UDC 321:34(497.11)"20"
DOI: 10.5937/spm95-61349
Original research article

Српска политичка мисао
(Serbian Political Thought)
No 1/2026.
Vol. 95
pp. 1-20

Marina Matić Bošković[*]

Institute of Criminological and Sociological Research, Belgrade

Jelena Kostić[**]

Institute of Comparative Law, Belgrade

JUSTICE UNDER SIEGE: CYBER THREATS AND THE MALICIOUS USE OF AI IN THE JUDICIARY[***]

Abstract

As judicial systems increasingly integrate digital technologies and artificial intelligence (AI), they become more efficient yet highly vulnerable to cyber threats and AI-driven manipulations. This paper examines the growing risks of cyberattacks targeting the judiciary, as well as the malicious use of AI in legal proceedings, both of which pose severe threats to judicial integrity, fairness, public trust, and the broader judicial policy framework. The article explores key cybersecurity vulnerabilities, including ransomware attacks on court databases, AI-powered deepfake evidence manipulation, algorithmic bias in automated decision-making, and AI-driven misinformation campaigns. The weaponisation of AI in

[*] Email: m.m.boskovic@roldevelopmentlab.com; ORCID 0000-0003-1359-0276
[**] Email: j.kostic@iup.rs; ORCID 0000-0001-6032-3045
[***] This paper is a result of research supported by the Ministry of Science, Technological Development and Innovations through Agreement on the realization and financing of scientific research work SRO in 2025 by Institute of Criminological and Sociological Research (contract number 451-03-136/2025-03/200039) and within the project "Adapting the Legal Framework to Social and Technological Changes with a Special Focus on Artificial Intelligence," carried out in 2025 by the Institute of Comparative Law with financial support from the Ministry of Science, Technological Development and Innovation (contract number 451-03-136/2025-03/200049).

legal contexts, through fraudulent case manipulation, automated hacking, and digital surveillance, raises profound concerns about due process, judicial independence, and access to justice. These challenges directly affect judicial policy, as they demand new safeguards and adaptive governance models capable of preserving impartiality and accountability in an increasingly digital justice environment. By analysing real-world incidents and international regulatory approaches, this paper outlines strategies for strengthening judicial cybersecurity and safeguarding AI applications. Recommendations include enhanced digital forensics, AI transparency requirements, independent auditing mechanisms, and cross-border legal cooperation to combat cyber threats and AI misuse in the judiciary. Crucially, these measures must be integrated into judicial policy at national and supranational levels to ensure the resilience of reforms. As courts continue to embrace digital transformation, a proactive and resilient security framework is essential to preserve the rule of law in an era of evolving cyber threats and AI-driven legal manipulations. This study underscores the urgent need for global legal and technological safeguards to protect justice systems from digital exploitation and AI-enhanced cyberattacks.

Keywords: cybersecurity, cyber threats, judicial policy, AI manipulation, digital forensics

INTRODUCTION

In recent years, the judiciary has become increasingly reliant on digital technologies to improve the delivery of justice. Innovations such as electronic filing systems, virtual hearings, AI-assisted legal research, and predictive analytics have promised greater efficiency, transparency, and accessibility in judicial processes (Matić Bošković 2024a, 482). These advancements have been accelerated by global trends, including the COVID-19 pandemic, which necessitated rapid digital transitions in court systems worldwide (Matić Bošković and Nenadić 2021, 265). However, this transformation has also exposed courts to a range of cyber and AI-related vulnerabilities that threaten the very principles upon which modern justice is built.

Courts and judicial authorities now face dual technological challenges: the escalating sophistication of cyber threats and the

emerging misuse of artificial intelligence. Cybercriminals and politically motivated actors increasingly target courts with ransomware, phishing campaigns, and denial-of-service attacks, often paralyzing judicial services and jeopardizing sensitive legal data (Brown 2024). At the same time, the misuse of AI, through deepfake evidence, biased algorithms, and misinformation campaigns, raises serious ethical, procedural, and legal concerns (Citron and Chesney 2019, 147; Toskić Cvetinović and Tošić, 2022, 333). Recognising these risks, some European countries have already started adapting their legal frameworks. In Denmark, for example, the government prepared amendments to the copyright law aimed at preventing the creation and dissemination of AI-generated deepfakes (Bryant 2025). This initiative, believed to be the first of its kind in Europe, seeks to strengthen the protection of individuals' rights over their identity, including their image and voice, and serves as a model of how targeted legislative innovation can safeguard judicial integrity in the face of rapidly evolving technological threats (World Economic Forum 2025).

