REGULATING PREDICTIVE POLICING THROUGH HUMAN SECURITY. INSIGHTS FROM THE US AND EUROPE

Daiana MauraVESMAȘ[1]
Andreea Nicoleta DRAGOMIR[2]
Ana MORARI (BAYRAKTAR)[3]
https://doi.org/10.54989/stusec.2025.19.02.03

Abstract

In a world where big data analytics and artificial intelligence are rapidly evolving into new forms of policing, attention has returned to the delicate line between public security and individual rights. Therefore, this article presents a modern, empirical framework on predictive policing technologies and defines human security as the protection of the individual that takes into consideration seven facets defined by the 1994 UNDP Report. With the rise of automated systems making decisions relating to suspicions and risks, the long-standing guarantees of presumption of innocence, equality of arms, and the right to a fair trial are under significant pressure. The analysis is doctrinal and interdisciplinary, based on developments in Europe and internationally. By examining experiences from the United States and Europe, the article highlights the contrasting ways in which democratic systems attempt to regulate predictive policing and balance efficiency with fundamental rights.

The focus is also on the new EU regulatory framework, namely the Artificial Intelligence Act, protections under the GDPR for automated decision making and the European Court of Human Rights' precedents in decisions like S. and Marper, Gaughran and Big Brother Watch. Used collectively, this brings critical standards to bear on the question of whether algorithmic policing can fit in with democratic legality. Predictive policing will continue to be deeply contested unless we have real institutional defenses to ensure transparency, accountability, and meaningful human oversight. To the extent that legal systems can manage the tension between technological disruption and respect for human dignity will ultimately decide the resilience of the rule of law in the age of algorithms.

Keywords: predictive policing; human security; artificial intelligence; algorithmic accountability; fundamental rights; rule of law

Introduction

[1] Associate Professor in the Department of Public Law, Faculty of Law, Lucian Blaga University of Sibiu, Romania. Her research and teaching are focused on administrative law, sustainable development, performance management, and public governance. https://ORCID.org/0009-0001-8464-3542, daiana.vesmas@ulbsibiu.ro
[2] Lecturer at the Faculty of Law, Lucian Blaga University of Sibiu, Romania. Her teaching and research focus on European Union law, security and defence policy, as well as cybersecurity governance and public-private partnerships in security. https://ORCID.org/0000-0002-9358-8098, andreea.dragomir@ulbsibiu.ro
[3] PhD Candidate, Faculty of Law, Lucian Blaga University of Sibiu, Romania. Her research and teaching focus on cybersecurity law, digital governance, and the legal implications of emerging technologies, with a particular interest in human security and data protection. She also examines technological transformations in public administration, cyber-diplomacy, and EU strategies against disinformation. https://ORCID.org/0009-0002-9363-8718, ana.morari@ulbsibiu.ro

The use of artificial intelligence (AI) and big data analytics in policing is one of the emerging developments in public security systems.

The notion of human security requires a precise doctrinal and institutional definition to assess the implications of predictive policing technologies. Modern notions of human security derive from the 1994 United Nations Development Programme (UNDP) Report, which shifted the focus from state-centred security to the protection of individuals. The report identifies seven interdependent dimensions, economic, food, health, environmental, personal, community, and political security, each contributing to a holistic vision of safety and human dignity[1]. Human security is consequently closely associated with the international human rights framework as it focuses on the protection and empowerment of individuals in contexts where technological or institutional practices may affect their fundamental rights. In light of this context, the evaluation of predictive policing systems must consider not only operational efficiency, but also the extent to which such technologies reinforce or undermine these core dimensions of human security.

Predictive policing, based on automated machine learning systems[2], uses algorithmic analysis of historical and sociodemographic data collected in large databases to identify the location, time of possible crime scenes or persons at risk before crimes are committed[3]. The shift from reactive to preventive policing has altered institutional priorities and sparked an international debate about the ethical, legal, and social ramifications of this shift. This study follows a doctrinal and qualitative analytical approach, combining legal interpretation with an examination of recent technological developments in predictive policing.

In the United States, predictive policing systems PredPol[4] [5] and HunchLab[6] [7] are now part of police programs in major cities. Reports from Los Angeles have shown a short-term decline in property crimes of approximately 4-11%, but have also sparked debates about racial profiling, transparency and constitutional rights[8]. Empirical evaluations from the United States show that some departments using PredPol reported short-term declines in property crimes - generally between 4% and 11% - particularly in Los Angeles and Atlanta, where patrol allocation was adjusted according to algorithmic forecasts. However, subsequent assessments have highlighted the instability of such gains, noting that reductions often diminish over time, while systemic biases in underlying datasets, methodological opacity, and

[1] United Nations Development Programme (UNDP), *Human Development Report 1994*, Oxford University Press, 1994

[2] Machine learning is a branch of AI that enables computers to learn from data and improve their performance automatically without being explicitly programmed. Instead of following fixed rules, ML algorithms detect patterns to make predictions or decisions.

[3] Paria Sarzaeim, Qusay H. Mahmoud, Akramul Azim, *A Framework for LLM-Assisted Smart Policing System*, "IEEE Access", Vol. 12, 2024, pp. 74915-74929, https://doi.org/10.1109/access.2024.3404862 (11.11.2025)

[4] The first predictive policing software was developed in 2011 through collaboration between researchers from three universities and the Santa Cruz Police Department. The system analysed three basic variables (type of crime, date, time and location) to generate maps of hotspots.

[5] Ishmael Mugari, Emeka E. Obioha, *Predictive Policing and Crime Control in the United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing*, "Social Science", Vol. 10, No. 6 (2021), p. 5., https://www.mdpi.com/2076-0760/10/6/234 (02.11.2025)

[6] HunchLab integrates multiple variables (crime rates, recidivism patterns, socioeconomic and temporal factors, local events) to generate predictions. Using machine learning, it updates predictions for each police shift and provides real-time risk maps on mobile devices, guiding officers to areas with a high probability of crime.

