UDC: 351.74:004
DOI: 10.5937/PDSC26019M

Darko M. Marković, PhD, Associate Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
Business Academy University in Novi Sad
darko.markovic@pravni–fakultet.edu.rs
ORCID ID: https://orcid.org/0000–0001–9124–6417

POLICE PRACTICES AND ALGORITHMIC RISK: IMPLICATIONS FOR SECURITY AND HUMAN RIGHTS IN THE DIGITAL AGE

Abstract: Digitization of police functions – predictive algorithms, automated risk assessments and digital traces – raises the question of who controls these systems and whose rights can be sacrificed in the name of efficiency. This is not a new dilemma. Although police authorities respect the sensitivity of certain categories of citizens, the question cannot be avoided as to how much digital tools serve security and how much they serve the expansion of state surveillance. In practice the line often shifts, sometimes imperceptibly. Even when not in an accusatory tone, such questions lead to rethinking the relationship between technological progress and democratic values. Science did not remain absent. Through the prism of criminology, law and sociology, the lack of transparency and technical dependence of police authorities is highlighted. This is visible in everyday practice. Belief that efficiency justifies limiting individual rights – a belief that, though outdated, still shapes institutional behaviour – is often the reason for passive acceptance of these practices. But is that really the case? This is where the problem begins. Observing police practice in digital society through an interdisciplinary prism, the aim of the paper is to show that the fear of technological backwardness is not the main reason for accelerated introduction of AI tools. Behind the mirror of efficiency often hides an unexamined desire to expand institutional power. Analysis of legal and operational frameworks points to algorithmic risk in the context of European approaches to security management, while the second part sheds light on the causes of institutional silence and their consequences for discrimination, privacy and decision–making autonomy.

Keywords: *digital tools; operational decision-making; oversight mechanisms; privacy; civil liberties*

1. INTRODUCTION

Digitization of police work is often presented as an inevitable, almost self–evident step forward – as a form of technical modernization that is assumed to speed up procedures, reduce the number of errors and enable institutions to more adequately respond to modern security challenges (Brayne, 2020; Ferguson, 2017). Nevertheless, behind that seemingly neutral narrative about "efficiency", questions arise that cannot simply be avoided: who in reality manages digital systems, on the basis of which exact criteria do these systems make assessments and decisions, and whose rights may be threatened at the moment when decision–making is actually left to algorithms, and not to specific individuals (Pasquale, 2015; Zuboff, 2019).

The dilemma as such is not new, but it has become more visible and complex in the digital environment. Police authorities, at least at the normative and declarative level, formally respect the sensitive position of certain categories of citizens, however, in actual practice, the border between legitimate security needs and the expansion of surveillance moves gradually, quietly and most often without a clear trace in the public debate (Lyon, 2018). It is precisely this invisibility that makes digital tools more powerful than they seem at first glance: when a decision is based on a model whose operation cannot be clearly explained to either the one implementing the decision or the one to whom it applies, it is difficult to talk about real transparency or responsibility in the classic, legal sense of the word (European Union Agency for Fundamental Rights [FRA], 2021)..

The aim of this paper is not only to describe how predictive algorithms, automated risk assessments and reliance on digital traces are introduced, but to show that this process cannot be explained primarily by the fear of technological backwardness in relation to other states or actors. It starts from the assumption that the accelerated acceptance of these tools largely stems from the often unspoken and insufficiently examined institutional desire to expand powers and control over citizens (Eubanks, 2018). Through the analysis of police practices in the digital society, consideration of the concept of algorithmic risk and changes in the understanding and application of the limits of police authority, the paper tries to point out that technological solutions are increasingly functioning as a new infrastructure

of power, whereby the mechanisms of external and internal supervision are either absent or remain only formally present (Yeung, 2018).

