TEME, Vol. L, Nº 2, April – June 2026, pp. 273–292

Original research paper
Received: December 25, 2025
Revised: February 19, 2026
Accepted: February 23, 2026

https://doi.org/10.22190/TEME251225019D
UDC 351.74/.76:342.7
340.131:[343.98:004.021

PREDICTIVE POLICING AND THE RULE OF LAW: RISKS OF DIGITAL PROFILING IN LAW ENFORCEMENT

Darko Dimovski[1*], Veljko Turanjanin[2], Zdravko Grujić[3]

[1]University of Niš, Faculty of Law, Center for Judicial Research, Serbia
[2]University of Kragujevac, Faculty of Law, Kragujevac, Serbia
[3]Faculty of Law, University of Mitrovica,
with temporary seat in Kosovska Mitrovica, Kosovska Mitrovica, Serbia

ORCID iDs: Darko Dimovski https://orcid.org/0000-0001-5068-3338
Veljko Turanjanin https://orcid.org/0000-0001-9029-0037
Zdravko Grujić https://orcid.org/0000-0001-7433-1468

Abstract

The use of predictive technologies in policing practice is increasingly the subject of legal and ethical debates. This paper explores the phenomenon of predictive policing—a model that, through algorithms and the analysis of large datasets, forecasts locations, times, and potential perpetrators of criminal acts. Although this approach is presented as a tool for more effective crime prevention, it raises serious concerns regarding the rule of law, the protection of human rights, and the principles of due process. Particular attention is given to the emergence of digital profiling, that is, the selective and potentially discriminatory treatment of citizens based on algorithmic predictions. The paper critically analyses the risks these systems pose to the right to privacy, the presumption of innocence, and equal access to justice. Through a comparative legal review of case law, the authors highlight the need to introduce mechanisms of transparency, human oversight over algorithms, and institutional accountability. The conclusion emphasises that predictive policing can only be acceptable if it develops within a framework that consistently protects the fundamental rights and freedoms of individuals.

Key words: predictive policing, digital profiling, rule of law, algorithmic discrimination, human rights.

[*] Corresponding author: Darko Dimovski, Faculty of Law, University of Niš, Judicial Research Center, Trg kralja Aleksandra 11, 18105 Niš, Serbia, darko@prafak.ni.ac.rs

© 2026 by University of Niš, Serbia | Creative Commons License: CC BY-NC-ND

ПРЕДИКТИВНО ПОЛИЦИЈСКО ПОСТУПАЊЕ И ВЛАДАВИНА ПРАВА: РИЗИЦИ ДИГИТАЛНОГ ПРОФИЛИСАЊА У ПРИМЕНИ ЗАКОНА

Апстракт

Употреба предиктивних технологија у полицијској пракси све више постаје предмет правних и етичких расправа. Овај рад истражује феномен предиктивног полицијског поступања — модела који путем алгоритама и анализа великих скупова података предвиђа места, време и потенцијалне учиниоце кривичних дела. Иако се овај приступ представља као инструмент ефикасније превенције криминалитета, он отвара озбиљна питања у погледу владавине права, заштите људских права и принципа правичног поступка. Посебна пажња посвећена је појави дигиталног профилисања, односно селективног и потенцијално дискриминаторног третмана грађана на основу алгоритамских предикција. Рад критички анализира ризике које овакви системи представљају по право на приватност, претпоставку невиности и равноправан приступ правди. Кроз упоредноправни преглед судске праксе аутори указују на потребу увођења механизама транспарентности, људске контроле над алгоритмима и институционалне одговорности. Закључује се да предиктивно полицијско поступање може бити прихватљиво само уколико се развија у оквиру система који доследно штити основна права и слободе појединаца.

Кључне речи: предиктивно полицијско поступање, дигитално профилисање, владавина права, алгоритамска дискриминација, људска права.

INTRODUCTION

With the development of modern technologies based on the processing of large amounts of data and artificial intelligence, policing has undergone significant transformation. Predictive policing, which involves the use of algorithms and data analysis with the aim of forecasting where criminal offences are likely to occur or who might commit them, represents one of the forms of this transformation. Although it can produce positive results, this model raises serious controversies reflected in legal, ethical, and social concerns. Therefore, the question is rightly posed whether predictive policing is compatible with the rule of law and whether its use undermines human rights. As the answer to this question is not simple due to the existence of numerous dilemmas, it is necessary to pay attention to all uncertainties in order to clarify issues related to the use of predictive policing.

Relying on the positions taken by international courts, as well as comparative solutions, this paper seeks to provide answers to the existing dilemmas, accompanied by a critical overview in order to determine whether predictive policing represents merely one of the tools used by law enforcement authorities to enhance efficiency in combating crime, or a tool that undermines the existing system of human rights protection. If this paper resolves any of the existing dilemmas, it will contribute both to reducing crime in the future and to ensuring the simultaneous protection of human rights.

THE CONCEPT AND TECHNICAL BASIS OF PREDICTIVE POLICING

In order to properly assess the risks of predictive policing, it is first necessary to determine what is meant by such policing. Predictive policing refers to the collection of data from various sources, its analysis, and the subsequent use of the results to predict, prevent, and more effectively respond to future crimes. In other words, the work of law enforcement shifts from focusing on what has happened to focusing on what will happen, thereby enabling the police to prevent crime. This shift in focus presupposes the use of specialised artificial intelligence or analytical software to predict the likelihood of criminal offences being committed. It is important to emphasise that predictive policing should not replace any other model of police work; rather, it should enable the police to perform their duties more effectively (Pearsall, 2010, pp. 16-17).