[7] *Ibidem Note 7*, p. 6

[8] Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, "Emory Law Journal", Vol. 62, 2012, p. 270, https://scholarlycommons.law.emory.edu/elj/vol62/iss2/1 (02.11.2025)

community-level contestations raise questions about the generalizability and long-term reliability of these reported effects.

Although much of the initial literature on predictive policing has focused on the North American space, the discussion cannot be separated from the European context, where the development of these technologies is directly conditioned by a much more demanding legal framework. In the European Union, recent regulatory developments, in particular the Artificial Intelligence Regulation (AI Act), the General Data Protection Regulation (GDPR) and the consistent case law of the European Court of Human Rights on state surveillance, outline high standards of transparency, necessity and proportionality. These benchmarks give the analysis of predictive policing a distinct dimension in the European space, where the protection of fundamental rights occupies a central place in the assessment of technologies used by law enforcement authorities.

The topic has gained particular relevance in both European and international debates, as states seek to modernize their security practices while maintaining compliance with constitutional and human rights standards. In Europe, PRECOBS and the Crime Anticipation System, framed as part of policing initiatives, aimed to shift crime control from reaction to anticipation and prevention. Using historical data and spatial analysis, they identify areas where offenses are statistically likely to recur, the so-called near-repeat phenomenon[1]. In Indonesia[2], the national police have begun testing AI-based predictive systems to map areas with high crime potential, marking an important step toward law enforcement in the digital realm[3].

Across jurisdictions, predictive policing has taken diverse operational forms. In the United States, systems such as PredPol and HunchLab have been deployed in major cities to anticipate property crimes and gun-related violence. In the United Kingdom, authorities have experimented with hot-spot mapping and the integration of facial-recognition-linked risk assessments. China has implemented predictive surveillance at a much broader scale, combining behavioural data and social scoring techniques, raising significant human-rights concerns. In Europe, France and Germany have used predictive models primarily for burglary forecasting and spatial crime pattern analysis, while in Brazil and Mexico algorithmic tools have focused on identifying zones with heightened risk of violent crime, often in contexts marked by unequal policing. These comparative examples illustrate that predictive policing is not confined to a single legal or institutional model, but operates across heterogeneous environments with varying safeguards and vulnerabilities.

In this context, scientific research on predictive policing is conducted through the lens of human security and the rule of law. Although predictive systems claim to increase safety and efficiency, they simultaneously jeopardize fundamental legal principles: equality of arms, presumption of innocence and the right to a fair trial. Consequently, this research aims to: examine the compatibility of predictive policing with the principles of human security and fair trial guarantees; analyses the legal and institutional mechanisms capable of ensuring transparency, accountability and democratic oversight of algorithmic systems; and assess how these mechanisms can prevent the arbitrary, discriminatory, or abusive application of AI policing. Finally, we will highlight the delicate balance between effective crime prevention

[1] *Ibidem.,* p.7

[2] Indonesia has also piloted limited AI-driven crime-mapping tools within its national police structures, although these initiatives remain less developed compared to the models implemented in the United States or Europe

[3] Radyan Kunto Wibisono, Joko Setiono, Ilham Prisgunanto, *Artificial Intelligence in Predictive Policing: A Systematic Literature Review and Its Implications for Indonesia*, ”Jurnal Greenation Sosial dan Politik”, 2025, pp. 597–598, https://doi.org/10.38035/jgsp.v3i3 (11.11.2025)

and the protection of individual rights. The resilience of the rule of law in the algorithmic age will depend on how societies reconcile technological innovation with the enduring imperative of human dignity and justice.

Methodological Approach

This article employs a doctrinal and interdisciplinary analytical methodology, combining legal analysis with insights from security studies, data governance, and algorithmic accountability. The study is informed by a qualitative examination of relevant legislation, jurisprudence, academic literature, and technical documentation concerning predictive policing algorithms. Conceptual analysis is employed to clarify the relationship between predictive policing and the principle of human security, and comparative elements are introduced when necessary to contrast approaches developed by EU law, U.S. constitutional doctrine, and emerging international standards. Its methodological framework aims to furnish a coherent legal evaluation of algorithmic policing tools and to determine whether human security can function as a normative benchmark in the regulation of automated decision-making systems used by law enforcement agencies. In particular, the methodology aims to integrate relevant European standards, as they provide one of the most developed and restrictive frameworks for evaluating the use of algorithms in law enforcement. This framework positions the study within current European and international debates on algorithmic governance and the future of law enforcement.

Predictive Policing and Automated Suspicion Algorithms (ASAs)

In an era where data increasingly influences decisions about safety and justice, understanding the intersection of technology and human security becomes essential. The idea of human security offers a lens through which to examine how new technologies influence the balance between state power and personal freedom. Predictive policing is a modern approach that helps police anticipate crimes before they occur. New tools, such as *Risk Terrain Modelling (RTM)* and *prospective hot spot analysis*, make predictions more accurate by identifying *temporary high-risk areas* that change over time[1]. These systems help police act proactively, but they should support, not replace, human judgment, because algorithms can show patterns but cannot explain the social causes behind them.

Predictive policing is based on the idea of *pattern-based suspicion*, the belief that data on past crimes contain detectable regularities that can predict future crimes. According to Meijer's definition, PP involves collecting and analyzing data on past crimes to identify individuals or locations with a higher statistical probability of criminal activity, guiding both preventive and intervention strategies[2]. Unlike traditional crime analysis, which relied on human intuition and experience, these systems can distinguish between person-based and place-based predictions[3]. Through this process, predictive algorithms transform uncertainty into probability, converting subjective judgment into seemingly objective calculations[4].