In the continuation of the work, it will be considered how the operational and legal frameworks of police work look like today, in practice, but also what it means that the institutions almost never openly talk about how digital systems really work, who technically "keeps them alive" and how their results turn into concrete decisions on the ground. In particular, problems related to how visible the entire process is to citizens, who and to what extent bears responsibility for decisions made with the help of these systems, as well as how realistically it is possible for the public to have insight into and influence such work will be highlighted. In addition, the power imbalance that arises when the appeal to efficiency is used as the main excuse for ever deeper intrusion into the privacy and independence of citizens is analyzed (FRA, 2021; Zuboff, 2019). This opens up a wider question to which this paper tries to offer an answer: how is it possible to ensure that digitization really contributes to the improvement of security, instead of becoming a means of a gradual and hardly noticeable expansion of surveillance.

2. POLICE PRACTICES IN DIGITAL SOCIETY

Today, there is a lot of talk about the changes brought about by the digital society – not only in the everyday, usual activities of the average person, but also in the activities in the economy, and especially in the work of state institutions (Meijer & Wessels, 2019). The need for the economy to adapt to new ways of working, especially in terms of communication and decision–making, is quite justified, because the willingness to accept new trends is directly proportional to the growth of income. State institutions are at the service of both citizens and the economy, so the digitization of their jobs is completely logical and necessary. However, nothing happened overnight, these changes came about through a gradual transition to an environment where information moves faster than people, and the expectations of citizens and consumers grow day by day. At some point, speed simply became the default, and everything that once served our needs suddenly became too slow and unacceptable. There was a time when you had to wait days for data or a decision; now, if the information doesn't appear immediately, it seems to be delayed.

Digital tools have made it possible for citizens and institutions to access data quickly, process it and monitor events in real time (Kitchin, 2014). Citizens have become accustomed to doing everything online – from

paying bills to buying tickets – so it was logical for them to expect the same from the state. That is why eGovernment, digital registers and various electronic services were introduced.

This pressure on the state to be faster and more open had to be reflected in the work of the police, causing corresponding changes. The classical approach depended in many respects on the human factor. Everything relied on reports, conversations and field work, which could not be unified due to differences in the character and professional abilities of police officers. That approach was inevitably slower and required a lot of experience and judgement. He was not perfect, but he had human logic, which nevertheless has some of its advantages. Nowadays, digital traces and automated analysis are increasingly used (Brayne, 2020). It speeds up processes and reduces room for error, but it also raises the question of the limits of police powers. Because the police, like every institution, has its weaknesses, so it is important to clearly separate what is an official need and what is supervision that goes beyond those limits (Ferguson, 2017).

One part of these practices includes OSINT (Open–Source Intelligence) – collecting data from publicly available sources that gather a large number of users, such as various social networks, forums, media archives. Users of digital social media themselves often do not see the danger in exposing certain information to the public. All this seems harmless to them at first glance: the information is public, so who could dispute its use? However, in reality it is not at all simple, especially since it is often done without clear rules and procedures. The way information is collected, verified and used is rarely completely transparent, especially when it comes from a form of mass surveillance (Bayerl & Akhgar, 2022; Domazet, Marković & Skakavac, 2024). How long is this data stored? Who has access to them? What happens when information taken from a forum – perhaps incorrect, perhaps taken out of context – ends up in police records? We face that every day. But is it really that harmless?

Another example is predictive policing systems. They analyze past events to indicate places or situations where incidents could occur. Based on this, patrols are planned and work priorities are determined. On paper, that makes sense – why not try to prevent crime before it happens? However, if the data on which the system is based is biased, so will its results. And the data is almost never neutral, because it comes from the history of police work, which in itself carries certain patterns and inequalities (Lum & Isaac, 2016; Richardson, Schultz & Crawford, 2019). Thus, the old models of surveillance are repeated, only now in digital form. And the same question opens again: who monitors the algorithm that

monitors the police?

More and more often, we leave the job of risk assessment to various automated systems. They "add and subtract" the likelihood of threats, security incidents or problems at large gatherings, and present themselves as completely objective, scientific and precise, as if beyond the reach of human error. In reality, few people really understand how these systems work. How they arrive at their results is mostly closed to the public, and what they end up with is accepted almost automatically (Oswald, Grace, Urwin & Barnes, 2018). Once a number appears, one gets the impression that it is a fact that does not need to be questioned. It is this blind faith in the "infallibility" of computers that is most worrying.

