Human-Centered Security in Society 5.0: Revisiting Algorithmic Bias and Methodological Constraints in Predictive Policing

Aleksandar Filipović and Željko Bjelajac

University Business Academy, Novi Sad, Serbia

Faculty of Law for Commerce and Judiciary in Novi Sad

Article Information*

Review Article • UDC: 351.741:343.98

Volume: 22, Issue: 3, pages: 74–88

Received: November 12, 2025 • Accepted: December 11, 2025

https://doi.org/10.51738/kpolisa.2025.3r.006

Author Note

Aleksandar Filipović https://orcid.org/0000-0002-1097-2079

Željko Bjelajac https://orcid.org/0000-0003-4953-8779

We have no known conflict of interest to disclose.

Corresponding author: Aleksandar Filipović

E-mail: sasha.filipovic@gmail.com

* Cite (APA): Filipović, A., & Bjelajac, Ž. (2025). Human-Centered Security in Society 5.0: Revisiting Algorithmic Bias and Methodological Constraints in Predictive Policing. *Kultura polisa, 22*(3), 74–88, https://doi.org/10.51738/kpolisa.2025.3r.006

Human-Centered Security in Society 5.0: Revisiting Algorithmic Bias and Methodological Constraints in Predictive Policing

Abstract

Society 5.0, envisioned as an advanced, human-centered civilization in which the physical and digital realms seamlessly complement one another, represents a sustainable model for the functioning of human communities on an increasingly overpopulated planet. In such an environment, a progressively deeper symbiosis between social processes and technological innovation is expected, with the security sector emerging as one of the key domains of this integration. Within the field of public security, predictive policing stands out in particular: its models, based on artificial intelligence and big-data analytics, enable the anticipation of criminal patterns and the potential for more effective risk prevention. This paper examines predictive policing as a transformative approach to law enforcement, while simultaneously problematizing its deeply embedded challenges - especially in the context of the value framework of Society 5.0, which seeks to ensure that technological advancement remains subordinate to human dignity, justice, and social inclusion. Through an analysis of case studies from Chicago, London, and Tokyo, the paper identifies the operational advantages of predictive techniques but also highlights key concerns such as algorithmic bias, lack of transparency, insufficient data quality, and methodological limitations that may jeopardize the fairness and legitimacy of police interventions. The findings demonstrate that although predictive algorithms can contribute to the enhancement of preventive strategies, their implementation must occur within a clearly defined normative framework that incorporates technical robustness, independent oversight, institutional accountability, and active citizen participation. In line with the principles of Society 5.0, the paper concludes that the successful application of predictive policing requires the development of systems that are ethically grounded, methodologically transparent, and oriented toward the protection of human rights - ensuring that technology serves society rather than the other way around.

Keywords: Society 5.0, security, predictive policing, artificial intelligence

Introduction

The concept of Society 5.0, formally introduced within Japan's Fifth Science and Technology Basic Plan (2016), represents a normative–strategic vision of a super-smart, human-centered society in which physical and cyber spaces are systematically integrated to enhance the quality of life for individuals and communities. In this model of social development, artificial intelligence, big-data systems, and the Internet of Things (IoT) constitute the foundational technological infrastructures that enable faster, more accurate, and contextually adaptive decision-making across almost all domains of public and private activity, including healthcare, education, transportation, energy, and public security.

Unlike earlier developmental paradigms - commonly described as Society 1.0 through 4.0 - which were predominantly oriented toward industrialization and digitalization (see: Cosan, 2021; Bjelajac & Bajac, 2022), Society 5.0 introduces a qualitatively new normative dimension rooted in the idea of seamless coexistence and synergy between cyber and physical spaces. This model presupposes the broad application of artificial intelligence, IoT infrastructures, robotics, autonomous systems, and advanced communication technologies to provide systemic responses to key contemporary challenges such as demographic aging, urban mobility, the sustainability of healthcare systems, and the increasing demands placed upon security.

Terminologically, it is necessary to distinguish between the interconnected but conceptually distinct frameworks of "Society 5.0" and "Industry 5.0." Although complementary, these concepts are not identical (Huang et al., 2022). Industry 5.0 emerges within European industrial policy as a critical response to the technocentric model of Industry 4.0, whereas Society 5.0 was developed in the Japanese context as a national strategy aimed at addressing broadly defined social problems. Their differing genealogical origins point to a divergence in normative focus: Industry 5.0 primarily addresses issues of labor, production, and economic transformation, while Society 5.0 offers a broader framework for understanding changes in everyday life, social cohesion, and overall societal well-being.

The literature identifies several key normative–technological characteristics of Society 5.0. First, human-centricity serves as its fundamental axiological principle, according to which the development and implementation of technologies are meant to prioritize the enhancement of human quality of life rather than merely increasing economic efficiency. Second, integration of the digital and physical worlds entails the continuous collection of data from the real environment, their algorithmic processing, and transformation into operationally relevant information, enabling a shift from reactive to proactive and preventive models of governance. Third, sustainability and inclusiveness stand out as essential political–ethical dimensions, emphasizing the reduction of social inequalities and broad accessibility of technological solutions. Fourth, smart resource management, enabled by AI and IoT systems, supports the optimization of infrastructure in both urban and rural settings. Fifth, participatory and proactive governance promotes the active involvement of citizens in decision-making through digital platforms and analytical tools for predictive planning. Finally, the development and application of these technologies are normatively framed by the requirements of ethics, safety, and legal protection of fundamental human rights (see: Bjelajac, Filipović & Stošić, 2022).