[1] Wim Hardyns, Anneleen Rummens, *Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges*, "European Journal on Criminal Policy and Research", 2017, pp. 3–4, https://doi.org/10.1007/s10610-017-9361-2 (02.11.2025)

[2] Duncan Purves, *Fairness in Algorithmic Policing*, "Journal of the American Philosophical Association", 2022, pp. 742–743, https://doi.org/10.1017/apa.2021.39, (02.11.2025)

[3] Gavin Rosser, Toby Davies, Kate Bowers, Shane Johnson, Tao Cheng, *Predictive Crime Mapping: Arbitrary Grids or Street Networks?*, "Journal of Quantitative Criminology", 2016, pp. 569–594, https://doi.org/10.1007/s10940-016-9321-x (02.11.2025)

[4] Duncan Purves, *Op.cit.,* p. 742-743

The next stage in this evolution is represented by automated suspicion algorithms (ASAs). These are machine learning systems trained on vast data sets from government and private sources to detect individuals "suspected of involvement in criminal activity[1]. Unlike earlier analytical tools, ASAs intervene directly in the legal process by automating the inference of reasonable suspicion, a judgment that has traditionally belonged exclusively to human officers. In doing so, they transform a foundational element of criminal procedure into a computational process that risks detaching suspicion from context or accountability[2].

A clear example of such an ASA is Chicago's *Strategic Subject List (SSL),* a database that used arrest and fingerprint data from 2012–2016 to assign each person a risk score for *gun violence*. The algorithm considered multiple variables to predict whether someone might later be a shooter or a victim[3]. Although race and gender were not explicitly included, researchers found that the model indirectly reproduced racial and social biases, disproportionately targeting young Black men in economically deprived areas[4].

Urban predictive models often reinforce systemic biases in law enforcement, unevenly redistributing police attention across different social groups and geographic areas. Algorithmic predictions tend to concentrate surveillance in already over-policed and marginalized neighborhoods, while wealthier or less diverse areas benefit from increased protection and visibility[5]. This imbalance arises because predictive systems rely heavily on historical data on arrests and incidents, which already reflect the effects of discriminatory policing practices. When such biased datasets are used for new predictions, they generate self-reinforcing feedback loops, in which past patterns of law enforcement are mistaken for objective indicators of crime. It is important to note that these systems operate on statistical correlations rather than proven causal relationships, meaning that their predictions reflect patterned associations in the data rather than any verified link between past and future behavior.

As a result, algorithms not only reproduce but also amplify structural inequalities, shaping perceptions of crime and influencing how justice and security are distributed in urban spaces. The human dimension remains crucial. Police officers often negotiate algorithmic outputs with their professional discretion, revealing tension between technological authority and human agency. Predictive systems do not eliminate judgment; they reshape it, embedding institutional priorities and computational logics into daily policing practice.

Legal and Ethical Challenges

The rise of predictive policing and Automated Suspicion Algorithms (ASAs) introduces profound legal and ethical dilemmas for modern criminal justice systems. These

[1] Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, „University of Pennsylvania Law Review", Vol. 164, 2016, p. 872, https://scholarship.law.upenn.edu/penn_law_review/vol164/iss4/2 (02.11.2025)

[2] Kyriakos N. Kotsoglou, Marion Oswald, *The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention*, "Forensic Science International: Synergy", Vol. 2, 2020, pp. 86-89, https://doi.org/10.1016/j.fsisyn.2020.01.002 (02.11.2025)

[3] Andrea L. DaViera, Bruce D. Baker, Linda R. Tropp, *Risk, Race, and Predictive Policing: A Critical Race Theory Analysis of the Strategic Subject List*, "American Journal of Community Psychology", 2022, pp. 93–94, DOI: 10.1002/ajcp.12671, https://pubmed.ncbi.nlm.nih.gov/37067014/ (02.11.2025)

[4] Renata M. O'Donnell, *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause*, "New York University Law Review", 2019, https://Nyulawreview.Org/Wp-Content/Uploads/2019/06/Nyulawreview-94-3-Odonnell.Pdf (02.11.2025)

[5] Victor Rotaru et al., *Precise Event-level Prediction of Urban Crime Reveals Signature of Enforcement Bias*, "Research Square", 2021, DOI: https://doi.org/10.21203/rs.3.rs-192156/v1 (05.11.2025)

technologies operate at the intersection of efficiency and accountability, promising objective decision-making while simultaneously raising concerns about privacy, due process, discrimination, and transparency.

Supporters of predictive policing argue that algorithmic tools can ease the operational burden on police forces, enabling earlier interventions in high-risk areas and helping officers allocate resources more efficiently. They also contend that, when properly designed, such systems may reduce certain forms of human judgment bias by grounding decisions in structured data rather than intuition. From this perspective, predictive models are presented not as replacements for professional discretion but as instruments that could strengthen evidence-based policing.

At the same time, several jurisdictions have begun implementing safeguards designed to reduce the risks associated with algorithmic policing. Bias audits, conducted periodically by independent bodies, aim to detect and mitigate discriminatory patterns embedded in training data. Complementary mechanisms such as explainable AI requirements and human-in-the-loop supervision seek to ensure that algorithmic outputs remain intelligible, contestable and ultimately subordinate to accountable human decision-making.

Erosion of Reasonable Suspicion

The emergence of automated suspicion algorithms (ASAs) and predictive policing represents a significant shift in how suspicion is formulated and sustained in contemporary law enforcement. The Fourth Amendment and other constitutional protections served as the basis for the traditional theory of reasonable suspicion, which required a police officer to provide specific, observable facts suggesting that a person was involved in a crime[1].

But this idea is beginning to be undermined by the increased reliance on algorithmic prediction and big data analysis, which replace individualized assessment with probabilistic inference[2]. Data-driven analysis, on the one hand, can reduce biases and errors based on human judgment by police officers, often influenced by race, social class, or age, and replace them with objective information. Instant checks using license plate readers, facial recognition, or databases can confirm identities, detect criminal connections, or quickly exonerate innocent people[3]. However, data errors, outdated records and biased data sets can produce false positives, flagging individuals as suspects based on erroneous correlations. Those who have been arrested before or who live in an area with heavy police surveillance remain under continuous algorithmic surveillance – the so-called" digital scarlet letter"[4].