Finally, police work increasingly relies on digital clues. Location data, communication metadata, video surveillance footage, digital fingerprints – all of these can be of crucial importance in investigations, and no one questions that. The problem arises when their mass availability and the possibility of combining open space for new forms of surveillance. For forms that go beyond the traditional limits of police powers. Those boundaries, no matter how broad or imprecise, still existed. Now they are moving. Sometimes quietly and almost imperceptibly. Sometimes quite consciously. And sometimes it seems that no one knows for sure where those borders are.

3. ALGORITHMIC RISK AS A NEW CATEGORY OF SECURITY MANAGEMENT

Recently, the term "algorithmic risk" has been mentioned more and more often, although almost no one used it in security policies until now. Previously, risk was assessed based on experience, judgment and concrete events, so within frameworks that people could understand and explain. However, with digitization a new logic has emerged: risk is no longer "assessed" but "calculated". Models, matrices, weightings, historical data – all of this is included in the calculation, and the result is presented as something objective, although in the background there are assumptions that are not always visible (Barocas & Selbst, 2016).

European institutions are trying to keep pace with these changes, but it appears that there is a gap between what technology can do and what institutions can control. The documents often talk about the "responsible use of artificial intelligence", but in practice it mostly remains at the level of recommendations and general guidelines. The most important question – who bears responsibility when an algorithm goes wrong – still remains

unanswered. Police services are increasingly using digital tools, but hardly anyone can explain how these tools actually work, what they are based on and where their limits are (Kroll et al., 2017).

In practice, the consequences are seen immediately. The moment the algorithm "calculates" the risk, that result is suddenly given more weight than a simple assessment would have. The number that appears on the screen is generally accepted without much thought. Few people question whether the data on which it is based is really reliable, whether there was bias in its collection, whether something is missing or perhaps misinterpreted (Richardson et al., 2019). The digital process is simply trusted.

Even if a police officer were to suspect such an assessment, there is usually no way to verify it, because he does not know how it came about in the first place. In this way, "algorithmic risk" becomes a new kind of authority – silent, invisible, but very influential (Oswald et al., 2018).

That's why it's wrong to see algorithmic risk as just a technical issue. In its background is actually the question of power: who has it and how it is used. Whoever manages these systems indirectly influences where people and equipment will be sent, what will be prioritized and what security policies will be formed. Behind an apparently neutral technical solution, human weaknesses, interests and decisions are hidden (Sandhu & Fussey, 2021).

If this aspect is neglected, if these processes are not monitored and controlled, it can easily happen that decisions are made by an algorithm in practice, while the responsibility of people is pushed aside. And then it is no longer just a question of the way the police work, but the way the whole society functions (Yeung, 2018; Brayne & Christin, 2021).

4. THE LIMITS OF POLICE POWERS IN THE DIGITAL ENVIRONMENT

The digital environment has opened up possibilities that did not exist before, but at the same time it has blurred the boundaries of police powers. What was once clearly defined – what police can and can't do – is now increasingly being refracted through technology that itself has no boundaries. Of course, the police are obliged to use modern tools, but the question arises: are the limits of authority moving because it is really necessary, or because technology makes it possible (Ferguson, 2017; Marković, 2021; Marković & Zirojević, 2025)?

In the traditional system, police powers were tied to specific actions:

search, collection of evidence, hearing, surveillance. It all had its own procedures and limitations. Today, however, much of the work is done through digital traces that are collected automatically, often without clear awareness of who collected them, when and under what conditions. When data is "somewhere in the system", it's easy to forget that it's subject to rules, just like any other piece of evidence (Brayne, 2020).

The problem arises the moment when different digital data starts to intersect. One piece of information often doesn't mean much by itself, but when combined with other pieces of information – location, communications, camera footage – you get a picture that wasn't previously possible without serious, targeted surveillance. That picture can reveal far more than that person has ever consciously agreed to share. This begs the question: does the police even have the right to make such combinations of data, or does this cross the limit that existed in the analog world (Bukazić, 2026; Joh, 2015)?