It is interesting to mention the view of George Gascón, the Chief of Police in San Francisco, who stated that with "predictive policing, we have the tools to place officers in the right place at the right time or to engage other services to influence crime, and we can do this at lower cost" (Pearsall, 2010, p. 17). Based on this, one may conclude that one of the most prominent characteristics of predictive policing is its ability to predict future behaviour on the basis of past data (Spencer, 2015, p. 493).

A reasonable question arises as to how this is possible. The answer is simple – through the use of artificial intelligence. Regardless of which crime-prediction software is used, its operation involves five stages. Specifically, the predictive policing model consists of phases such as: data collection, data analysis, police operations, criminal justice response, and returning to data collection (Bennett Moses, Chan, 2018, pp. 807-809).

The form of artificial intelligence used for crime prediction is so-called deep learning. This form of artificial intelligence represents a specialised type of machine learning in which it imitates the functioning of the human brain in processing data and creating patterns for use in decision-making. By using hierarchically structured artificial neural networks for the machine-learning process, deep learning functions in a manner similar to the human brain. In deep learning, the learning process is carried out autonomously, meaning that the system is provided with raw data and a task to perform—such as classification—and it learns how to accomplish this on its own, automatically performing feature extraction and modelling steps. Programmers have identified certain issues, such as open-ended reasoning based on common sense and the acquisition of biases. However, it should be noted that efforts are being made to eliminate the identified shortcomings (Dimovski, Grujić, 2024, p. 75).

Predictive policing may rely on two approaches. One is known as the location-based approach, while the other is known as the person-based approach. In cases where predictive policing is based on the location-based

approach, predictive policing programs focus on a single goal: deploying police officers to the right place at the right time (Spasić, Butorac, 2020, p. 321). In other words, this approach is grounded in specific geographic areas for which data on previously committed criminal offences are analysed, resulting in the mapping of so-called hot spot zones. These zones are generated through the use of statistical and algorithmic models, among which PredPol is particularly notable. Predictive Policing software (PredPol), developed through cooperation between the Los Angeles Police Department (LAPD) and the University of California in Los Angeles, uses algorithms to predict where a crime is likely to occur. Based on the so-called near-repeat effect—where the commission of a crime in a particular area tends to lead to an increase in the commission of similar offences in that area—PredPol has been used as a tool for predicting vehicle theft and theft from vehicles by displaying predictions as areas measuring 500 × 500 square feet in which there is a significantly higher risk of repeated criminal activity[1].

A reasonable question arises regarding the effectiveness of PredPol in crime prevention. In this respect, it is sufficient to note that Los Angeles and Santa Cruz recorded a reduction in crime of between 12% and 25% in burglaries and automobile thefts compared to the previous year.[2] It is also interesting to mention a study related to celebratory gunfire in Richmond, Virginia. Each New Year's Eve, a significant increase in random gunfire was recorded. Consequently, the local police began analysing the data and drew certain conclusions, which resulted in the police department deploying officers to pre-selected locations on New Year's Eve in 2003 in order to prevent crime and respond more quickly. This approach led to a 47% reduction in random gunfire and a 246% increase in seized weapons, while saving approximately $15,000 in personnel costs (Pearsall, 2010).

On the other hand, predictive policing is also used through the person-based approach, which focuses on individuals or groups who, according to the algorithm, are identified as high-risk for committing criminal offences or for victimisation. In addition to the fundamental difference between the two approaches, it should be emphasised that location-based predictive policing is typically used to forecast property crime, whereas person-based predictive policing is more commonly applied to the prediction of violent crime. The underlying premise of person-based predictive policing rests on the idea that violent crime is committed by a relatively small group of individuals. Therefore, concentrating law enforcement resources on specific individuals who are at the highest risk of committing a violent offence or becoming victims of violent crime should reduce the overall

[1] Retrieved: 21. July 2025, from: https://www.publicethics.org/post/what-s-wrong-with-predictive-policing

[2] Retrieved: 21. July 2025, from: https://www.prnewswire.com/news-releases/predpols-innovative-predictive-policing-software-results-in-dramatic-crime-reduction-227802601.html?utm

volume of violent crime. An individual may be identified as high-risk on the basis of previous criminal reports, frequency of contact with the police, place of residence, school discipline, and associations with other (potentially) delinquent individuals (Brayne, 2018, p. 297).

The development of the criteria used to classify an individual as high-risk originated from an initiative of the National Institute of Justice (NIJ). In 2009, the NIJ issued a call for proposals to award several million U.S. dollars to police departments capable of developing a predictive policing program. The largest sum was awarded to Chicago, which was directed toward the development of a model called *Party to Violence* (PTV). This model indicated the likelihood that an individual would be either a victim or a perpetrator in a shooting. Soon after, a new model called the *Heat List* was developed through cooperation between the CPD's Information Services Division and engineers at the Illinois Institute of Technology. Using an algorithm, this model assigned a risk score to every previously arrested individual, indicating the probability that they would become involved in a shooting (Cheng, 2025, p.7).