Unlike other public institutions, the judiciary plays a unique constitutional role: it must uphold impartiality, protect individual rights, and serve as a final arbiter in legal conflicts. Any disruption to this function, whether through compromised data, manipulated evidence, or undermined trust, has far-reaching implications not only for individual cases but also for the integrity of democratic governance. Yet, despite these risks, judicial systems have often been slower than other sectors to implement comprehensive cybersecurity strategies or critically assess the use of AI tools within their proceedings (Yoon 2023, 358). Addressing these challenges requires not only technological responses but also the development of judicial policies that integrate cybersecurity and AI governance into broader justice sector reforms. By embedding these policies into national judicial strategies and aligning them with EU rule of law standards, courts can ensure that digital innovation reinforces, rather than undermines, judicial independence and accountability.

This article critically examines the intersection of digital technology, cybersecurity, and AI within the justice sector. It addresses the growing exposure of courts to cyberattacks and the weaponization of artificial intelligence, both of which can compromise judicial independence, fairness, and public trust. Drawing on global cybersecurity intelligence, regulatory frameworks, and real-world incidents, the paper aims to shed light on the evolving threat landscape and propose strategic

solutions. In doing so, it highlights the need for a robust, rights-based, and technologically informed approach to safeguarding justice in the digital age.

CYBERSECURITY VULNERABILITIES IN JUDICIAL SYSTEMS

Judicial systems handle highly sensitive and mission-critical information, rendering them frequent targets for cybercriminals, state-sponsored entities, and ideological hacktivist groups. One of the most severe threats comes from ransomware attacks on court databases, which have, in some instances, halted court operations and resulted in data loss and disruptions to public services. While global examples such as the 2020 ransomware attack on the Texas judiciary (Bleiberg 2020) and the 2021 breach of South Africa's Department of Justice has received broad attention (Pieterse 2021, 3), recent high-profile attacks in Europe underscore the regional relevance and urgency of this issue.

One of the most disruptive attacks occurred in the Netherlands in 2023, when the digital court platform used for remote hearings and document filing was brought down by a distributed denial-of-service (DDoS) attack, delaying hearings and obstructing access to legal filings (NL Times 2023). The attack highlighted the judiciary's growing dependence on continuous online availability and the fragility of national infrastructure under targeted pressure.

Ransomware attacks have increasingly targeted justice sector institutions, with notable examples illustrating the severe operational and data security risks they pose. In January 2022, the French Ministry of Justice fell victim to the LockBit ransomware group, which claimed responsibility for a cyberattack that exposed internal documents. The attackers published a selection of files on the dark web and threatened further leaks unless a ransom was paid. While the Ministry claimed that critical judicial services were not affected, the incident highlighted weaknesses in protecting governmental legal data and prompted reviews of cybersecurity protocols (Kovacs 2022). The same year, in March 2022, the Los Angeles County Superior Court experienced a significant ransomware attack that disrupted access to online services and caused delays in court operations. Although the court did not confirm whether sensitive case data was exfiltrated, internal communications

acknowledged the compromise of IT systems and emphasized efforts to restore services securely (Los Angeles County Superior Court 2024).

These cases reveal patterns of vulnerability that are exacerbated by the continued use of outdated IT infrastructure in many courts, which often lack necessary security patches and updates. A 2023 report from the European Union Agency for Cybersecurity (ENISA) found that phishing and credential theft remained among the top three attack vectors across judicial systems in member states. Judicial personnel, including clerks and judges, frequently receive minimal training in digital hygiene, making them susceptible to deceptive links, malicious attachments, and social engineering tactics.

Additionally, cascading risks from interconnected systems remain a critical concern. The 2025 cyberattacks on the Legal Aid Agency in the UK temporarily compromised coordination with the Courts Service, delaying hearings for vulnerable populations reliant on public legal support (Mitigo 2025). The breach affected approximately 2.1 million records, including highly sensitive personal data such as criminal histories, national insurance numbers, and financial details. This example illustrates how a breach in one part of the justice ecosystem can disrupt broader judicial processes. Recent cases also reveal how breaches in one part of the digital justice chain can have cascading effects (Check Point Research 2023, 25).