In contemporary criminological and sociological literature, predictive policing refers to the use of statistical methods and machine-learning algorithms to assess the likelihood of future criminal events in relation to specific spatial, temporal, or demographic variables (Meijer & Wessels, 2019). Theoretically, it is important to emphasize that these systems are not based on notions of precognition or any form of paranormal foresight, which have no empirical grounding in modern security studies or criminology. Contrary to popular-cultural representations, real predictive-policing systems rely entirely on quantitative data, statistical models, and algorithmic processing.

Within the normative context of Society 5.0, predictive policing is presented as a potential tool for strengthening the preventive function of the state in the field of public security, provided that the principles of legality, transparency, accountability, and human rights protection are strictly respected. The conceptual framework of Society 5.0 thus enables a deeper understanding of the ethical, legal, and methodological tensions that accompany the implementation of predictive systems in the security sector, making this framework theoretically relevant for analyzing contemporary security policies.

Historically, early institutional forms of analytical police management were developed through systems such as CompStat, which relied primarily on descriptive and retrospective analyses of crime patterns (Eterno & Silverman, 2006). With the advancement of machine learning and increased computational power, specialized commercial software solutions for predictive analytics emerged, the most frequently cited in the literature being PredPol (later Geolitica), HunchLab, and ShotSpotter (Egbert & Esposito, 2024; Degeling & Berendt, 2017; Feathers, 2021). These systems apply a wide spectrum of

methods - ranging from regression models and Bayesian networks (Ben-Gal, 2007) to cluster analysis and deep neural networks - in order to generate risk estimates based on historical crime data, demographic indicators, and spatio-temporal patterns.

The core theoretical premise of predictive policing is that the allocation of police resources can be rationalized and optimized through empirically processed data rather than relying solely on the heuristic knowledge and experience of officers. However, empirical literature provides ambivalent findings: while some studies indicate improvements in operational efficiency and more targeted deployment of police units (Mohler et al., 2015; Perry et al., 2013), others warn of structural risks such as the reproduction of institutional bias and the emergence of self-fulfilling prophecies (Lum & Isaac, 2016; Brayne, 2020). In this sense, predictive policing cannot be understood as a neutral technological tool, but rather as a socio-technical system whose implementation raises complex methodological, ethical, and legal questions - questions that demand critical and interdisciplinary analysis.

Methodological Framework

This research is grounded in a qualitative–interpretative methodological approach aimed at examining the normative, theoretical, and empirical dimensions of predictive policing within the conceptual framework of Society 5.0. The central premise of the study is that predictive policing cannot be adequately understood as a purely technical matter; rather, it represents a complex socio-technical phenomenon that simultaneously encompasses technological, legal, ethical, and socio-political dimensions.

The primary research method is qualitative content analysis of relevant scholarly literature, reports issued by international organizations, and normative documents. This includes works from the fields of criminology, security sociology, science and technology studies (STS), data-protection law, and digital policy, as well as strategic documents of national governments and supranational institutions concerning the development of artificial intelligence and smart security systems. The literature review was conducted as a thematic analysis, through which dominant theoretical models, key debates, and critical gaps in existing research were identified.

Additionally, a comparative method was employed through the examination of different models of predictive-policing implementation in selected national contexts - primarily in the United States and the member states of the European Union. This comparative perspective enabled the identification of patterns of similarity and divergence in regulatory approaches, institutional arrangements, and forms of public legitimation of these systems.

A normative–legal analysis was used to assess the compliance of predictive-policing systems with the core principles of criminal law and human-rights protection, including the principles of legality, proportionality, the presumption of innocence, and the right to privacy. Special attention was devoted to relevant European standards, particularly the General Data Protection Regulation (GDPR), as well as documents of the Council of Europe and the European Union pertaining to artificial intelligence and digital rights.

The empirical component of the research is limited to secondary analysis of available case studies and evaluation reports of predictive-policing systems. Rather than collecting primary data, the study relies on a critical synthesis of existing empirical findings to identify structural limitations, unintended consequences, and potential risks associated with the practical deployment of these technologies.

Finally, the research adopts an interdisciplinary analytical framework, integrating insights from criminology, legal studies, sociology, and digital-technology studies. This approach makes it possible to understand predictive policing not merely as an instrument of security policy, but as an indicator of the broader transformation of relations between the state, technology, and citizens in contemporary societies.

The Concept of Predictive Policing – Technical Foundations, Human-Centric Orientation, and Conceptual Limitations

Predictive policing represents one of the most ambitious attempts to apply artificial intelligence in the field of security, relying on advanced statistical models, machine-learning algorithms, and social-network analytics to identify patterns of criminal behavior and forecast future risks. These systems promise more efficient allocation of police resources and improvements in public safety, yet they simultaneously raise complex ethical and methodological questions. Their accuracy and reliability depend on the quality and structure of the data, the design of the algorithms, and the manner in which they are implemented in practice - factors that make them particularly vulnerable to various forms of bias. Understanding the technological basis of these models - from spatio-temporal analysis to classification algorithms and probabilistic approaches - is essential for evaluating the risks posed by predictive-policing systems within a society striving for value-oriented and inclusive digital transformation, as envisioned by Society 5.0.