Its practical application consisted of police officers visiting high-risk individuals to warn them that they had been placed on the list. This process of notifying specific individuals was termed *custom notification*.[3] Regarding effectiveness, according to newspaper reports, this approach did not prove successful, and numerous controversies emerged concerning its use.[4]

RULE OF LAW AND DIGITAL PROFILING – AREAS OF CONFLICT

Several contentious issues have emerged among experts regarding digital profiling and the rule of law. The most frequently cited issues include problems related to transparency, accountability, bias—particularly automation bias—and 'positive' feedback loops. With respect to transparency, the central problem is that machine learning, as the fundamental operational model of artificial intelligence used in predictive policing practices, is so complex that it is difficult for end users to understand. In other words, the key issue is the problem of opacity, which refers to situations in which input data is fed into the system, a result is produced at the output, yet it remains impossible to explain what exactly occurred within the algorithm to generate that result. In addition to the fact that artificial intelligence is capable of collecting and processing enormous quantities of data, it is also capable of learning while performing its functions, which further complicates the question of transparency. This means that it becomes im-

[3] Retrieved: 22. July 2025, from: https://teamupturn.gitbooks.io/predictive-policing/content/systems/chicago.html

[4] Retrieved: 21. July 2025, from: https://www.bbc.com/news/technology-37154918

possible to determine the reasoning behind a specific output. Opacity may also result from programming designed for self-protection and for maintaining competitive advantage. *PredPol*, as a program used in predictive policing practices, is characterised by proprietary, secret algorithms. In this regard, it is not incorrect to refer to machine-learning algorithms as 'black boxes,' alluding to the absence of transparency (Storbeck, 2022, pp. 10-11).

The next issue concerns accountability. Artificial intelligence, as a highly complex system, requires the involvement of a large number of experts and organisations from various fields. This is especially true for artificial intelligence used in predictive policing. This leads us to a situation in which it becomes impossible to clearly determine who is responsible for harm or violations of fundamental rights arising from the use of artificial intelligence in predictive policing practices, due to the so-called "problem of many hands" (Storbeck, 2022, p. 11). It suffices to note that the successful application of artificial intelligence in the work of law enforcement depends on a wide range of actors—including programmers, vendors, police administrations, and individual police officers—which further complicates the establishment of responsibility. The existence of numerous involved actors results in mutual accusations, with each pointing the finger at the others. Internationally relevant documents concerning responsibility for harm caused by inadequate use of artificial intelligence will be discussed in the next section of the paper.

The third issue arising from the use of artificial intelligence in police work is potential bias. Generally speaking, experts identify two sources of bias in artificial intelligence systems. Algorithmic bias refers to the bias of programmers, as they—despite good intentions—carry their own prejudices, particularly when it comes to white male programmers, and these biases may be reflected in the algorithm. The second source of bias, known as big-data bias, refers to bias contained within the data itself. It is possible—even when dealing with large quantities of data—that such data is not representative, which directly undermines objectivity in police operations (Storbeck, 2022, p. 11).

A related problem particularly affects women, because in the context of predictive policing, so-called 'gender-neutral' risk assessments are applied, which leads to an overestimation of the risk of reoffending among female offenders. At the same time, the results generated by the use of artificial intelligence for crime prediction disproportionately target minority groups. This directs police work toward those communities and the areas in which they live, potentially causing additional problems and deepening mistrust between state authorities and minority populations (Storbeck, 2022, p. 11). To illustrate these points, we may note that artificial intelligence in Los Angeles, for example, recommended that police activities be focused on areas that were disproportionately poorer and more Latino compared to the city as a whole. At the same time, contemporary empirical

studies confirm that algorithmic bias in predictive policing perpetuates historical injustices through feedback loops, as surveillance of marginalised communities (e.g., Black and Latino communities) is intensified. This situation persists even when the accuracy of predictions is low. In this way, disproportionate targeting of poor and minority neighbourhoods occurs, without any real reduction in crime, but rather with an increase in mistrust and discrimination.[5] Even predictions concerning predominantly white neighbourhoods in which AI forecasted increased criminal activity were clustered in blocks inhabited almost exclusively by Latino residents. Nonetheless, leaders of nongovernmental organisations—such as Thomas Saenz, President and General Counsel of the Latino civil rights group MALDEF, headquartered in Los Angeles—argued that policing in the city was already burdened by bias (Dimovski, Grujić, 2024, p. 80).

From the problem of bias arises automation bias, which refers to the tendency of involved professionals to rely uncritically on computer-generated outputs without any verification of the results, accompanied by a tendency to place greater trust in AI-generated findings than in findings derived from empirical research conducted directly by scholars. Under such conditions, the effects of predictive policing may be questionable. At the same time, 'positive' feedback loops may emerge, further exacerbating existing biases. To explain this in more detail: artificial intelligence may be programmed to identify people of certain ages, races, or neighbourhoods as potential criminals. This establishes a 'positive' feedback loop that increases both operator bias and the bias of the AI system itself. As AI instructs police officers to concentrate their work on particular areas or individuals—thereby increasing the number of arrests—the algorithm ultimately 'learns' that it was correct and that police activity should be further directed toward those specific communities and individuals, regardless of the actual crime rate. In other words, this initially leads to misdirected police priorities. Because feedback data 'confirms' the assumptions produced by artificial intelligence—even when clear security shortcomings exist—the algorithm learns that it is 'accurate' in associating individuals of particular racial, ethnic, and/or socioeconomic backgrounds with criminal behaviour, and will therefore rely on that association more heavily in future predictions. This may result in individuals being wrongly characterised as prone to criminality, inevitably accompanied by discrimination (Storbeck, 2022, p. 11). Recent studies confirm the existence of a feedback loop resulting in intensified police activity in certain areas and toward members of particular racial groups, whereby the algorithm is fed inaccurate data based on biased arrest records. This further reinforces discrimination against minority groups, even in cases where the predictions are inaccurate (Arslan, 2025, p. 49).

[5] Retrieved: 22. July 2025, from: https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes

LIABILITY FOR THE MISUSE OF ARTIFICIAL INTELLIGENCE

The previous section revealed numerous problems that may lead to a range of undesirable consequences. It is sufficient to note that predictive policing based on the use of artificial intelligence may result in unlawful deprivation of liberty, discrimination, violations of human rights, unauthorised data collection, harm, and unfair decisions. Therefore, the question of liability arises for legitimate reasons. In other words, questions may be raised concerning criminal and civil liability. Since this analysis concerns predictive policing, the focus will be placed on criminal liability.