Another problem is that digital surveillance is mostly invisible. Classic surveillance was palpable: a policeman on the street, a camera on the corner, an officer asking for ID. Digital surveillance doesn't work like that. It takes place "behind the scenes", through the exchange of information between different systems and databases (Domazet, Marković & Skakavac, 2024).. Most citizens do not even know that they are covered by some form of monitoring. When surveillance becomes invisible, the limits of authority become even more important, but at the same time more difficult for surveillance and public control (Pasquale, 2015)..

Finally, the question of responsibility is raised. When a police officer makes a decision based on his own judgment, it is clear who is responsible for it. When a decision is "suggested" by an algorithm, responsibility is spread between the institution, the software manufacturer, and the system itself. In practice, this easily leads to no one really being held accountable, even though the decision had serious consequences for someone's life or rights. That is why the limits of police powers in the digital environment cannot be reduced to a legal issue only; they are at the same time a matter of protection of basic rights and trust of citizens in institutions (Yeung, 2018).

5. TRANSPARENCY, RESPONSIBILITY, AND PUBLIC CONTROL

As with many other scientific achievements, primarily progressive effects were expected from digitization, but in practice the opposite

happened. Thus, it was quite justifiably believed that the introduction of new technologies will make the work of state bodies more transparent, that citizens will be able to more easily monitor how decisions are made, that there will be clear traces, records, databases that can be accessed and analyzed. It was thought that the computer would "illuminate" the process, not darken it further. This, of course, should also apply to the police.

In reality, however, it often happens that the more technical innovations are built into a system, the harder it is to explain how it all actually works. Most of the classic police actions and procedures were relatively comprehensible even to a layman. It was known who receives the application, who goes to the field, who writes the report, who signs it, who makes the decision and on what basis. Of course, when a person forms the backbone of the procedure, subjectivity is inevitable, and with it the possibility of mistakes, but at least it was clear who was doing what and at what time. In the digital environment, a good part of these procedures takes place somewhere "behind the screen", where they are managed by software modules instead of the people we see (Brayne, 2020). For the purposes of digitized procedures, internal databases, interfaces used only by officials, and automated assessments that are executed in the background are used. This means that what was once visible, now takes place imperceptibly and, often, not even the police officers themselves are able to see the entire path from the initial information to the final decision. The algorithm determines in which direction everything will take place. For example, in risk assessment, the algorithm calculates the risk, and the system pulls data from several different databases and creates a list of risky situations or people. All this turns out to be a finished result, and the path that led to it is not visible to citizens, often not even to police officers (Bukazić, 2026; Oswald et al., 2018). The outcome in the form of a number, mark or recommendation does not contain an explanation of the logic behind it. Thus, even those who are supposed to carry out internal supervision cannot always clearly reconstruct what actually happened in the system itself.

This creates a serious problem for public control. Citizens formally have the right to know how decisions affecting them are made – whether they will be stopped, checked, put under surveillance, included in some "risky" category. However, it is difficult to explain a procedure that even the police officers themselves cannot fully follow. When the decision is based on an algorithm, what we usually get is just a result: "high risk subject", "high risk zone", "suspicious activity". How it came about, in which order the data was processed, which criteria were applied – this mostly remains invisible (Domazet et al., 2024; Marković & Marković,

2025; Pasquale, 2015). And without that insight, the word "transparency" remains an empty form.

One of the problems is how these digital systems are talked about, both in public and within the state authorities themselves. They are often presented as "neutral", "objective" or "scientifically based", so it turns out that what the system "puts out" has nothing to do with human weaknesses – as if there are no emotions, prejudices, pressures or misjudgments. In reality, any such tool is only as reliable as the data it "eats" and the people who build and use it (Richardson et al., 2019). If half–hearted, biased or outdated information enters it, so will the results, regardless of whether they are presented as pretty tables, graphs or precise numbers.