The technological foundation of predictive policing typically rests on a combination of advanced analytical approaches. These include, above all, spatio-temporal models such as Poisson regression and spatio-temporal point-processes, which estimate the likelihood of crime occurring in specific locations within defined time intervals. In addition, a wide range of classification algorithms (Belcic, n.d.), including random-forest models, support-vector machines (SVM), and neural networks, are used to categorize events according to type or estimated probability. Social-network-analysis models play a particularly important role in mapping criminal networks and relationships among offenders, while Bayesian probabilistic models (Ben-Gal, 2007) combine diverse data sources to provide more accurate risk assessments. Despite their technical sophistication, the accuracy and reliability of these algorithmic approaches depend critically on the quality, scope, and representativeness of the underlying data, raising the central issue of algorithmic bias.

Algorithmic bias refers to systematic deviations in model outputs that arise from unbalanced, incomplete, or incorrectly labeled input data, as well as from the design choices embedded in the algorithm itself (Jonker & Rodgers, n.d.). This appears to be the core structural problem of predictive policing: models that analyze crime do not observe the world as it is, but rather as it is represented in the data. When those data reflect historical patterns of selective law enforcement or institutional prejudice, algorithms may reproduce - and even intensify - the very patterns society seeks to overcome. As a result, predictive policing can lead to disproportionate deployment of police resources to certain geographic areas or toward particular demographic or ethnic groups, thereby reinforcing existing social inequalities.

The literature commonly distinguishes three dominant types of bias in predictive policing. Data bias arises when historical datasets reflect institutional patterns of selective control rather than the actual distribution of crime. Model bias occurs when the choice of models, parameters, or underlying assumptions systematically privileges certain types of predictions while neglecting more complex patterns. Finally, user

bias emerges from the ways police officers interpret and apply model outputs, potentially amplifying discriminatory outcomes.

The aim of this paper is to identify, through a critical analysis of existing case studies and methodological approaches, the key challenges in designing and implementing AI-based predictive-policing systems, particularly in light of the value-oriented goals and infrastructural characteristics of the Society 5.0 framework.

Dominant Types of Algorithmic Bias in Predictive Policing and How They Arise

The implementation of predictive policing rests on the belief that algorithmic analysis of large datasets can enable more precise allocation of police resources and thus contribute to crime reduction. However, empirical experiences show that these systems are not neutral; they incorporate various forms of bias that can seriously undermine fairness, legitimacy, and public trust in institutions. In this context, algorithmic bias is not merely a technical flaw but a direct reflection of social relations and historical patterns of policing. Predictive policing does not operate in a vacuum: it reproduces - and frequently intensifies - existing inequalities and prejudices, thereby risking the reinforcement of structural injustice rather than improving public safety.

The most common sources of bias emerge at the level of the data on which these systems are trained. When historical records are shaped by selective law enforcement - for example, if police have disproportionately patrolled certain neighborhoods or social groups - algorithms internalize these patterns, marking the same communities as “high risk,” regardless of their actual crime rates. Bias also appears in data sampling: non-representative datasets can mislead the system into false conclusions. Wealthier areas, for instance, tend to report fewer incidents, which the algorithm may interpret as evidence of genuine safety. Measurement practices additionally affect prediction quality, as citizen reports often reflect subjective fears and prejudices; algorithmic systems may then treat these perceptions as objective facts, even when they do not reflect actual criminal activity.

Biases are further embedded in the very design of the algorithm, since the selection of variables, weighting factors, and model assumptions is shaped by the value judgments of engineers and the institutions that determine what counts as a “relevant” risk indicator. Including variables such as unemployment or low socioeconomic status can automatically stigmatize disadvantaged citizens as more prone to criminal behavior. Even model evaluation can be problematic: systems are often assessed through metrics such as precision and recall, but these measures may reflect only where police tend to intervene, not where crimes actually occur. Finally, the feedback-loop effect reinforces bias: when algorithms repeatedly direct police to the same locations, increased police presence generates more recorded incidents, which the system then interprets as confirmation of its predictions, creating a closed cycle of self-confirming error amplification.

Although machine learning is often perceived as a neutral and objective technology, its models possess numerous methodological limitations that can significantly reduce the accuracy and reliability of predictive outputs. These limitations are especially pronounced in predictive policing, where algorithmic systems function not merely as technical tools but as complex socio-technical constructs vulnerable to errors, biases, and misinterpretations. Among the most significant methodological weaknesses are challenges related to generalization, transparency, and performance evaluation. Overfitting leads models

to perform well on historical data but poorly in new contexts. Lack of transparency - particularly in deep neural networks - prevents users from understanding how predictions are generated, creating a "black box" in which even experts cannot fully trace the logic of the model. Performance metrics such as precision and recall (Juba & Le, 2019) can obscure broader societal implications, especially when "high accuracy" does not translate into fair policing outcomes. Limited replicability - stemming from the restricted availability of operational data - further undermines independent verification and critical validation.