Although it is more than clear that, under the law of the Republic of Serbia, there are several criminal offences relevant to the aforementioned harmful consequences—such as abuse of office under Article 359 of the Criminal Code (Кривични законик, 2005) where an official, using data obtained through artificial intelligence, unlawfully deprives someone of liberty, conducts a search, or engages in discrimination thereby causing harm or seriously violating another person's rights; unlawful deprivation of liberty under Article 132 of the Criminal Code, where an official, relying on data generated through artificial intelligence, unlawfully detains a person through abuse of authority; violation of equality under Article 128 of the Criminal Code, where an official, in the exercise of duties, denies or restricts human or civil rights on the basis of data derived from AI; and unauthorised collection of personal data under Article 146 of the Criminal Code, where an official, in the course of duties, unlawfully obtains, communicates, or uses personal data collected, processed, and used on the basis of law for purposes for which they are not intended—it is evident that proving these criminal offences when committed through the use of artificial intelligence may create additional difficulties in practice. This is because it would be necessary to demonstrate a causal link between the police officer's use of artificial intelligence in predictive policing and the consequences prescribed by the relevant criminal offences. In addition to causation, it is also necessary to establish intent, which further complicates efforts to prove the commission of these offences. Since no prosecutions have yet been initiated for criminal offences committed through the use of artificial intelligence in predictive policing, it is possible that the first such case will reveal additional, as yet unidentified, problems.

Therefore, it is recommended to examine the practices of other countries, as the views of foreign courts may provide guidance in resolving certain dilemmas. One of the earliest relevant decisions is the case *State v. Loomis* from the United States.[6] The case concerned a decision of the Supreme Court of the State of Wisconsin. According to the indictment, Eric Loomis was prosecuted for five criminal offences related to a drive-by shooting in La Crosse. He denied involvement in the shooting; however,

[6] State v. Loomis, 881 N.W.2d 749 (Wis. 2016)

he admitted that earlier that evening he had driven the vehicle used during the shooting, which led him to plead guilty to two counts—attempting to flee from a traffic officer and operating a motor vehicle without the owner's consent. A member of the Wisconsin Department of Corrections included in the Presentence Investigation Report (PSI) a risk assessment generated by COMPAS (Correctional Offender Management Profiling for Alternative Sanction). The risk of recidivism is evaluated on the basis of an interview with the offender and information from the offender's criminal history, while the functioning of the algorithm is a trade secret. The trial court relied on the risk assessment when determining the sentence, ultimately sentencing Loomis to six years of imprisonment and five years of extended supervision (State v. Loomis, 2017, p. 1531).

In his appeal, Loomis argued that reports based on COMPAS software are relevant only to certain groups, while the methodology used to generate the reports is a trade secret, and that the court violated his right to an individualised sentence and his right to be sentenced on the basis of accurate information. It is also important to note that, according to Loomis's claim, the trial court considered gender when determining the sentence, because gender was taken into account by the software as a factor increasing the risk of reoffending (State v. Loomis, 2017, pp. 1531-1532).

The Wisconsin Supreme Court dismissed the convicted defendant Loomis's arguments regarding due process. As for the question of individualised sentencing, it is undisputed that COMPAS provides raw recidivism data for a group of individuals whose characteristics are similar to those of the defendant. At the same time, the Court emphasised the importance of individualisation when determining a sentence. Nevertheless, the Supreme Court concluded that the COMPAS risk assessment did not represent the sole circumstance considered in sentencing, because a judgment that takes COMPAS into account would still remain sufficiently individualised, given the existence of numerous other factors that may influence whether a sentence is more or less severe. This means that judges who rely on risk assessments must explain the factors—apart from the assessment itself—that support the imposed sentence. Every court has the discretionary authority, provided it has the necessary information, to disagree with the assessment when appropriate in the specific case (State v. Loomis, 2017, pp. 1531-1532).

The Court also addressed the defendant's claims concerning the accuracy of the information, emphasising that COMPAS uses only publicly available data and data provided by the defendant, and that Loomis had the opportunity during the proceedings to dispute any piece of information used in preparing the report. Furthermore, the Court affirmed the judgment by rejecting Loomis's argument that gender was used as an aggravating factor in sentencing, stressing that the use of gender as a factor in the risk assessment served a non-discriminatory purpose of promoting the accuracy of the software-generated data (State v. Loomis, 2017, p.1532).

Although the decision of the Wisconsin Supreme Court was that the use of COMPAS was lawful, legal experts pointed out that the Court examined the source code of COMPAS rather than its input and output data, thereby creating the basis for the conclusion that COMPAS was constitutionally compliant. In other words, the Supreme Court focused on the question of whether it was necessary to disclose the algorithm's source code, since the defence could not verify how the system predicted whether an individual would reoffend. It is evident that COMPAS assessed African Americans as being at a higher risk of recidivism, but this occurred because of the input data. This leads to the conclusion that it is more important to analyse the input data than the source code itself, because it is precisely input data that generates hidden bias.[7]

In addition, a particular problem lies in the fact that it is considered that a detailed examination of COMPAS would likely reveal that it is even more biased than a judge. Namely, COMPAS is not necessarily less biased than a judge, because the algorithm itself reflects the biased input data on which it is based. Contemporary studies of fairness metrics applied to COMPAS (e.g., Statistical Parity Difference, Disparate Impact, Equal Opportunity Difference) show that the algorithm does not meet standards of group fairness, exhibiting significant racial disparities in recidivism predictions, which calls for additional measures to enhance transparency and reduce bias (Farayola et al., 2025). If the algorithm is not monitored and corrected, it will certainly not only maintain existing prejudices, but even reinforce them. This means that judges still have an advantage, as they can individualise each case and detect complex causal relationships[8].