It is also important that wrong or biased decisions are more easily "masked" in digital form. When a policeman stopped someone on the street because he "seemed suspicious", at least it was clear that this was a personal assessment, which could be questioned, challenged or reconsidered. When a system labels a person as "at risk" based on a set of criteria that no one on the outside can see, the misjudgment takes on the appearance of scientific validity. Transparency in the digital environment cannot therefore be reduced to the mere publication of final results; it also implies understanding the process that leads to those results.

Although there are organizational units for information technology within the police, with employed programmers, digital tools for the police's needs are not created within the service, but are procured from private companies. This makes public scrutiny even more difficult because the software, acquired in such a way, often comes as "ready–made solutions", with closed contracts, license clauses and references to trade secrets (Marković & Zirojević, 2025). Such solutions tie the hands of the state, or in this case the police, because there is limited insight into how the obtained software works "from the inside" (Sandhu & Fussey, 2021). The company that developed and sold the software locks down the algorithms, and the documentation, if available at all, is often sparse with information, so the possibility of independent peer review is minimal. Thus a paradox arises: an institution that has the right to limit the freedom of citizens relies on a tool that it cannot fully explain itself.

When you add to that the fact that citizens usually do not have any access to these systems, it is clear why there is room for abuse, but also for loss of trust. If a person cannot find out why they are on a list, why they are controlled more often than others, or why a certain event is marked as "risky", it is logical that they will feel helpless and suspicious. Trust in institutions is not only built on the fact that they "follow the law", but also

on the fact that they are able to explain their actions to the common man. In a digital system, where everything is "behind the scenes", that task becomes much more difficult (Yeung, 2018).

That is why it is important that transparency in the digital environment is not understood narrowly, only as an obligation to disclose a certain amount of data or statistics. Transparency should also mean an obligation to explain the way in which this data is collected, connected, filtered and turned into concrete decisions. Who chooses the criteria? Who checks whether the system gives wrong or discriminatory results? Is there an independent body that has the right to look at the algorithm and say, "This is not right" (Kroll et al., 2017)?

Without answers to these questions, digitization can easily become just another layer of non–transparency, a thin shell behind which old problems are disguised in new technical clothes. Instead of facilitating insight into the work of institutions and strengthening citizens' trust, it risks creating the impression that "somewhere in the system" something is being decided, without anyone knowing exactly where, how and why. And once trust is lost, it's hard to get it back – no matter how advanced the software behind the scenes.

6. EFFICIENCY, PRIVACY AND POWER IMBALANCE

Digital tools have brought police capabilities that sounded like science fiction twenty or thirty years ago. Today, it is normal for huge amounts of data to be processed in a few seconds, for different databases to be "connected" with one click, for events to be monitored almost in real time. From the point of view of work organization, it seems like a great civilizational leap: less paper, faster decisions, more information available to those who need to react (Richards & King, 2013).

Advances in technology aren't free – it's just that the cost isn't immediately apparent. Most often it is paid for by giving up a part of privacy. When we talk about "efficiency", we easily forget that behind each line in the table there is a concrete person, with his daily life, problems and mistakes.

In the old, "paper" system, everything was much more tangible. You knew when a policeman stopped you, when he asked for your ID card, when you received a summons or when a case was filed against you. There was a clear moment when you could say, "Here, now something is happening to me and I can see it". Today, much of it flies under the radar. Systems automatically pull data from registers, cameras, communication

logs, location records and various other traces we leave along the way (Stojšić Dabetić, Mirković & Aleksić Oliveira, 2025). That data is combined in the background, filtered, compared with old cases and eventually emerges as some kind of risk assessment, label or ranking. In most cases, people have no idea at all that they have ended up in someone's template or "profile" (Brayne, 2020).

In such an environment, the right to privacy ceases to be just a paragraph in the law and becomes a question of whether you even have a sense of control over your own life. Privacy means that you at least roughly know who has what information about you and why. When everything happens "behind the scenes", that feeling slowly disappears (Domazet et al., 2024; Marković & Zirojević, 2025). Instead of people deciding what to share, it turns out that their data decides about them – through decisions made somewhere in the system, without clear explanation (Mladenov & Stojšić Dabetić, 2021; Stojšić Dabetić et al., 2025; Zuboff, 2019).