In parallel, judicial personnel frequently do not receive adequate cybersecurity training, thereby increasing susceptibility to phishing attacks and credential theft (Dixon 2022, 38). Court systems often lag in providing consistent, up-to-date cybersecurity training to judges, administrators, and staff, particularly on phishing risks and credential protection. Moreover, cybersecurity professional emphasizes that, across sectors, employees remain a key vulnerability (University of Chicago 2025).

The vulnerabilities extend beyond technical infrastructure. The rapid transition to virtual hearings and electronic filings has increased dependence on third-party vendors and cloud-based solutions. Courts have grown reliant on external digital platforms for managing case files, conducting remote processing, and maintaining digital archives. This reliance introduces critical risks related to supply-chain vulnerabilities, software misconfigurations, and insufficient contractual safeguards for data protection (Moyer 2021). Inadequate vetting of service providers and

fragmented procurement practices exacerbate these threats, especially in lower-capacity judicial systems.

These developments underscore the urgent need to integrate cybersecurity as a core element of judicial reform agendas. In addition to infrastructure upgrades and technical safeguards, building a cybersecurity culture across the judiciary through awareness, training, and regular stress-testing is essential to reducing systemic risk.

THE WEAPONISATION OF AI IN LEGAL CONTEXTS

The use of artificial intelligence in legal settings introduces another layer of complexity and risk that goes beyond traditional cybersecurity concerns. AI technologies, ranging from large language models to facial recognition and deepfake generators, can be weaponised in ways that undermine judicial processes, distort evidence, and compromise the principles of fairness and impartiality.

Deepfake technology, for instance, enables the generation of synthetic audiovisual content that can be misused to fabricate evidence, thereby misleading judges, juries, and even opposing counsel (Citron and Chesney 2019, 150). Chesney and Citron warn that deepfakes represent a 'new disinformation war' that could corrupt the evidentiary process by making it difficult to determine what is authentic. For example, fabricated video recordings of confessions, threats, or illicit activities could be submitted as digital evidence, especially in systems without robust forensic verification protocols.

Algorithmic decision-making tools, including risk assessment instruments used for pre-trial release or sentencing, often rely on historical data that reflect entrenched social and racial biases (Matić Bošković 2024a, 486). As demonstrated in the ProPublica investigation, the COMPAS algorithm, widely used in US courts, disproportionately labels Afro-Americans defendants as high-risk compared to white defendants with similar records (Angwin *et al*. 2016). Similar concerns have been echoed in European jurisdictions where predictive policing and AI-assisted legal analytics are being introduced without sufficient transparency or regulatory oversight (Sartor 2020, 32).

Generative AI models also introduce new risks through the automated creation of fraudulent or malicious legal documents. There have already been reported cases where generative AI tools like ChatGPT were used to draft entire legal pleadings, including fabricated case

citations. In 2025, the UK's High Court justice issued a warning after multiple lawyers cited entirely fictitious legal cases generated by AI in their briefs (Lawless 2025). In one £90 million lawsuit, a lawyer referenced 18 cases that did not exist. In another housing dispute, five phantom precedents were used. Chief Justice cautioned that such behaviour "has serious implications for the administration of justice and public confidence" in the legal system.

Facial recognition technologies, increasingly used in court-adjacent law enforcement processes, also raise serious legal and ethical concerns. Multiple studies have demonstrated higher error rates for non-white individuals, potentially leading to wrongful accusations or mistaken identity in courtroom proceedings (Garvie *et al*. 2016; Buolamwini and Gebru 2018, 1). In legal settings where such evidence is admitted without rigorous scrutiny, the results may be miscarriages of justice grounded in flawed AI outputs.

The integration of artificial intelligence into judicial processes poses significant risks of "techno-capture" and authoritarian oversight. As noted by the UN Special Rapporteur on the independence of judges and lawyers (A/80/169) from July 2025, influence over AI tools is likely to become a focal point for executive and legislative actors seeking to curtail judicial independence. Judges from multiple jurisdictions have expressed concern that AI may be deployed not as a neutral support tool, but as an instrument to standardize decisions and align them with political or institutional priorities (UN Rapporteur 2025, 18). The example of China illustrates this risk most vividly; courts there have incorporated AI systems to monitor and evaluate judicial reasoning, with the stated aim of promoting consistency, but in practice, these tools incentivize conformity with the model's outputs, reduce space for judicial discretion, and open the door to political oversight. Such practices risk undermining judicial autonomy and transforming AI into a tool for reinforcing state power, rather than safeguarding impartial justice (Stern *et al*. 2021, 518).