Another suggestion concerned the idea that the application of algorithms such as COMPAS in the judicial system requires that their creators be subjected to the same standards as other actors in the system. In other words, programmers, as the creators of the algorithm, should meet the same high ethical and legal standards that we apply to other actors in the criminal justice system (prosecutors and judges)[9].

Although controversial, the decision of the Wisconsin Supreme Court represents an indication of the types of dilemmas that may arise in practice, as well as the way in which they may be resolved, because every algorithm used for predicting criminal behaviour is based on the same principles and has potentially the same shortcomings. In this regard, it is necessary to work on correcting these shortcomings in the coming period.

In addition to the aforementioned court decision, it is important to mention the activities of the European Union in the field of artificial intelligence. Namely, among EU officials, the idea emerged of the need to reg-

[7] Retrieved: 8. Avgust 2025, from: https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1
[8] Ibidem
[9] Ibidem

ulate artificial intelligence in order to ensure better conditions for the development and use of this innovative technology. Thus, in April 2021, the European Commission proposed the first EU law on artificial intelligence. After lengthy negotiations, the European Parliament adopted the final text in March 2024, while the Council of the EU gave its final approval in April 2024. This formally enacted Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts. Among experts, this act is commonly referred to as the Artificial Intelligence Act.

If we were to observe this act through the lens of predictive policing, we could state that Article 14 concerns human oversight over high-risk systems. In order to properly understand Article 14, it is necessary to emphasise that the act classifies AI systems, based on the so-called 'risk-based' approach, into four categories: unacceptable (prohibited), high-risk, limited-risk, and minimal-risk[10]. It is undoubtedly the case that artificial intelligence used as a basis for predictive policing falls under the category of high-risk systems. Therefore, high-risk artificial intelligence systems, as prescribed by Article 14 of the Act, must be designed and developed in such a way—including with appropriate human–machine interface tools—that natural persons can effectively supervise them during the period in which they are in use. At the same time, the purpose of human oversight is to prevent or minimise risks to health, safety, or fundamental rights that may arise when a high-risk artificial intelligence system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. This applies particularly where such risks continue to exist despite the application of other requirements laid down in this section. As for the oversight measures, they must be appropriate to the risk, the level of autonomy, and the context in which the high-risk artificial intelligence system is used[11].

As types of measures that may be applied, the Regulation mentions a measure identified and embedded by the provider, when technically feasible, in the high-risk artificial intelligence system before it is placed on the market or put into use. Additionally, one of the measures refers to the provider, who is responsible for identifying it before the high-risk artificial intelligence system is placed on the market or put into use, and which it is appropriate for the deployer to implement. It is important to emphasise that one or more types of measures may be applied. Furthermore, the supervisory person must be enabled, as necessary and proportionate, to correctly understand the relevant capacities and limitations of the high-risk artificial intelligence system, and must be able to properly monitor its operation,

[10] Retrieved: 19. Avgust 2025, from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[11] Retrieved: 19. Avgust 2025, from: https://artificialintelligenceact.eu/article/14/

including detecting and addressing anomalies, malfunctions, and unexpected performance. The supervisory person must also be aware of the possibility of so-called automation bias, particularly for high-risk artificial intelligence systems used to provide information or recommendations for decisions to be made by natural persons, which includes artificial intelligence systems used in predictive policing. Since understanding the results of high-risk artificial intelligence systems is extremely important, the supervisory person has the obligation to interpret them correctly, taking into account the available tools and interpretation methods. Likewise, in any particular situation, the supervisory person may decide not to use the high-risk artificial intelligence system. For additional safety, the supervisory person may intervene in the operation of the high-risk artificial intelligence system or stop the system using the 'stop' button.[12]

Finally, it is prescribed that for high-risk artificial intelligence systems, the above measures must ensure that, moreover, the deployer does not take any action or make any decision based on an identification generated by the system unless that identification has been specifically verified and confirmed by at least two natural persons with the necessary competence, training, and authorisation. The requirement for specific verification by at least two natural persons does not apply to high-risk artificial intelligence systems used for the purposes of law enforcement, migration, border control, or asylum, where Union or national law considers the application of this requirement to be disproportionate.

The prescribed measures provide significantly better control over high-risk artificial intelligence systems, but for such measures to be implemented, the supervisory person must possess expert knowledge of how artificial intelligence systems function. Engaging such experts to work within an internal affairs authority must be accompanied by adequate financial compensation, which in practice may represent a major challenge. In other words, engaging such experts requires offering appropriate salaries. This may be a problem for economically weaker states, such as the Republic of Serbia, which ultimately increases the risk associated with the use of such artificial intelligence systems.

PREDICTIVE POLICING IN THE REPUBLIC OF SERBIA

As leading countries in the field of artificial intelligence have made significant progress in implementing AI in predictive policing, and as international organisations have established a normative framework, the question rightly arises whether the Republic of Serbia has begun applying artificial intelligence within the work of internal affairs authorities. In connection with this, another question emerges: if the internal affairs authori-

[12] Ibidem

ties do use artificial intelligence, do the competent courts take into account AI-based predictions regarding recidivism when applying Article 54 of the Criminal Code within the general rules on sentencing?

Providing an answer to the first question requires an analysis of the normative framework—the Law on Police (Закон о полицији, 2016), the Law on Records and Processing of Data in the Field of Internal Affairs (Закон о евиденцијама и обради података у области унутрашњих послова, 2018), and the Law on Personal Data Protection (Закон о заштити података о личности, 2018). Under the Law on Police, Article 24(1) prescribes that the Police Directorate shall develop a strategic assessment of public security in cooperation with the organisational unit responsible for strategic planning. Articles 25(2) and 25(3) stipulate that the tasks of a police administration include developing an operational assessment of public security in accordance with the act referred to in Article 24(1) of that Law, and adopting an operational plan of the police administration in accordance with the act referred to in Article 24(2) of that Law. Likewise, it should be emphasised that the legislator, within the types of police tasks listed in Article 30, recognised the need to include crime prevention and the improvement of community safety as one of these tasks (Dimovski, Grujić, 2024, p. 81).