Predictive analytics is increasingly integrated into the "total circumstances" test, expanding the range of factors that can satisfy a stop or search[5]. Police officers are no longer limited to what they observe directly; rather, they can rely on digital predictions that indicate that a person, place, or object is "statistically linked" to a crime. This evolution transforms the standard of reasonable suspicion from a context-dependent legal judgment to a data-driven

[1] Kaitlynd Hiller, *Predictive Policing and the Charter*, "Manitoba Law Journal", 2022, p. 237, https://doi.org/10.29173/mlj1303 (05.11.2025)

[2] Emily Berman, *Individualized Suspicion in the Age of Big Data*, "Iowa Law Review", Vol. 105, 2020, p. 491, https://www.questia.com/library/journal/1P4-2381617248/individualized-suspicion-in-the-age-of-big-data (02.11.2025)

[3] Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, "University of Pennsylvania Law Review", 2015, pp. 388–389

[4] *Idem*

[5] Fabio Arcila Jr., *Nuance, Technology, and the Fourth Amendment: A Response to Predictive Policing and Reasonable Suspicion*, Legal Studies Research Paper Series, No. 15-11, 2014, p.4, https://scholarlycommons.law.emory.edu/elj-online/30 (10.11.2025)

statement of probability[1]. In practice, predictive systems generate an appearance of scientific neutrality, even though they operate based on complex assumptions, historical biases, and opaque algorithms. This development undermines the very purpose of reasonable suspicion. When machine learning models flag a person as "high risk" based on these statistical correlations, they are often treated as equivalent to individualized suspicion[2]. However, the logic of prediction is fundamentally different from the logic of justification. Probability scores describe what might happen, not what has happened[3]. As such, the use of algorithmic predictions as a legal trigger redefines suspicion from a reasoned assessment of human behavior to an actuarial calculation of risk[4].

This dependency introduces a ”constitutional shortcut” into policing, eroding safeguards designed to prevent pretextual or discriminatory interventions. Probabilistic policing encourages what he calls ”preventive law enforcement without cause”, an approach that risks normalizing the logic of pre-criminality, in which suspicion is directed toward potential future behavior rather than current actions[5]. These predictive mechanisms do not operate in a social vacuum. They tend to reinforce existing inequalities, as the data used to train algorithms often reflects historical police biases, disproportionately targeting marginalized communities[6]. When such data is fed into new predictive systems, it creates self-reinforcing feedback loops - the same neighborhoods and individuals flagged in the past become perpetual subjects of surveillance in the future.

From a human rights perspective, this erosion of reasonable suspicion challenges fundamental guarantees of proportionality, legality, and due process. As noted in Brazilian legal scholarship, algorithmic policing risks distorting the very boundaries of lawful intervention by transforming risk management into law enforcement[7].

Fundamental Rights at Risk

The principle of equality of arms, as part of the fundamental right to a fair trial, enshrines full access for the parties to the evidence used in the trial and a real opportunity to challenge its reliability.

Predictive policing tools often function as ”*black boxes*”, protected by proprietary and undisclosed code[8]. When defendants cannot see how the risk score was obtained, they cannot examine whether the data underlying it is even accurate. Instead, they are confronted with a numerical score, which inevitably becomes a powerful and seemingly authoritative indicator[9].

---

[1] *Ibidem,* p.7

[2] Lindsey Barrett, *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, “N.Y.U. Review of Law & Social Change”, Vol. 41, Issue 3 (2017), https://socialchangenyu.com/review/reasonably-suspicious-algorithms-predictive-policing-at-the-united-states-border/ (10.11.2025)

[3] Bernadette McSherry, *Risk Assessment, Predictive Algorithms and Preventive Justice*, Palgrave Macmillan, Cham, 2020, pp. 17-42, https://doi.org/10.1007/978-3-030-37948-3_2 (10.11.2025)

[4] Lindsey Barrett, *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, “N.Y.U. Review of Law & Social Change”, Vol. 41, No. 3 (2017), https://socialchangenyu.com/review/reasonably-suspicious-algorithms-predictive-policing-at-the-united-states-border/ (10.11.2025)

[5] Fabio Arcila, *Op. cit.,* p.5

[6] Kaitlynd Hiller, *Op. cit., p. 281*

[7] Antonio José Cacheado Loureiro et al., *Reasonable Suspicion and Predictive Policing: Technology and Legality in the Context of Brazilian Public Security*, “Revista PPC – Políticas Públicas e Cidades”, 2024, https://doi.org/10.23900/2359-1552v13n2-407-2024 (11.11.2025)

[8] Sonia K. Katyal, *The Paradox of Source Code Secrecy*, “Social Science Research Network (SSRN)”, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3409578, (11.11.2025)

[9] Nicki James Shepherd, *Algorithmic Justice: The Legal Implications of AI in Criminal Sentencing and Risk Assessment*, “Journal of Artificial Intelligence General Science”, Vol. 8 (2025), https://doi.org/10.60087/jaigs.v8i1.391 (10.11.2025)

A high-risk individual presenting a score to a judge can create an implicit presumption of future guilt, shifting the burden of proof onto the defendant. Instead of the state justifying the use of predictive evidence, the defendant must attempt to refute an algorithmic prediction whose logic remains inaccessible[1]. This reversal undermines procedural equality and erodes the presumption of innocence, placing individuals at a structural disadvantage simply because technology labels them as a high risk[2].

Moreover, this imbalance is exacerbated by *legal gaps*. Existing legal frameworks, including civil law and administrative liability rules, *are not equipped to deal with harm caused by AI-based decision-making systems*. When public agencies develop tools in collaboration with private technology firms, responsibility becomes diffuse and often impossible to attribute. The result is a growing vacuum of accountability, in which technological opacity becomes a shield against legal scrutiny[3]. Taken together, these transparency deficits reveal why procedural fairness is at risk: when states rely on opaque AI tools to justify coercive actions, the defendant loses the ability to meaningfully challenge the evidence, and the judiciary loses the ability to ensure that the evidence meets constitutional standards[4].

Against this backdrop, AI tools used by police or courts cannot be allowed to operate as inscrutable machines that convert probabilistic inferences into authoritative conclusions. Without mandatory explainability, independent oversight, and the ability for individuals to demand review or correction, algorithmic outputs risk being treated as objective facts - even though they are built on historical data, value-laden design choices, and potential biases[5].