This creates an imbalance of power. The state, especially the police and security services, has an increasing amount of information at its disposal, and the individual has fewer and fewer ways to check what is being said about him. The system outputs a number, grade, "high risk" label, or a recommendation on how to proceed. On paper – perfectly organized: reports, graphs, statistics. In practice, no one can say with certainty whether this data is correct, outdated, taken out of context or simply entered incorrectly (Citron & Pasquale, 2014).

Once some data enters the system, it begins to "live its own life". It can affect who will be stopped more often, who will wait longer at the border, whose event will be declared risky or who will end up on a list. If the information is wrong, the path to correction is long, complicated and often without a clear outcome. The biggest problem is that the citizen often does not even know that there is something that should be corrected – he only sees the consequences, but does not see the source.

Even more insidious is that the line between justified data collection and invasion of privacy is gradually shifting. First, some measure is introduced "only in exceptional situations". After a couple of years, it becomes a routine, because it turns out to be "useful". What is the exception today becomes the new norm tomorrow. Today something is justified by the fight against the most serious crimes, tomorrow the same mechanism will be extended to less serious situations without much fuss.

Thus, little by little, control moves from citizens to institutions, without most people even noticing. We get used to cameras "for security", to

saving location data "just in case", to automatic analysis of communication "because that's what practice dictates". Every single step sounds reasonable. But when all these steps are added up, we end up with a society where constant surveillance has become the default, not the exception.

That is why the relationship between efficiency and the right to privacy cannot be reduced to the question of "does the system work properly". It is not only a technical matter, but above all a political and social question: how much we as a community are willing to give states "in sight" in return for a sense of security. The police and other services really need technology, without it it is difficult to work today. But at the same time, people must clearly know how far this technology can go – what data is collected, for what purpose, how long it is stored, who can access it and whether there is even a possibility to delete or correct something. If there are no concrete answers to these questions, the appeal to "efficiency" remains half–hearted and at some point begins to sound like an excuse (Sandhu & Fussey, 2021).

A democratic society is not only recognized by how quickly it responds to an incident or threat, but also by how it treats those over whom it has power. It is not enough to say "we work according to the law" if citizens do not have an insight into how that law is applied in practice. If the conversation about digital surveillance is reduced to technical terms and general phrases about "security reasons", the risk is to enter, little by little, a state in which surveillance is constantly present, but rarely visible. It is a field where mistakes and abuses are difficult to notice, and even more difficult to correct. This is exactly why it is important to talk about these things clearly and in time, while there is still room to set rules, instead of justifying decisions that have already been made afterwards.

CONCLUSION

When the digitization of police work is not looked at with sufficient attention, without delving into the essence of the process. superficially, from afar, it is easy to accept the story that it is about something completely natural: technology advances, so institutions are "modernized" to keep up with the times. However, as soon as you get a little closer, the picture becomes more complex. Something is not introduced into the system just because it is new or popular, but because that "something" increases the efficiency of the system. When we talk about digital tools, they are desirable in the system because they allow the expansion of

institutional power in a new, more efficient way, which was not feasible before.

On the example of predictive models, automated risk assessments and reliance on various digital traces, it can be seen that a new surveillance structure is gradually being established, which does not function through classic, visible control mechanisms, but through technological procedures integrated into the regular work of security authorities. The problem is that these tools are introduced and developed much faster than the corresponding mechanisms for monitoring their use are developed, which is to some extent expected: a certain technical solution is introduced first, while the issue of its limitations and control is opened only afterwards. In everyday police practice, it does not look spectacular or dramatic – the law does not change overnight, no decisions are made that attract special attention from the public. Instead, a new function is introduced into the software system, two databases are connected for "more efficient work", another risk assessment criterion is added, the set of parameters that the system takes into account is expanded. Everything is presented as a technical improvement, so such changes rarely become the subject of serious public discussion. Classic, gross abuses of authority are relatively easy to spot, they are reported by the media, it is possible to initiate proceedings and determine responsibility. The situation is much more complex when the decision is formally correct, but it is not possible to clearly reconstruct how it was reached. In those cases, the decision exists, produces very specific consequences for a certain individual, but the path from the initial data to the final decision is "closed" within the system and practically inaccessible to external verification. In this way, space is opened for the system, step by step, to start functioning in a way that is contrary to the interests of the citizens, while maintaining the formal explanation that everything was done for their safety.