In addition to the Law on Police, as already noted, the Law on Records and Processing of Data in the Field of Internal Affairs is also significant. Considering its provisions through the lens of data processing for decision-making related to crime prevention, Article 21 should be mentioned. Article 21 prescribes the keeping of an event record. This event record contains: (1) a description of the event, the reporting level, and the classification of the event; (2) the location of the event (city, street, intersection, house number, entrance, floor, information on the location, GPS coordinates, road, road kilometre, meter of the road, border crossing, border marker, navigable waterway kilometre, location, specific location name, security sector, traffic sector, and the locally competent organisational unit of the Ministry); (3) the date and time of the event and the time the notification was received; (4) the reporting level and classification of the event; (5) the name, surname, address, and contact information of the person who reported the event; (6) the name and surname, personal identification number, address, and contact information of the person involved in the event; and (7) information on the police officer or member of the fire and rescue unit who received the notification or participated in the intervention. Although not all of this data is relevant when creating a crime prevention plan, it should be emphasised that proper maintenance of the event record is an essential prerequisite for correctly understanding the dynamics of criminal activity and for undertaking preventive measures. Based on the above, it can be stated that the legislator has recognised the need for collecting and analysing data on committed criminal offenses.

Regarding the Law on Personal Data Protection, it should be emphasised that, pursuant to paragraph 1 of Article 3, it also applies to the processing of personal data carried out, in whole or in part, by automated means. In this regard, the legislator has provided in Article 5 that personal data must be based on the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability. Although data minimisation is prescribed as one of the principles on which the legal text rests, the question arises as to whether the application of algorithms used for predictive policing would be in accordance with this principle, bearing in mind that databases on (potential) perpetrators of criminal offenses contain a large amount of data.

The legislator provided in Article 9 that a clear distinction must be made between data concerning different categories of persons whose data is being processed: persons for whom there are grounds for suspicion that they have committed or intend to commit criminal offenses, persons for whom there is reasonable suspicion that they have committed criminal offenses, persons convicted of criminal offenses, persons harmed by a criminal offense or persons presumed to be at risk of being harmed by a criminal offense, and other persons connected with a criminal offense, such as witnesses, persons who may provide information on the criminal offense, associated persons, or accomplices of the persons listed in items 1) to 3) of this Article. Namely, when processing data concerning these persons for special purposes, the competent authority is obliged, where possible, to make a clear distinction between data related to each category of persons whose data is being processed. We take the view that it is beneficial that the legislator prescribed maintaining separate records for each of these categories, as this serves to protect their rights.

It is important to establish the conditions under which the lawful processing of personal data is permitted. Thus, the processing of personal data is lawful, among other things, when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (paragraph 1, item 5 of Article 12). At the same time, Article 17 prohibits the processing that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health, or data concerning the sex life or sexual orientation of a natural person. Accordingly, the question arises whether such a legal solution would be compatible with existing algorithms used for predictive policing. On the other hand, we must be aware that disclosing such data could lead to discrimination, which may result in the commission of certain criminal offenses.

A particular problem regarding the full implementation of predictive policing relates to the rights of the data subject. A citizen has the right to

receive from the controller, in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, all information relating to data processing. The information may be provided in written or other form, including electronic form, if appropriate. If the data subject requests it, the information may be provided orally, provided that the identity of the person is unquestionably established. The legislator distinguishes two situations—when personal data is collected from the data subject (Article 23) and when personal data is not collected from the data subject (Article 24). In the first case, the controller is obliged, at the moment of collecting the personal data, to provide the data subject with information on the identity and contact details of the controller and its representative, if one has been appointed. Likewise, the controller must provide contact information for the data protection officer, if appointed, information on the purpose of the intended processing and the legal basis for the processing, as well as information on the recipient or categories of recipients of the personal data, if they exist. This situation applies in cases where data that would be used to assess recidivism is collected through direct conversation with a specific person, as in the example mentioned from the United States.

Regarding the second situation, the controller is obliged to provide the data subject with the following information: the identity and contact details of the controller and its representative, if one has been appointed; the contact details of the data protection officer, if one has been appointed; the purpose of the intended processing and the legal basis for the processing; the type of data being processed; and information on the recipient or categories of recipients of the personal data, if they exist. However, in both situations, the controller is obliged to provide the data subject with additional information necessary to ensure fair and transparent processing in relation to the data subject.

The right of access to information may be restricted under conditions prescribed by law (Article 28). Full or partial restriction of the right of access to information may occur if it is necessary and constitutes a proportionate measure in a democratic society, while respecting the fundamental rights and legitimate interests of the data subject, in order to: (1) prevent interference with official or legally regulated information collection, investigations, or procedures; (2) enable the prevention, investigation, and detection of criminal offenses, the prosecution of perpetrators, or the execution of criminal sanctions; (3) protect public security; (4) protect national security and defence; and (5) protect the rights and freedoms of other persons. Based on these grounds for restricting the right of access, it follows that this right would be restricted for a given individual in the event of the application of artificial intelligence in predictive policing.