The Dutch SyRI system has linked tax, social assistance, and other registries to generate *fraud risk reports* without disclosing the risk model, indicators, or even notifying the individuals concerned, and has been applied in so-called "*problem districts*"[6]. In this context, individuals living in heavily monitored areas or appearing in multiple databases are much more likely to be flagged as "*high risk*," even if they have not committed any crime. This dynamic effectively transforms the presumption of innocence into a *conditional privilege*[7]. To safeguard these rights, a robust legal framework is essential - one that enforces algorithmic transparency, mandates human oversight, and ensures explainability of all AI systems used in law enforcement.

PredPol vs. HunchLab

Although PredPol and HunchLab are two radically different approaches to how crime occurs and how police should respond to it, predictive policing technologies often appear

[1] Alexandra L. Washington, *How to Argue with an Algorithm: Lessons from the COMPAS ProPublica Debate*, "Social Science Research Network (SSRN)", 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3357874 (11.11.2025)
[2] *Ibidem,* p.260
[3] Iwannudin Iwannudin, Istiana Heriani, Rajab Lestaluhu, *Legal Challenges in Regulating Artificial Intelligence Use in Criminal Justice Systems*, "The Journal of Academic Science", 2025, https://doi.org/10.59613/whvhd326 (11.11.2025)
[4] *Ibidem*., p. 1605
[5] Matúš Mesarčík, *Policajné profilovanie v kontexte základných ľudských práv a slobôd*, "Acta Facultatis Iuridicae Universitatis Comenianae", 2019, pp. 190–193
[6] Athina Sachoulidou, *Going beyond the "common suspects": To Be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence*, "Artificial Intelligence and Law", 2023, pp. 7–9, https://doi.org/10.1007/s10506-023-09347-w (10.11.2025)
[7] *Ibidem.,* pp. 7–9

similar at first glance. Assessing the operational value of these differences and their effects on justice, transparency, and the rule of law requires an understanding of them.

PredPol uses only three variables, crime type, time, and location, to predict where future crimes might occur. Because the system excludes demographic, ethnic, and socioeconomic indicators, PredPol promotes itself as "objective" and free from human bias (Figure 1)[1].

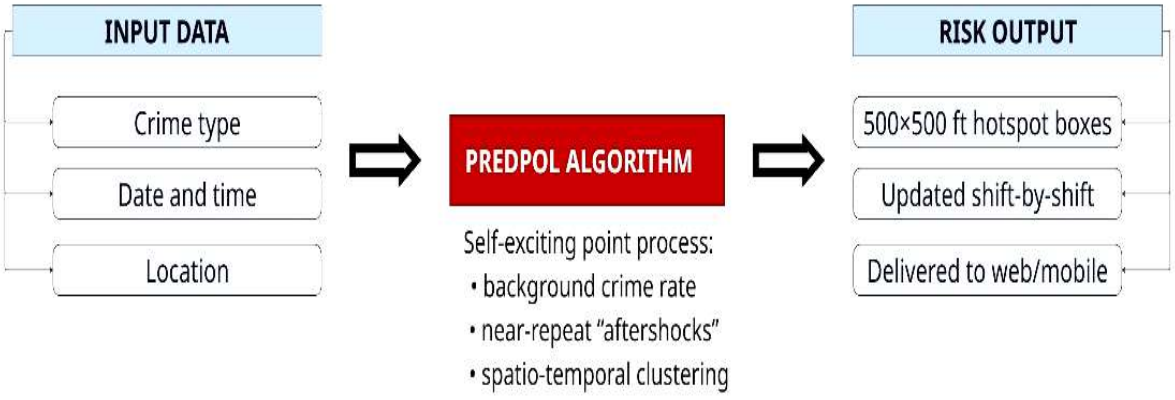

Figure 1. PredPol Predictive Policing Workflow[2]

Its results are equally simplified: officers receive small 500×500 ft red squares on a map for each shift, indicating where patrols should be concentrated. Police departments appreciate this ease of integration, and PredPol has rapidly expanded to cities across the US, such as Los Angeles, Atlanta, Richmond, and Chicago, and even to parts of the UK[3].

HunchLab represents a more complex, second-generation model. Unlike PredPol, which relies on thin historical data, HunchLab incorporates hundreds of variables, including weather conditions, public transport hubs, socio-economic indicators, and major events[4]. HunchLab applies Risk Terrain Modeling and machine learning to detect the underlying environmental and situational factors that create opportunities for crime (Figure 2)[5].

[1] Ajay Sandhu, Peter Fussey, *The "Uberization of Policing"? How Police Negotiate and Operationalise Predictive Policing Technology*, "Policing and Society", 2021, p. 69, https://doi.org/10.1080/10439463.2020.1803315 (10.11.2025)
[2] Figure designed by the article authors, based on the analysed data
[3] Wim Hardyns, Anneleen Rummens, *Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges*, "European Journal on Criminal Policy and Research", 2017, pp. 9–10, https://doi.org/10.1007/s10610-017-9361-2 (10.11.2025)
[4] Ajay Sandhu, Peter Fussey, *Op. cit.* p.69
[5] Simon Egbert, *Predictive Policing and the Platformization of Police Work*, "Surveillance & Society", 2019, p. 85, https://ojs.library.queensu.ca/index.php/surveillance-and-society/index (11.11.2025)

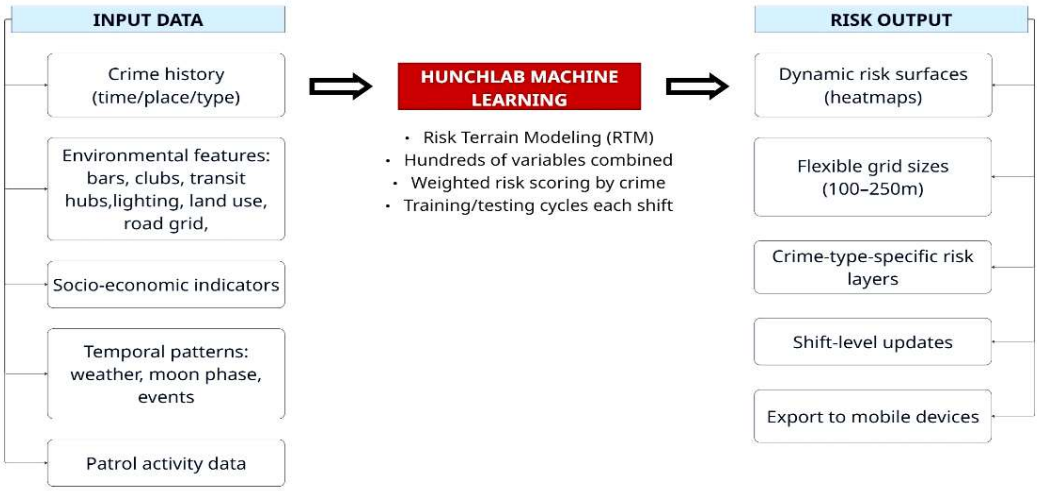

Figure 2. HunchLab Predictive Policing Workflow[1]