In the introduction to the paper, the question was asked whether the fear of technological backwardness is really the main reason why AI tools are so quickly introduced in police work, i.e. whether the key motive is the fear that "our" police will lag behind "theirs". Based on what has been discussed here, such an explanation does not seem to be the most convincing. The point of view that digital systems, which are introduced under the pretext of efficiency and modernization, actually provide institutions with the opportunity to expand supervision, to standardize and mold assessments, and to reduce the visibility of their own decisions – both for citizens and for part of internal control – seems much more realistic. This, of course, does not mean that every single use of technology is

necessarily abuse, but it means that one cannot uncritically accept the thesis that "greater efficiency" through automation is a sufficient reason for the introduction of new digital solutions. Behind that word – efficiency – something else is often hidden: shifting the center of gravity of power even more to the side of the institutions, while at the same time reducing the space in which the individual can understand, question or challenge the decision that concerns him.

The concept of algorithmic risk further complicates this relationship, because it creates the impression that it brings order and objectivity to the field of security decision–making: decisions are presented through numbers, percentages, models, risk categorizations, so at first glance they seem orderly, "clean" and neutral. However, the problem arises the moment it turns out that the decision is fundamentally based on a model whose operation no one can clearly explain – neither those who use the system, nor those who should supervise its implementation, nor those to whom the decisions refer. At that moment, one of the basic elements of legal security is lost, which is the possibility to understand the decision, to follow the path from the initial data to the final result and, if there is a reason, to question and challenge it. If it is not known who exactly supervises the operation of the system, nor on the basis of which criteria it is adjusted, nor who specifically bears responsibility when the model "wrongs", then it is no longer a question of the technical issue of the functioning of the software, but of the issue of distribution of power between the state and citizens – about how much space is left for the freedom and autonomy of the individual in relation to decisions that are formally conducted as decisions of an institution, but in fact depend on the work of the algorithm.

Because of all this, the digitization of police work should not be seen as a natural, self–evident process of modernization, which "must happen" and which, supposedly, will automatically lead to better work of the institutions. This process must not be left to itself, but requires clearly defined boundaries, rules and mechanisms of public supervision. In addition, it is necessary to constantly monitor its implementation – to periodically check how specific tools are used, in which situations, with what consequences for citizens' rights and the way decisions are made. If these issues are pushed aside or approached formally, without a real will to reconsider things, the risk is to get a system that makes decisions quickly and behind closed doors: from the outside it will seem like work is more efficient, but the responsibility for the consequences of those decisions will become more and more nebulous. In such an environment, technology can

work impressively, while the standards of democracy, control and protection of the individual will be visibly weakened at the same time.

REFERENCES

1. Barocas, S., & Selbst, A. D. (2016). Big Data's disparate impact. *104 California Law Review 671*. DOI:10.2139/ssrn.2477899
2. Bayerl, P. S., Akhgar, B., Raven, A., Gibson, H., & Day, T. (2022). Future challenges and requirements for open source intelligence in law enforcement investigations: Results from a horizon scanning exercise. *European Law Enforcement Research Bulletin, 22*(6). Downloaded 2026, June 2 from https://shura.shu.ac.uk/30775/9/Bayerl-FutureChallengesAndRequirements%28VoR%29.pdf
3. Brayne, S. (2020). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.
4. Brayne, S., & Christin, A. (2021). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. *Social problems*, *68*(3), 608–624. DOI:10.1093/socpro/spaa004
5. Bukazić, D. (2026). The discretionary powers of public enforcement officers and their limits. *Kultura polisa, 23*(1), 155–167. DOI:10.51738/kpolisa.2026.1r.d
6. Citron, D. K., & Pasquale, F. A. (2014). *The scored society: Due process for automated predictions. Washington Law Review, 89*, 1–33. U of Maryland Legal Studies Research Paper No. 2014–8. Downloaded 2026, June 2 from https://ssrn.com/abstract=2376209
7. Domazet, S., Marković, D. M., & Skakavac, T. (2024). Privacy under threat – The intersection of IoT and mass surveilance. *Pravo – teorija i praksa*, *41*(3), 109–124. DOI: 10.5937/ptp2403109D
8. Eubanks, V. (2018). *Automating Inequality: How high–tech tools profile, police, and punish the poor*. St. Martin's Press.
9. European Union Agency for Fundamental Rights [FRA]. (2021). *Getting the future right – Artificial intelligence and fundamental rights*. Publications Office of the European Union. Downloaded 2026, June 1 from https://fra.europa.eu/sites/default/files/fra_uploads/fra–2021–artificial–intelligence–summary_en.pdf
10. Ferguson, A. G. (2017). Policing predictive policing. *Washington University Law Review, 94*(5). Downloaded 2026, June 1 from https://ssrn.com/abstract=2765525