Particular attention must be paid to Article 38, which provides that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, if such a decision produces legal

effects concerning that person or significantly affects that person's position. If this article is viewed through the lens of artificial intelligence and predictive policing, it may be concluded that if an algorithm assesses the risk of recidivism or the likelihood of committing a criminal offense—which is indeed the case—the provision prevents the use of the algorithm for such purposes when the decision is based solely on automated processing. The legislator has also prescribed several exceptions, namely, when such automated processing is necessary for entering into or performing a contract between the data subject and the controller; or when it is based on law, provided that the law prescribes appropriate measures for protecting the rights, freedoms, and legitimate interests of the data subject; or when it is based on the explicit consent of the data subject. In our case, only the second exception is relevant. Although the legislator has provided additional safeguards under the first and third exceptions—such as the participation of a natural person under the controller's authority in decision-making, the right of the data subject to express their view regarding the decision, and the right to challenge the decision before the controller's authorised person—these safeguards do not apply when automated processing is based on a special law, which would likely be the case in the context of predictive policing. This means that the position of a person whose risk of recidivism or committing a criminal offense in a specific area is being assessed would be deprived of these safeguards, while human oversight of such algorithms is an obligation under the EU Artificial Intelligence Act.

On the other hand, Article 39 prohibits competent authorities, when acting for special purposes, from making decisions based solely on automated processing, including profiling, if such a decision may produce adverse legal effects concerning the data subject or significantly affect that person's position, unless the decision is based on law and the law prescribes appropriate measures to protect the rights and freedoms of the data subject, at minimum ensuring the participation of a natural person under the controller's authority in the decision-making process. Nevertheless, Article 40 establishes certain limitations, provided that they do not affect the essence of fundamental rights and freedoms and that they constitute a necessary and proportionate measure in a democratic society for the protection, among other things, of the prevention, investigation, and detection of criminal offenses, the prosecution of perpetrators of criminal offenses, or the execution of criminal sanctions, including the prevention of and protection against threats to public safety.

Likewise, the role of the Commissioner in the implementation of the law should not be overlooked. It is sufficient to mention Article 78 and conclude that the Commissioner has the authority to supervise the application of the law, impose measures, and issue warnings regarding unlawful processing. If his powers are viewed through the lens of predictive polic-

ing, the Commissioner would have to be granted access to algorithms and data in order to verify legality.

The second question raised at the beginning of this chapter concerns the application of Article 54 of the Criminal Code. Specifically, the court shall determine the punishment for the perpetrator of a criminal offense within the limits prescribed by law for that offense, taking into account the purpose of punishment and considering all circumstances that affect whether the punishment should be mitigated or aggravated (mitigating and aggravating circumstances), particularly: the degree of guilt, the motives for committing the offense, the extent of endangerment or violation of the protected legal interest, the circumstances under which the offense was committed, the offender's prior life, his personal circumstances, his conduct after the commission of the criminal offense, especially his attitude toward the victim, as well as other circumstances relating to the offender's personality. A correct answer to this question requires an analysis of Article 55 of the Criminal Code, according to which, if the perpetrator of an intentional criminal offense has previously been convicted for an intentional criminal offense, the court shall consider that fact as an aggravating circumstance, provided that five years have not elapsed since the previous conviction or since the execution of the sentence. By analysing the existing provisions of the Criminal Code, we may conclude that there is no normative basis for excluding the consideration of potential recidivism projected by an algorithm as an aggravating circumstance when determining the punishment.

CONCLUSION

Artificial intelligence has made a significant leap in the way such systems function, enabling their application in areas where this was until recently unimaginable. It is rightly expected that the role of artificial intelligence in combating crime will continue to grow, even though certain problems exist at this moment. Therefore, it is necessary to work on eliminating these problems in order to fully utilise the potential that artificial intelligence brings. Whether these problems will indeed be resolved remains uncertain, but it is evident that states around the world, as well as certain international organisations, have undertaken measures aimed at creating a normative basis for its application in various fields, including predictive policing. Only its full implementation in the future can provide a sound basis for properly assessing the benefits of using artificial intelligence for crime prevention.

On the other hand, one should not remain passive and fail to work on improving the normative framework, because the progress—occurring daily—in the performance of artificial intelligence will not wait for legislators to adopt the necessary regulatory acts. Establishing a sound norma-

tive foundation requires the involvement not only of members of national parliaments but also of artificial intelligence experts, since only synergistic efforts can eliminate as many potential problems as possible.

In conclusion, it should be emphasised that the increased use of algorithms for assessing recidivism creates a serious problem with regard to individual criminal responsibility. The fundamental concept of criminal law is that it is based on subjective guilt, which is determined in judicial proceedings on the basis of established facts. On the other hand, algorithms such as COMPAS operate in a completely different manner. These algorithms base their assessments on the future, predicting what a particular individual might do based on statistical patterns derived from past data. In such a situation, the defendant is transformed into an object whose future behaviour is evaluated by an algorithm. In some jurisdictions, the algorithm's assessment is used as a basis for imposing harsher sentences, thereby leading to a de-individualisation of punishment. It is precisely in this that the greatest danger of the broader use of recidivism risk assessment algorithms lies.

ACKNOWLEDGMENT: *The paper was created as a result of funding by the Ministry of Science, Technological Development, and Innovation, under Contract No. 451-03-34/2026-03/200120 dated February 5, 2026. This paper is the result of research funded by the Ministry of Science, Technological Development and Innovation under Contract No. 451-03-137/2025-03/200254 dated 4 February 2025. The paper was created as a result of funding by the Ministry of Science, Technological Development, and Innovation, under Contract No. 451-03-34/2026-03/200254 dated February 5, 2026. The paper is the result of the author's scientific research conducted within the 2026 Research Program of the Faculty of Law, University of Kragujevac, funded by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia.*

REFERENCES

Arslan, S. (2025). The legal implications of predictive policing algorithms: Bias, oversight, and public accountability. *Journal of Legal Studies and Digital Age*, 2(3), 49,

Bennett Moses, L., Chan, J. (2018), Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society An International Journal of Research and Policy*, 28(7),

Brayne, S. (2018), The Criminal Law and Law Enforcement Implications of Big Data, *Annual Review of Law and Social Science*, San Mateo,14,

Cheng, S. (2025), Predictive Policing in Practice: A Case Study of Chicago's Strategic Subject List, Claremont Colleges, Claremont.