Despite these differences, both tools present similar normative problems (Table. 1). While HunchLab's complexity can obscure the process by which risk scores are generated, making judicial or democratic oversight difficult, PredPol's limited design makes it susceptible to perpetuating existing inequalities. HunchLab offers nuance but risks opacity and technocratic excess, while PredPol offers clarity but risks self-fulfilling surveillance loops.

Both systems demonstrate that predictive policing is more of a governance decision than just a technical advance, one that influences police priorities, relations between citizens and the state, and ultimately what public safety means in data-driven societies.

Legal Dimension	PredPol	HunchLab
Risk of Discrimination	Reinforces historical policing biases and concentrates surveillance in poor, non-white areas.	Uses socio-economic and environmental proxies that can indirectly reproduce structural discrimination.
Presumption of Innocence	Spatial “hotspot” logic risks treating all residents of a flagged zone as suspects.	Individualized and area-based risk scores may pre-criminalize entire communities.
Equality of Arms	Defendants cannot access model logic; limited ability to contest algorithmic evidence.	Even more opaque; impossible to know which variables influenced a risk designation.
Accountability	Outsourced to a private company; weak oversight and unclear responsibility.	More data sources and ML complexity create deeper accountability gaps and diffuse liability.
Compatibility with Rule of Law	Simplifies crime to location patterns; risks undermining human-centred policing.	Expands surveillance logic into social context; risks normalizing structural monitoring of daily life.

Table 1. PredPol vs. HunchLab[2]

[1] Figure designed by the article authors, based on the analyzed data
[2] Table designed by the article authors, based on the analysed data

European Legal Framework Applicable to Predictive Policing

The regulation of artificial intelligence in the European Union has evolved rapidly in recent years, driven by the need to reconcile technological innovation with the protection of fundamental rights. Any analysis of predictive policing from a legal perspective must therefore be anchored in the broader European framework governing automated decision-making, data processing, and state surveillance. The absence of such an analysis risks leaving the discussion incomplete, especially since predictive policing is one of the high-stakes fields explicitly addressed in recent legislative and judicial developments.

The Artificial Intelligence Act (AI Act) adopted by the European Union represents the most ambitious regulatory instrument for AI worldwide. Its relevance for predictive policing is direct and substantial. The text classifies certain AI systems used in law enforcement as "high-risk", while others, including real-time remote biometric identification in public spaces, are subject to strict prohibitions or nearly-prohibitive conditions.

Predictive policing tools fall within the high-risk category because they influence decisions that may significantly affect individuals' rights, including the right to liberty, privacy, non-discrimination, and access to justice. The AI Act requires that all high-risk systems comply with rigorous obligations:

- documented risk assessments,
- high-quality and bias-mitigated training data,
- transparency measures,
- human oversight ensuring the possibility of intervention,
- clear accountability structures for developers and deployers,
- operational logs enabling traceability and auditing.

These requirements fundamentally challenge the manner in which existing predictive policing systems operate. Many of them, such as those based on historical crime data or neighborhood-level profiling, rely on datasets marked by structural bias, incomplete variables, or disproportionate policing practices. In a European context, such systems would be presumptively incompatible with the AI Act unless they undergo extensive redesign and validation. Furthermore, the AI Act strengthens the principle of human-in-command, requiring law enforcement authorities to be able to override automated outputs. This represents a safeguard against the automated reproduction of discriminatory policing patterns frequently observed in academic studies on predictive policing[1].

While the AI Act and GDPR establish some of the most rigorous safeguards for algorithmic decision-making, their practical implementation presents significant challenges. Ensuring compliance requires substantial institutional resources, technical expertise, and the capacity of law enforcement agencies to conduct or commission independent audits capable of detecting bias or methodological flaws. Many police structures lack the infrastructural and human capital necessary to interpret complex machine-learning systems, creating risks of superficial oversight or overreliance on vendors. In practice, effective enforcement depends not only on formal legal requirements but also on sustained investment, cross-sector cooperation, and the development of specialized supervisory bodies capable of scrutinizing high-risk AI systems in real time.

[1] Duncan Purves, *Fairness in Algorithmic Policing*, "Journal of the American Philosophical Association", 2022, pp. 742–743, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A93BD2FBA25DEDBC6620B25D1C9A8A26/S2053447721000397a.pdf/fairness_in_algorithmic_policing.pdf (11.11.2025)

In parallel with the AI Act, the General Data Protection Regulation (GDPR) already provides a robust framework relevant to predictive policing. Three sets of provisions are crucial:

- Article 22 (prohibition of decisions based solely on automated processing),
- Article 13–14 (right to information),
- Article 15 (right of access to meaningful information about the logic involved).

Under Article 22, individuals have the right not to be subject to a decision based exclusively on automated processing which produces legal or similarly significant effects. Predictive policing outputs often determine enhanced surveillance of specific individuals or neighborhoods, the deployment of patrol units, or the classification of persons into high-risk categories. Even if these outputs do not amount to formal "decisions", they materially shape the behavior of police forces and may lead to disproportionate interventions. Academic literature has argued that such indirect effects still fall within the scope of Article 22, particularly when they expose individuals to heightened scrutiny[1].