11. Joh, Elizabeth E., The New surveillance discretion: Automated suspicion, Big Data, and policing. *Harvard Law & Policy Review*, 2015 (forthcoming). UC Davis Legal Studies Research Paper No. 473. Downloaded 2026, June 1 from https://ssrn.com/abstract=2680266
12. Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big Data & Society*, *1*(1). DOI:10.1177/2053951714528481
13. Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review, 165*(3), Forthcoming Fordham Law Legal Studies Research Paper No. 2765268. Downloaded 2026, June 1 from https://ssrn.com/abstract=2765268
14. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19. DOI:10.1111/j.1740–9713.2016.00960.x
15. Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.
16. Marković, D.M. (2021). The role and importance of border police in detecting forged documents. *Nauka i društvo*, 7(1), 202–217. DOI: 10.5281/zenodo.5572518. UDC 351.746.1
17. Marković, D. M., & Marković, D. (2025). Cybercrime and law – managing challenges and prospects in the digital age. *Pravo – teorija i praksa*, *42*(2), 49–61. DOI:10.5937/ptp2502049M
18. Marković, D. M., & Zirojević, M. (2025). *Justice in the digital society: Legal frameworks for addressing ethical challenges in cybersecurity.* In: Počuča, M. (Ed.), XXII International Scientific Conference "Legal Days – Prof. Slavko Carić: Law and Justice". Novi Sad: Faculty of Law for Commerce and Judiciary in Novi Sad (Vol. 2, pp. 546–548). DOI:10.5937/pdsc25546m
19. Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, *42*(12), 1031–1039. DOI:10.1080/01900692.2019.1575664
20. Mladenov, M., & Stojšić Dabetić, J. (2021). Ažuriranje „prava da se bude zaboravljen" kao principa zaštite podataka u Evropskoj uniji [An update on the right to be forgotten as a principle of personal data protection in European union]. *Kultura polisa*, *18*(44), 99–109, DOI: 10.51738/Kpolisa2021.18.lr.2.04
21. Oswald, M., Grace, J., Urwin, S., & Barnes, G. (2018). Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'experimental' proportionality. *Information & Communications Technology Law*. Advance online publication.

DOI:10.2139/ssrn.3029345
22. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press. Downloaded 2026, June 2 from https://raley.english.ucsb.edu/wp–content/Engl800/Pasquale–blackbox.pdf
23. Richards, N. M., & King, J. H. (2013). Three paradoxes of big data. *66 Stanford Law Review* Online 41 (2013). Downloaded 2026, June 3 from https://ssrn.com/abstract=2325537
24. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions. *New York University Law Review, 94*(1), 15–55.
25. Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society*, *31*(1), 66–81. DOI:10.1080/10439463.2020.1803315
26. Stojsic Dabetic, J., Mirković, P., & Aleksić Oliveira, N. (2025). The emergence of digital identity as a new legal concept. *Pravo – teorija i praksa*, *42*(3), 21–34. DOI:10.5937/ptp2503021M
27. Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance, 12*(4), 505–523. DOI:10.1111/rego.12158
28. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.