The most important methodological limitations identified in predictive-policing models point to deep structural weaknesses (see: Kenge, 2020). The first concerns the limited quality, scope, and representativeness of available data: algorithms learn exclusively from historical records, which are often incomplete, inconsistent, or shaped by structural biases. This leads to the second major limitation - generalization - since models that function effectively on familiar datasets may become unreliable when confronted with demographic changes, crises, or shifts in social behavior. Their predictive accuracy implicitly relies on the assumption that "the future will resemble the past," an assumption that, as Hume (1739) warned, lacks epistemological grounding. Predictive systems also rely on correlations rather than causal understanding, making them susceptible to identifying statistically convincing patterns that have no real connection to criminal behavior.

Algorithmic outputs are further sensitive to design choices and hyperparameter configurations; even small adjustments can generate radically different predictions, reducing model reliability and reproducibility. The feedback-loop effect intensifies these problems: algorithm-driven deployments shape future datasets, reinforcing inaccurate assumptions. The opacity of complex models - especially deep neural networks - presents a serious challenge in security contexts, where institutions and citizens have a legitimate right to understand the foundations of decisions affecting their lives (Rawashdesh, n.d.). Lastly, excessive reliance on statistical performance metrics risks masking discriminatory outcomes: a model may be "accurate" in predicting repeated police interventions, while simultaneously producing unfair and unequal treatment of certain social groups.

Examining different forms of algorithmic bias and methodological limitations reveals that predictive policing, despite its technological sophistication, remains deeply entangled in pre-existing institutional and societal patterns. Model accuracy cannot be separated from historical inequalities, data-collection practices, or the ways in which police actors interpret and implement algorithmic recommendations. If such systems are introduced without critical scrutiny, they can reproduce and even amplify structural injustices. For this reason, it is essential to develop methodologically transparent, ethically grounded, and socially responsible approaches to ensure that technological innovation aligns with the human-centered principles of Society 5.0 - a society in which people, not algorithms, remain at the core of security policy.

Society 5.0 as a Framework for the Ethical and Legal Regulation of Predictive Policing

The concept of Society 5.0, envisioned as a global reference point for future socio-technological systems, is grounded in the idea of a "super-smart society" in which digital technologies, artificial intelligence, and the Internet of Things (IoT) serve the human being rather than the other way around. Its core principle is the harmonization of technological progress with human values, which makes Society 5.0 a suitable framework for reflecting on the ethical and legal regulation of predictive policing. Society 5.0 can function as a normative compass for the development of predictive-policing systems, insisting

that technology must remain subordinate to human needs. This ensures that predictive systems are not only efficient but also ethically legitimate, legally regulated, and socially acceptable.

Society 5.0 begins from the premise that technology must serve human beings and that every digital system - regardless of its complexity - must contribute to the preservation and enhancement of human dignity. This establishes a clear normative foundation for all forms of artificial-intelligence applications, including predictive policing. Within such a conceptual environment, algorithms must not be constructed solely to maximize efficiency and operational output; rather, they must be aligned with the foundational principles of human rights, including privacy protection, non-discrimination, and equal access to justice. One of the central ethical principles of Society 5.0 is the requirement of full transparency and accountability of digital systems. In the domain of predictive policing, this implies mandatory mechanisms for algorithmic auditing, public access to information about the data, statistical patterns, and logical assumptions that inform operational decisions, as well as institutional accountability for all consequences arising from algorithm-driven actions.

The concept of balancing security and liberty is especially significant. Society 5.0 emphasizes that security goals must never be achieved at the expense of fundamental civil rights. Predictive policing may serve as a preventive tool that enhances public safety, but only within clearly defined boundaries that prevent excessive surveillance, the normalization of population control, and the stigmatization of particular social groups based on statistical predictions. Furthermore, the idea of digital inclusion and fairness is one of the pillars of Society 5.0. This implies that predictive-policing algorithms must not rely on data that are selective, exclusionary, or biased, as such systems would directly undermine the principles of equality and social cohesion. Instead, the ethical framework requires the development of models that minimize the risk of bias, ensure equitable representation of all social groups, and promote fairness in decision-making.

Parallel to this, Society 5.0 advocates the establishment of a legal infrastructure that evolves simultaneously with technological innovation, rather than reactively and post festum. This ensures that legal norms clearly define the boundaries of algorithmic use, establish mechanisms of institutional oversight, create independent supervisory bodies, and guarantee citizens the right to legal remedy if they are harmed by an unjust algorithmic decision. Finally, since Society 5.0 promotes international cooperation and global standardization of ethical principles in digital technologies, the same logic can be applied to the regulation of predictive policing. Harmonized international rules and minimum human-rights standards could significantly reduce the risk of misuse, increase transparency, and ensure responsible and just application of artificial intelligence in the security sector.