GDPR Articles 13–15 impose transparency obligations: authorities must provide individuals with meaningful information about the logic underlying automated systems. In practice, this is extremely difficult when predictive policing systems use machine learning models trained on opaque datasets. Without a clear explanation, individuals cannot meaningfully contest the basis on which they have been labelled as "at-risk" or why their neighborhood is subject to increased patrols. Predictive policing thus raises structural tensions with the GDPR, revealing the limits of data protection law when applied to algorithmic policing.

Because predictive policing systems sometimes infer sensitive characteristics—such as ethnicity, migration status, or socio-economic vulnerability—their processing of data may indirectly involve special categories protected under Article 9 GDPR. Such inferences are often derived statistically rather than explicitly recorded, but the European Data Protection Board has clarified that inferred sensitive data also falls under heightened protection. This places additional restrictions on the legality of predictive policing systems whose datasets reflect racialized or socio-economic disparities.

Predictive policing systems must also be analyzed under the European Convention on Human Rights (ECHR) and the European Court of Human Rights's (ECtHR) jurisprudence. The relevance of the European Convention on Human Rights becomes clearer when considering the specific safeguards embedded in its core provisions. Article 6 guarantees the right to a fair trial, encompassing equality of arms and the ability to challenge evidence used by the state. Article 8 protects the right to private life, requiring that any interference, such as large-scale data retention or predictive surveillance, meet strict tests of legality, necessity, and proportionality. Article 13 ensures individuals an effective remedy before an independent authority, while Article 14 prohibits discrimination in the enjoyment of Convention rights, a safeguard particularly important where algorithmic systems risk amplifying structural biases[2]. Although the Court has not yet ruled on predictive algorithms, it does provide its case law on data retention, biometric databases, and state surveillance, a thorough footing to evaluate the compatibility of predictive policing with the Convention.

[1] Emily Berman, *Individualized Suspicion in the Age of Big Data*, "Iowa Law Review", Vol. 105, 2020, p. 491, https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2022-10/Individualized%20Suspicion%20in%20the%20Age%20of%20Big%20Data%20.pdf (11.11.2025)

[2] Articles 6, 8, 13 and 14 ECHR provide the central safeguards relevant in this context: the right to a fair trial, the right to private life, the right to an effective remedy and the prohibition of discrimination.

In the case S. and Marper v. United Kingdom (2008), the Court ruled that the continual retention of fingerprints and DNA profiles of people not convicted of a crime constitutes a violation of Article 8 ECHR (the right to private life)[1]. The judgment also highlighted the increased sensitivity of biometric information and the need for strong necessity and proportionality. Thus, predictive policing systems based on biometric or behavior pattern data have very high justification thresholds.

In Gaughran v. United Kingdom (2020)[2], the Court found a new violation of Article 8, holding that the indefinite retention of biometric data, even in respect of convicted persons, is not permissible without clear and effective safeguards; this conclusion is all the more relevant in the context of predictive policing, where data are often retained long after minor offences have been committed, without any real mechanisms for their periodic review or deletion.

In the case of Big Brother Watch and Others v. United Kingdom (2021)[3], the Court examined mass interception and surveillance practices at the state level, concluding that such extensive data collection, carried out without strong safeguards, effective independent oversight and precise legal rules, does not comply with the requirements of Article 8. The Court's observations are directly relevant to the field of predictive policing, where the functioning of systems often depends on large volumes of data stored over the long term, sometimes combined with technologies such as facial recognition, thus raising the same issues of proportionality and protection of privacy.

A few principles become clear from such cases: data minimization and purpose limitation, strict necessity of surveillance, sufficient and independent oversight, transparency and accountability and protection against discriminatory effects. Predictive policing, and in particular systems that are integrated into everyday operational policing, need to be interrogated against these principles. Given the predictive and inherently uncertain nature of algorithmic predictions and the substantial risk of replicating discriminatory patterns already embedded in historical data, many current systems would struggle to showcase strict necessity or proportionality.

Combined, the AI Act, GDPR, and the European Court of Human Rights (ECtHR) jurisprudence construct a triangular set of legal frameworks around the legality of predictive policing. Even though the three instruments focus on different aspects (technical design, data processing rights, and fundamental rights), predictive policing will converge among them. Together, these regulations create a highly rigorous regime of justification, transparency, and oversight. A bona fide predictive policing system in the European context would have to prove that:

- Adherence to AI Act principles, such as risk assessments, bias mitigation, high-quality data, and human oversight;
- Respect for data protection rights, especially the rights regarding automated decision-making and transparency obligations;
- Compliance with ECtHR principles, maintaining that such AI predictions do not cause disproportionate or discriminatory interference with private life.

[1] European Court of Human Rights, *S. and Marper v. United Kingdom,* Judgment of 4 December 2008, HUDOC, https://hudoc.echr.coe.int/eng?i=001-90051 (15.11.2025)
[2] European Court of Human Rights, *Gaughran v.* United Kingdom, 2020, https://hudoc.echr.coe.int/eng?i=001-200050 (10.11.2025)
[3] European Court of Human Rights, *Big Brother Watch and Others v. United Kingdom,* 2021, https://hudoc.echr.coe.int/eng?i=001-210077 (15.11.2025)

Without these protective barriers, predictive policing technologies could potentially undermine the very tenets on which the European human rights protection scheme rests. As a consequence, a responsible regulatory approach has to be taken to guarantee that technological innovation does not undermine fundamental rights, but that it is instead a necessary part of a security strategy based on human dignity and democratic accountability.

Conclusions

The conflict about predictive policing and Automated Suspicion Algorithms demonstrates how much technology and its applications are transforming public safety. They suggest speeding up, streamlining and more effectively managing the police resources, but the effects in practice go far beyond day-to-day operational ease. A growing sense of suspicion based on correlations extracted from massive swathes of data rather than proven, observable behavior is what undermines existing legal protections. The presumption of innocence, the necessity of an individualized justification and a person's capacity to comprehend and contest evidence that is used against them are all challenged.

This conversation is further complicated by the European legal landscape. The AI Act, the GDPR and the case law of the European Court of Human Rights take different approaches to the topic: technical standards, data-processing rights and fundamental rights protection. Collectively, they make up a very complex legal structure that has very high standards in terms of transparency, accountability, and human intervention. Viewed in this light, many of the existing predictive policing tools would be hard to prove strict necessity, proportionality or an absence of discriminatory effects, at least when they exploit historical data framed by structural inequality.

