that the analysis of data (especially those found on social networks) used as a tool for intelligence and fact prevention, has been employed for a long time – at least in the context of warfare. It has not, however, been used in civilian contexts, which are instead the subject of the regulatory efforts analysed in the paper.

Therefore, the answer to the first question must be negative, as the technically objective (unconditional) use of these instruments would inevitably have an unacceptable negative impact on the legal sphere of individuals.

Nevertheless, an objective (unconditional) use of predictive policing tools in cyber defence and cyber espionage systems could also be useful. As is well known, cyber security has four dimensions: cyber-resilience, cyber-crime, cyber-intelligence, and cyber-warfare[80]. In all these areas of cybersecurity[81], the adoption of fully (and unconditional) automated predictive policing tools to counter and prevent cyber-attacks, on networks and software source codes, could be used to ensure national defence and security, while saving many lives, without threatening individuals' fundamental rights (but rather guaranteeing them).

This marginal area is probably the 'exception that proves the rule'. The unconditional use of these tools is too risky for the integrity of individuals' fundamental rights, which is why the EU legislator decided to not allow their use, seems reasonable. Ultimately, however appealing the idea of using these tools may be, given their disruptive effects, in a democratic context, the sacrifice of individuals' fundamental rights would be too great: 'it's not worth the risk'.

[79] Cf. Ben Kesslen, 'Ukraine hits base of Russian paramilitary group Wagner after photos revealed location' (2022), *New York Post*, August 15, <https://s.uniupo.it/7gynl> (accessed 21st October 2025).

[80] In this way, the 2022–2026 Italian National Cyber-Security Strategy: cf. Agenzia per la Cybersicurezza Nazionale – ACN, *Strategia nazionale di cybersicurezza 2022–2026* (2021), <https://s.uniupo.it/s6a0p> accessed 21st October 2025.

[81] On this topic, see Stefano Rossa, 'Administrative Law Reflections on Cybersecurity, and on its Institutional Actors, in the European Union and Italy' (2022), *Italian Journal of Public Law*, Vol. 14, (2), 426 ff.

Funding
This article received no funding.

Declaration of Conflict of Interests
The authors declared no potential conflicts of interest with respect to the research, authorship and publication of this article.

Declaration about the scope of AI utilisation
The author did not use artificial intelligence tools in the preparation of this article, except for the translation of the abstract into French.