Given this, the use of biased and methodologically limited predictive-policing systems must be deemed unacceptable in a highly sophisticated, experimental society that cannot tolerate error or improvisation. The fundamental question arises: How can the concept of predictive policing be purified of bias, methodological limitations, and other deficiencies before it is certified as a safe, humanistic, and human-centered technology worthy of Society 5.0? If we have established that predictive policing suffers from two fundamental weaknesses - algorithmic bias and methodological limitations - then it becomes evident that this technology, in its current form, cannot exist within the envisioned framework of Society 5.0. This is a society built on the assumption that human dignity cannot be compromised under any circumstances and that technological intervention is justified only if it contributes to greater humanity,

security, and social justice. The question that follows is unavoidable: What must be done for predictive policing to become a legitimate candidate for use in such a society?

The first task belongs exclusively to the scientific and academic community. Those who develop algorithms must assume responsibility for the origin and quality of the data. In practice, this means that datasets must be purged of historical layers of discrimination, class and ethnic stereotypes, and the uneven or distorted representation of particular social or ethnic groups. It is not enough to build "stronger" models on top of flawed datasets; new datasets must be created - carefully designed to be representative, plural, and ethically neutral. In other words, science must recognize that a dataset is as normative as a legal statute, since it defines the framework within which the algorithm "sees" reality.

We have already identified many existing methodological procedures as technologically obsolete, if not technologically ruinous. It is therefore necessary to encourage technological innovation - an obligation that falls to the technology industry. The industry developing software and hardware for predictive policing cannot remain confined to its present state. Instead of relying on simple statistical correlations and predictive models that reduce complex social phenomena to raw numerical data, the industry must develop multimodal, adaptive, and hybrid machine-learning approaches (Sheng et al., 2024). Such approaches do not analyze only quantitative data; they incorporate qualitative aspects such as social context, urban spatial dynamics, and even cultural patterns. The industry must abandon "fast and cheap" models and adopt models that are slow, expensive, but reliable - because Society 5.0 will not tolerate improvisation or erroneous assessments.

If algorithms are to be used in such a sensitive field as predictive policing, transparency must be an obligation, not an option. Regulatory bodies must establish clear protocols for independent audits, periodic evaluations, and publicly accessible reports on algorithmic performance. No model may remain a "black box." Citizens, as the ultimate bearers of sovereignty, have the right to know the parameters and logic by which an algorithm produces predictions. Only such transparency can guarantee public trust and reassure citizens that the state respects the ethical standards of a human-centered society. This also means that ethics must not be added later as an ad hoc or unwanted corrective, but must be integrated directly into the architecture of the algorithm itself. This task cannot be carried out by science alone or industry alone; it requires interdisciplinary collaboration. As we argued in an earlier study (Bjelajac & Filipović, 2022), since contemporary humanity is unwilling to think of itself outside the technological paradigm, scholars - especially philosophers, sociologists, and theologians - are not prepared to entrust the development of AI ethics to engineers and technicians alone. Teams must include philosophers, lawyers, sociologists, anthropologists, and psychologists, alongside engineers and mathematicians. Together they must design algorithms in which ethical principles are encoded internally rather than merely imposed externally. In this way, predictive policing is prevented from ever crossing the humanitarian threshold that Society 5.0 defines as a mandatory standard.

Finally, no technology - even the most sophisticated - can be implemented in a vacuum. A strong legal framework must define the scope and limits of predictive-policing use. Citizens must have the right to appeal, the right to explanation, and the right to protection from the errors of the algorithm. Moreover, society must establish institutions capable of monitoring the long-term consequences of these technologies, so that systemic risks and failures can be detected in time. Without these guarantees, no technology can be considered "worthy" of Society 5.0.

Empirical Experiences with Predictive Policing: The Cases of Chicago, London, and Tokyo

Chicago is one of the first cities in the United States to attempt a systematic, real-world implementation of predictive policing. As early as 2012, the Chicago Police Department developed the so-called Strategic Subjects List (SSL), a "list of high-risk individuals," using machine-learning algorithms and statistical models (Tucek, n.d.). The idea behind the program was simple yet highly ambitious: to predict which individuals were most likely to commit, or become victims of, violent crimes.

At first glance, this approach appeared promising. Instead of responding only after a crime is committed, the police could act preventively, guided by "probability-based data" (Jeffrey, 1992). In a Society 5.0 environment - where proactive, integrated security mechanisms are emphasized - such a concept would seem like a perfect testing ground. However, the reality soon revealed a deep gap between ambition and practice. The SSL program proved to reproduce longstanding patterns of bias embedded in police work (DaViera et al., 2023). The training data derived from historical police records carried with them decades of accumulated distortions and inequalities, particularly affecting Black and Latino communities. Instead of eliminating discrimination, the algorithm reinforced and institutionalized it. Individuals with no criminal history could find themselves on the list simply because they lived in "the wrong neighborhoods" or had social ties to people under police scrutiny.

Academic and civil-rights organizations were sharply critical. They argued that the program undermined the presumption of innocence and stigmatized citizens without just cause. After years of debate, Chicago officially discontinued the SSL in 2019, noting that "there is insufficient evidence that the algorithm reduces crime rates" (Advisory Concerning the Chicago Police Department's Predictive Risk Models – Chicago Office of Inspector General, 2023).