These problems indicate that the task is more than correcting the algorithmic bias, but to discover a way to integrate the technological innovation into legal regimes that were not established for automatic decision-making. The courts, oversight bodies and police organizations are increasingly facing systems where the internal logic of their systems becomes difficult to interpret and even more difficult to challenge. In the absence of substantial transparency and robust preventive and counter measures, the danger is to treat algorithmic inferences as if they're objective truths, even when they are driven by design choices or encoded assumptions.

In the future, more research is required to understand what predictive policing looks like in practice, who's affected by it, officers' use of algorithmic outputs in day-to-day practice and what kinds of oversight actually work. Indeed, a comparative perspective of human security and practical regulation could provide a clearer indication on how to ensure that preventative policing might not diminish the rights it is professed to safeguard. Ultimately, how to make the rule of law sustainable enough to withstand an algorithmic world, it turns out, hangs on societies being capable of maintaining human dignity, fairness, and accountability during an age where machines are becoming progressively more important tools of power.

Protecting human security in the algorithmic age requires more than technological calibration, it requires reaffirming the constitutional principles and human rights that define democratic societies.

Bibliography

Book

1. McSherry, Bernadette, *Risk Assessment, Predictive Algorithms and Preventive Justice*, Palgrave Macmillan, Cham, 2020

Studies and Articles

1. Arcila Jr., Fabio, *Nuance, Technology, and the Fourth Amendment: A Response to Predictive Policing and Reasonable Suspicion*, Legal Studies Research Paper Series No. 15-11, 2014
2. Barrett, Lindsey, *Reasonably Suspicious Algorithms: Predictive Policing at the United States Border*, "N.Y.U. Review of Law & Social Change", Vol. 41, Issue 3, 2017
3. Berman, Emily, *Individualized Suspicion in the Age of Big Data*, "Iowa Law Review", Vol. 105, 2020
4. DaViera, Andrea L.; Baker, Bruce D.; Tropp, Linda R., *Risk, Race, and Predictive Policing: A Critical Race Theory Analysis of the Strategic Subject List*, "American Journal of Community Psychology", 2022
5. Egbert, Simon, *Predictive Policing and the Platformization of Police Work*, "Surveillance & Society", 2019
6. Ferguson, Andrew Guthrie, *Big Data and Predictive Reasonable Suspicion*, "University of Pennsylvania Law Review", 2015
7. Ferguson, Andrew Guthrie, *Predictive Policing and Reasonable Suspicion*, "Emory Law Journal", Vol. 62, 2012
8. Hiller, Kaitlynd, *Predictive Policing and the Charter*, "Manitoba Law Journal", 2022
9. Iwannudin, Iwannudin; Heriani, Istiana; Lestaluhu, Rajab, *Legal Challenges in Regulating Artificial Intelligence Use in Criminal Justice Systems*, "The Journal of Academic Science", 2025
10. Katyal, Sonia K., *The Paradox of Source Code Secrecy*, "Social Science Research Network (SSRN)", 2019
11. Kotsoglou, Kyriakos N.; Oswald, Marion, *The Long Arm of the Algorithm? Automated Facial Recognition as Evidence and Trigger for Police Intervention*, "Forensic Science International: Synergy", Vol. 2, 2020
12. Loureiro, Antonio José Cacheado et al., *Reasonable Suspicion and Predictive Policing: Technology and Legality in the Context of Brazilian Public Security*, "Revista PPC – Políticas Públicas e Cidades", 2024
13. Mesarčík, Matúš, *Policajné profilovanie v kontexte základných ľudských práv a slobôd*, "Acta Facultatis Iuridicae Universitatis Comenianae", 2019
14. Mugari, Ishmael; Obioha, Emeka E., *Predictive Policing and Crime Control in the United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing*, "Social Science", Vol. 10, No. 6, 2021
15. O'Donnell, Renata M., *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause*, "New York University Law Review", 2019
16. Purves, Duncan, *Fairness in Algorithmic Policing*, "Journal of the American Philosophical Association", 2022
17. Rosser, Gavin; Davies, Toby; Bowers, Kate; Johnson, Shane; Cheng, Tao, *Predictive Crime Mapping: Arbitrary Grids or Street Networks?*, "Journal of Quantitative Criminology", 2016

18. Rotaru, Victor et al., *Precise Event-level Prediction of Urban Crime Reveals Signature of Enforcement Bias*, "Research Square", 2021
19. Sandhu, Ajay; Fussey, Peter, *The 'Uberization of Policing'? How Police Negotiate and Operationalise Predictive Policing Technology*, "Policing and Society", 2021
20. Sarzaeim, Paria; Mahmoud, Qusay H.; Azim, Akramul, *A Framework for LLM-Assisted Smart Policing System*, "IEEE Access", Vol. 12, 2024
21. Sachoulidou, Athina, *Going Beyond the "Common Suspects": To Be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence*, "Artificial Intelligence and Law", 2023
22. Shepherd, Nicki James, *Algorithmic Justice: The Legal Implications of AI in Criminal Sentencing and Risk Assessment*, "Journal of Artificial Intelligence General Science", Vol. 8, 2025
23. Washington, Alexandra L., *How to Argue with an Algorithm: Lessons from the COMPAS ProPublica Debate*, "Social Science Research Network (SSRN)", 2019
24. Wibisono, Radyan Kunto; Setiono, Joko; Prisgunanto, Ilham, *Artificial Intelligence in Predictive Policing: A Systematic Literature Review and Its Implications for Indonesia*, "Jurnal Greenation Sosial dan Politik", 2025

Documents

1. European Court of Human Rights, *S. and Marper v. United Kingdom*, HUDOC, Judgment of 4 December 2008
2. European Court of Human Rights, *Gaughran v. United Kingdom*, 2020
3. European Court of Human Rights, *Big Brother Watch and Others v. United Kingdom*, 2021
4. United Nations Development Programme (UNDP), Human Development Report 1994, Oxford University Press, 1994