Farayola, M. M., Tal, I., Saber, T., Connolly, R., & Bendechache, M. (2025). A fairness-focused approach to recidivism prediction: Implications for accuracy, trust, and equity. *AI & Society,*

Pearsall, B. (2010). Predictive Policing: The Future of Law Enforcement?, *NIJ Journal*, no. 266,

Spencer, S. (2015). When Targeting Becomes Secondary: A Framework for Regulating Predictive Surveillance in Antiterrorism Investigations, *Denver University Law Review*,

Spasić, D., Butorac, K. (2020). Predictive policing: one step further to a safe community, *Archibald Reiss days - thematic conference proceedings of international significance*, Kriminalističko-policijski Univerzitet, Beograd,

State v. Loomis, 881 N.W.2d 749 (Wis. 2016)

State v. Loomis (2017). Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing, *Harvard Law Review*, 130(5),

Storbeck, M. (2022). *Artificial intelligence and predictive policing: risks and challenges*, EUCPN, Brussels,

Димовски, Д., Грујић, З. (2024). Могућности употребе вештачке интелигенције у превенцији криминалитета [Possibilities of Using Artificial Intelligence in Crime Prevention], *Безбедност*, Министарство унутрашњих послова Републике Србије, Београд, 2,

Закон о евиденцијама и обради података у области унутрашњих послова [Law on Records and Processing of Data in the Field of Internal Affairs], Сл. гласник РС, бр. 24/2018

Закон о заштити података о личности [Law on Personal Data Protection], Сл. гласник РС, 87/2018

Закон о полицији [Law on Police], Сл. гласник РС, бр. 6/2016, 24/2018 и 87/2018

Кривични законик [Criminal Code], Сл. гласник РС, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 и 94/2024

Retrieved: 21. July 2025, from: https://www.publicethics.org/post/what-s-wrong-with-predictive-policing

Retrieved: 21. July 2025, from: https://www.prnewswire.com/news-releases/predpols-innovative-predictive-policing-software-results-in-dramatic-crime-reduction-227802601.html?utm

Retrieved: 21. July 2025, from: https://www.bbc.com/news/technology-37154918

Retrieved: 22. July 2025, from: https://teamupturn.gitbooks.io/predictive-policing/content/systems/chicago.html

Retrieved: 22. July 2025, from: https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes

Retrieved: 8. Avgust 2025, from: https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1

Retrieved: 19. Avgust 2025, from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Retrieved: 19. Avgust 2025, from: https://artificialintelligenceact.eu/article/14/

ПРЕДИКТИВНО ПОЛИЦИЈСКО ПОСТУПАЊЕ И ВЛАДАВИНА ПРАВА: РИЗИЦИ ДИГИТАЛНОГ ПРОФИЛИСАЊА У ПРИМЕНИ ЗАКОНА

Дарко Димовски[1], Вељко Турањанин[2], Здравко Грујић[3]

[1]Универзитет у Нишу, Правни факултет,
Правосудни истраживачки центар, Ниш, Србија
[2]Универзитет у Крагујевцу, Правни факултет, Крагујевац, Србија
[3]Правни факултет Универзитета у Митровици, са привременим седиштем
у Косовској Митровици, Косовска Митровица, Србија

Резиме

Савремена полицијска пракса све више почива на предиктивним технологијама – софтверима који на основу историјских података о криминалу, геолокацији, па чак и података са друштвених мрежа покушавају да предвиде где ће се, када и ко би могао починити кривично дело. Овакав, савремени начин рада се већ увелико примењује од стране појединих полицијских управа. Довољно је навести Чикаго, Лос Анђелес, али и поједине европске градове како би се илустровала употреба предиктовног полицијског поступања. Иако се сматра револуционарним, овај начин рада отвара доста питања, недоумица и контроверзи. Стога, је неопходно на сва питања покушати дати одговор јер је само тако могуће вршити превенцију вршења криминалитета, са једне стране, и заштити људска права, са друге стране. Битно је истаћи да предиктивно полицијско поступање често појачава постојеће друштвене предрасуде, што резултира томе да полиција усмерава свој рад ка 'ризичним' категоријама становништва. На тај начин се крши претпоставка невиности, права на приватност и начела једнакости пред законом. Поред овога, поставља се питање у вези транспарентности алгоритама. Несумњиво је да је већина софтвера, који представљају основу предиктивног полицијског поступања, производ приватних компанија. Тиме се долази до тога да компаније штите алгоритам тиме што га проглашавају пословном тајном. На крају уколико полиција интензивније контролише одређено подручје само зато што је алгоритам означио као 'врућу тачку', аутоматски расте број евидентираних дела, што додатно 'храни' алгоритам и ствара зачарани круг. Аутори у раду анализирају случај ССттааттее вв. Лоооммиисс (2016) у којем је од стране суда употребљена предикција криминалног понашања као отежавајућа околност. С тим у вези последњи део рада посвећен је употреби предиктивног полицијског поступања у Републици Србији, при чему аутори покушавају да одговоре на постављена питања у вези тога да ли је Република Србија почела са применом вештачке интелигенције у раду органа унутрашњих послова и да ли надлежни судови узимају предикцију вештачке интелигенције у погледу рецидивизма као отежавајући околност код општих правила о одмеравању казне.