This case clearly illustrates what Society 5.0 must never permit. A highly sophisticated, human-centered society cannot allow experimentation with tools that generate social injustice. The Chicago example teaches that the foundational prerequisites for any predictive technology are full methodological transparency, independent ethical oversight, and continuous assessment of impacts across different social groups.

Unlike Chicago - which entered early and failed quickly - London has taken a more cautious and fragmented approach to predictive policing. The Metropolitan Police Service, along with several local police forces, experimented with various algorithmic tools, including systems predicting crime "hot spots," geographic areas with an elevated likelihood of criminal activity (London Assembly, 2013).

One of the most well-known experiments was conducted with the support of PredPol, a company whose algorithmic methods were originally inspired by earthquake-prediction models. The system relied on past crime data (time, location, type) to generate maps of "hot spots." Police patrols were then directed to these zones for preventative purposes. Initial results seemed encouraging: in several neighborhoods, minor crimes such as burglaries or thefts decreased.

However, critical questions soon emerged. Do such systems, in fact, create "self-fulfilling prophecies"? In other words, if police repeatedly send patrols to the same areas, it is natural that more incidents will be detected there, thus reinforcing the algorithm - even if no actual rise in criminal behavior has occurred. British public opinion, characterized by strong commitments to privacy and human rights, reacted cautiously. Facial-recognition technologies, often associated with predictive policing, came under

particular scrutiny. Courts and independent regulators repeatedly warned that such systems must be strictly regulated and their use tightly constrained.

London's lesson is dual: on one hand, predictive systems can help optimize resource allocation and yield measurable short-term results; on the other, without robust legal and ethical safeguards, they risk eroding public trust and paving the way for mass surveillance. In Society 5.0 - where public trust must be a foundational pillar - London's experience demonstrates that the balance between efficiency and freedom is fragile, contested, and highly sensitive.

As the country that originally launched the Society 5.0 concept, Japan offers a particularly insightful example of how predictive policing can develop in a different social and cultural context. Unlike Western metropolises, where debates center on individual rights and legal restrictions, Japanese society is characterized by a strong cultural consensus around the importance of collective safety and social harmony.

The Tokyo Metropolitan Police have long employed advanced statistical tools for analyzing crime patterns, and over the past decade have integrated elements of artificial intelligence (Itakura, n.d.). These systems analyze vast quantities of data - from citizen reports and historical case files to urban sensor networks and video surveillance. The goal is not only to predict crime hot spots but also to optimize the deployment of police resources in accordance with the city's dynamic rhythms.

What distinguishes the Japanese case is the high level of public trust in institutions and the relatively low crime rate. In such an environment, predictive policing has not been perceived as a threat but rather as a natural extension of societal digitalization. Nevertheless, critical voices exist (Ema, 2020), particularly within academia, warning that algorithms can become "black boxes" and that mechanisms of independent oversight are essential (Tsunoda & Komatsu, 2022).

The Japanese model illustrates how Society 5.0 might integrate predictive policing: through gradual implementation, process transparency, and ongoing communication with citizens. The key is not eliminating all risks - an impossible task - but ensuring that technology remains aligned with societal values and continuously subject to democratic control.

Concluding Recommendations for the Implementation of Predictive Policing in Society 5.0

For predictive policing to function in accordance with the high humanistic and technological standards of Society 5.0, it is necessary to establish a framework that goes beyond mere technical functionality and incorporates a broader range of ethical, legal, and social criteria. The first and most important requirement is strict compliance with human rights. Predictive-policing systems must be designed to guarantee privacy, freedom of movement, and non-discrimination. Without these safeguards, such systems would become instruments of social control rather than tools for enhancing public safety. The second pillar is transparency. Algorithmic decision-making must not remain enclosed within "black boxes." Institutions that develop and deploy predictive models must publish documentation such as model cards and datasheets that clearly present data provenance, methodological assumptions, and system limitations. Mandatory algorithmic impact assessments should demonstrate how a system affects different social groups. The third element concerns citizen participation. Predictive policing cannot be imposed from above as a ready-made technological package. Its legitimacy depends on the involvement of local communities, which must take part in the design, evaluation, and oversight of these systems. Such participation builds

trust and reduces the risk of alienation between the police and the society they are meant to protect. The fourth aspect involves technical safeguards. The most advanced systems should incorporate tools such as differential privacy, federated learning, and transparent disclosure of prediction uncertainty intervals. These mechanisms reduce the risk of data misuse while increasing public confidence in the technical soundness of the models. The fifth principle relates to institutional oversight. Independent regulatory bodies should perform regular inspections, while public algorithm registries must be accessible in ways that enable expert and civic scrutiny. Additionally, periodic stress tests and red-teaming simulations can reveal potential abuses and system vulnerabilities before they cause actual harm. The sixth requirement concerns the evaluation of fairness. Accuracy alone cannot serve as the primary measure of value; it is equally important to assess the fairness of algorithmic outcomes. This includes monitoring indicators such as calibration, selection parity, or false-positive rates. When different fairness metrics come into conflict, a formalized decision-making procedure is needed - one that incorporates legal, ethical, and social considerations.

Ultimately, predictive policing in Society 5.0 must remain dynamically adaptable. Crime patterns, social contexts, and technological capabilities evolve constantly, and the systems must undergo periodic review and recalibration. This ensures that algorithms remain aligned with contemporary ethical and legal standards while keeping pace with the realities in which they operate. Taken together, these recommendations form a practical framework for responsible implementation of predictive policing. They make it clear that predictive policing cannot be seen merely as a technical experiment but must be treated as a social project rooted in the humanistic values of Society 5.0.

Predictive policing as we know it today is not acceptable in a society aspiring to perfect synergy between humans and technology. However, this does not mean the idea is doomed. On the contrary, within the conceptual horizon of Society 5.0, predictive policing can serve as a test: if human communities manage to free it from bias, methodological weaknesses, and lack of transparency, then it may be possible to create a technology that truly serves humanity. If they fail, that will be a clear signal that there are limits to what can be delegated to algorithms. Society 5.0 will not tolerate improvisation or untested experimentation. It demands technologies that are humanitarianly safe, legally protected, and ethically sound. Only then can predictive policing be verified as secure and worthy of such a society. Until that point, it remains a transitional concept - situated between an imperfect present and a possible future ideal.

References

Advisory concerning the Chicago Police Department's predictive Risk models - Chicago Office of Inspector General. (2023, August 8). Chicago Office of Inspector General. https://igchicago.org/publications/advisory-concerning-the-chicago-police-departments-predictive-risk-models/

Belcic, I. (n.d). *What is classification in machine learning?* IBM. https://www.ibm.com/think/topics/classification-machine-learning

Ben‐Gal, I. (2007). Bayesian Networks. *Encyclopedia of Statistics in Quality and Reliability*. https://doi.org/10.1002/9780470061572.eqr089

Biggs, M. (2013). Prophecy, Self-Fulfilling/Self-Defeating. *Encyclopedia of Philosophy and the Social Sciences*. https://doi.org/10.4135/9781452276052.n292

Bjelajac, Ž., Filipović, A. (2021). Artificial Intelligence: Human Ethics in Non-Human Entities. In *Proceedings of the 3rd Virtual International Conference „Path to a Knowledge Society-Managing Risks and Innovation* - PaKSoM 2021".

Bjelajac, Ž., & Bajac, M. (2022). Blockchain Technology and Money Laundering. Pravo - Teorija i Praksa, 39(2), 21–38. https://doi.org/10.5937/ptp2202021B

Bjelajac, Željko, Filipović, A. M., & Stošić, L. V. (2022). Internet Addiction Disorder (IAD) as a Consequence of the Expansion of Information Technologies. International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 10(3), 155–165. https://doi.org/10.23947/2334-8496-2022-10-3-155-165

Brayne, S. (2020). Predict and surveil. In *Oxford University Press eBooks*. https://doi.org/10.1093/oso/9780190684099.001.0001

Coşan, B. (2021). Toplum 5.0'ın Mimarı Japonya'da Dezavantajlı Gruplar: Freeter, Hikikomori ve Parasaito Shinguru [Disadvantaged groups in Japan, the architect of Society 5.0: Freeter, Hikikomori, and Parasaito Shinguru]. *Sosyal Siyaset Konferansları Dergisi / Journal of Social Policy Conferences*, 81, 393–419.

DaViera, A. L., Uriostegui, M., Gottlieb, A., & Onyeka, O. (2023). Risk, race, and predictive policing: A critical race theory analysis of the strategic subject list. *American Journal of Community Psychology*, *73*(1–2), 91–103. https://doi.org/10.1002/ajcp.12671

Degeling, M., & Berendt, B. (2017). What is wrong about Robocops as consultants? A technology-centric critique of predictive policing. *AI & Society*, *33*(3), 347–356. https://doi.org/10.1007/s00146-017-0730-7

Egbert, S., & Esposito, E. (2024). Algorithmic crime prevention. From abstract police to precision policing. *Policing & Society*, *34*(6), 521–534. https://doi.org/10.1080/10439463.2024.2326516

Ema, A. (2020). AI and Society: A Pathway from Interdisciplinary-alone to Interdisciplinary Research. *Trends In the Sciences*, *25*(7), 7_29-7_37. https://doi.org/10.5363/tits.25.7_29

Eterno, J. A., & Silverman, E. B. (2006). The New York City Police Department's Compstat: Dream or nightmare? *International Journal of Police Science & Management*, *8*(3), 218–231. https://doi.org/10.1350/ijps.2006.8.3.218

Feathers, T., & Feathers, T. (2024, July 27). *Police are telling ShotSpotter to alter evidence from Gunshot-Detecting AI*. VICE.

https://www.vice.com/en/article/police-are-telling-shotspotter-to-alter-evidence-from-gunshot-detecting-ai/

Huang, S., Wang, B., Li, X., Zheng, P., Mourtzis, D., & Wang, L. (2022). Industry 5.0 and Society 5.0 - Comparison, complementation and co-evolution. *Journal of Manufacturing Systems*, *64*, 424–428. https://doi.org/10.1016/j.jmsy.2022.07.010

Hume, D. (1739). A treatise of human nature. In *Oxford University Press eBooks* (pp. 1–689). https://doi.org/10.1093/oseo/instance.00032872

Itakura, D. (n.d). *NPA to use AI to identify leaders of 'tokuryu' crime groups*. The Asahi Shimbun. https://www.asahi.com/ajw/articles/15995228

Jeffrey, R. (1992). *Probability and the Art of Judgment*, Cambridge University Press.

Jonker, A. & Rogers, J. (n.d). *What is algorithmic bias?* IBM. https://www.ibm.com/think/topics/algorithmic-bias

Juba, B., & Le, H. S. (2019). Precision-Recall versus Accuracy and the Role of Large Data Sets. *Proceedings of the AAAI Conference on Artificial Intelligence*, *33*(01), 4039–4048. https://doi.org/10.1609/aaai.v33i01.33014039

Kenge, R. (2020). Machine learning, its limitations, and solutions over IT. *International Journal of Applied Research on Information Technology and Computing*, *11*(2), 73. https://doi.org/10.5958/0975-8089.2020.00009.3

London Assembly. (2013). *Predictive policing.* London Assembly. https://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/predictive-policing

Lum, K., & Isaac, W. (2016). To predict and serve? *Significance*, *13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Meijer, A., & Wessels, M. (2019). Predictive Policing: Review of benefits and drawbacks. *International Journal of Public Administration*, *42*(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664

Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., & Brantingham, P. J. (2015). Randomized controlled field trials of predictive policing. *Journal of the American Statistical Association*, *110*(512), 1399–1411. https://doi.org/10.1080/01621459.2015.1077710

Perry, W. L., McInnis, B., Price, C. C., Smith, S., & Hollywood, J. S. (2013, September 25). *Predictive Policing: The role of crime forecasting in law enforcement operations*. RAND. https://www.rand.org/pubs/research_reports/RR233.html

Rawashdeh, S. (n.d) *AI's mysterious 'black box' problem, explained.* University of Michigan-Dearborn, https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained

Sheng, Y., Zhang, G., Zhang, Y., Luo, M., Pang, Y., & Wang, Q. (2023). A multimodal data sensing and feature learning-based self-adaptive hybrid approach for machining quality prediction. *Advanced Engineering Informatics*, *59*, 102324. https://doi.org/10.1016/j.aei.2023.102324

Tsunoda, T. & Komatsu, S. (2022). *The landscape of AI ethics and law in Japan, PAI Summit 2022, Global Partnership on Artificial Intelligence*, https://www.nishimura.com/en/knowledge/seminars/20221121-93381

Tucek, A. (n.d). *Constraining Big Brother: The legal deficiencies surrounding Chicago's use of the strategic subject list.* The University of Chicago Legal Forum. https://legal-forum.uchicago.edu/print-archive/constraining-big-brother-legal-deficiencies-surrounding-chicagos-use-strategic

Humanocentrična bezbednost u Društvu 5.0: Razmatranje algoritamske pristrasnosti i metodoloških ograničenja u prediktivnoj policiji

Aleksandar Filipović i Željko Bjelajac

Pravni fakultet za privredu i pravosuđe, Novi Sad

Sažetak

Društvo 5.0, zamišljeno kao napredna, humanocentrična civilizacija u kojoj se fizička i digitalna sfera međusobno neprimetno dopunjuju, predstavlja održiv model funkcionisanja ljudskih zajednica na sve prenaseljenijoj planeti. U takvom okruženju očekuje se sve dublja simbioza društvenih procesa i tehnoloških inovacija, pri čemu se sektor bezbednosti izdvaja kao jedno od ključnih područja ove integracije. U domenu javne bezbednosti posebno se ističe prediktivna policija: njeni modeli, zasnovani na veštačkoj inteligenciji i analitici velikih podataka, omogućavaju anticipaciju kriminalnih obrazaca i potencijalno efikasniju prevenciju rizika. Ovaj rad razmatra prediktivnu policiju kao transformativni pristup sprovođenju zakona, istovremeno problematizujući njene duboko ukorenjene izazove - naročito u kontekstu vrednosnog okvira Društva 5.0, koje teži tome da tehnološki napredak ostane podređen ljudskom dostojanstvu, pravednosti i društvenoj inkluziji. Kroz analizu studija slučaja iz Čikaga, Londona i Tokija, rad identifikuje operativne prednosti prediktivnih tehnika, ali ističe i ključne probleme kao što su algoritamska pristrasnost, nedostatak transparentnosti, nezadovoljavajući kvalitet podataka i metodološka ograničenja koja mogu ugroziti pravičnost i legitimitet policijskih intervencija. Nalazi pokazuju da, iako prediktivni algoritmi mogu doprineti unapređenju preventivnih strategija, njihova primena mora biti uokvirena jasno definisanom normativnom strukturom koja uključuje tehničku robusnost, nezavisni nadzor, institucionalnu odgovornost i aktivno učešće građana. U skladu sa principima Društva 5.0, rad zaključuje da uspešna primena prediktivne policije zahteva razvoj sistema koji su etički utemeljeni, metodološki transparentni i usmereni ka zaštiti ljudskih prava - obezbeđujući da tehnologija služi društvu, a ne obrnuto.

Ključne reči: Društvo 5.0, bezbednost, prediktivna policija, veštačka inteligencija