Taken together, these developments raise serious concerns about due process, judicial independence, and access to justice. The opacity of many AI systems, especially proprietary models that are not open to audit, means that litigants, defence counsel, and even judges may be unaware of how decisions are being shaped. This 'black box justice' problem undermines transparency and the right to a fair trial (Garret and Rudin 2023, 561).

IMPACTS ON JUDICIAL INTEGRITY AND THE RULE OF LAW

The cybersecurity vulnerabilities and AI manipulation discussed in the preceding sections converge to undermine the core principles of judicial functioning. These technological risks, while often viewed through a technical lens, have profound normative consequences for legal certainty, procedural fairness, public trust in the rule of law, and judicial legitimacy.

The increasing frequency and severity of cyberattacks on judicial infrastructure can delay or derail legal proceedings, leading to the erosion of due process rights. For instance, ransomware incidents that lock court databases or corrupt evidence files may prevent timely hearings, disrupt the chain of custody, and impair evidentiary integrity (Dixon 2018, 37). These digital disruptions disproportionately affect vulnerable populations with limited access to alternative legal resources, thereby exacerbating existing inequalities in the justice system (Quintanilla *et al*. 2023, 250).

Simultaneously, the misuse of AI tools introduces new vectors for undermining judicial integrity. Deepfake technology can fabricate persuasive but false evidence, while generative AI can automate the production of fraudulent filings or synthetic legal arguments designed to overwhelm the judiciary (Citron and Chesney 2019, 149). When manipulated audio-visual materials are indistinguishable from authentic recordings, courts may struggle to verify the credibility of key evidence or witness statements, thereby eroding confidence in the fact-finding process and weakening the perceived impartiality of justice. Such falsifications not only risk wrongful convictions or acquittals but also undermine public trust in the judiciary's ability to distinguish truth from fabrication in an increasingly digital environment. The integrity of judicial reasoning depends on transparency, verifiability, and accountability, all of which are threatened when AI systems are used to obscure provenance or manipulate evidentiary foundations.

These developments challenge fundamental principles such as judicial independence, equality before the law, and the right to a fair trial. Surveillance-enabled malware and digital profiling tools can be used to monitor or influence judicial decision-makers, undermining impartiality and creating chilling effects, particularly in politically sensitive or high-profile cases (Liger and Gutheil 2023, 25). Research shows that when

courts become vulnerable to technological manipulation, public trust in their impartiality and competence declines significantly (Angwin *et al*. 2016).

Furthermore, the lack of regulatory oversight for AI-based legal tools heightens the risk of automated discrimination. Risk assessment algorithms and sentencing recommendation systems, if unregulated and opaque, can perpetuate historical biases and reinforce social disparities (Angwin *et al*. 2016). Without mandatory transparency and auditing requirements, these technologies may invisibly distort judicial outcomes, calling into question the objectivity of decisions and the fairness of proceedings.

To uphold the rule of law in an increasingly digital legal ecosystem, judicial institutions must proactively embed safeguards for technological integrity. This includes not only upgrading IT infrastructure and enhancing cybersecurity literacy but also establishing ethical and legal frameworks for the accountable use of AI. Institutional resilience in the digital age depends on the judiciary's capacity to maintain transparency, independence, and equitable access to justice despite evolving technological threats.

INTERNATIONAL AND REGULATORY RESPONSES

The international community has begun to recognise the profound implications of artificial intelligence on cyber threats for judicial integrity and the rule of law. In response, a series of legal and regulatory initiatives have been launched at national, regional, and global levels, each addressing different dimensions of the challenge. Efforts to address these challenges vary across jurisdictions.

At the European Union level, the 2024 Artificial Intelligence Act marks the EU's first comprehensive regulatory framework for AI, introducing a graduated, risk-based approach to governing the development and use of artificial intelligence systems (Regulation 2024/1689). The Act explicitly classifies certain uses of AI in the justice sector as high-risk applications, including systems for predictive justice, biometric identification, and evidence analysis (Matić Bošković 2024b, 115). For these uses, the Regulation requires strict conformity assessments, transparency obligations, and ongoing monitoring to mitigate bias and ensure accountability. The inclusion of the judiciary in the high-risk category highlights the EU's recognition of the sensitivity

of court proceedings and the need for safeguards to preserve both procedural fairness and fundamental rights.

In the United States, the National Institute of Standards and Technology (NIST) has introduced its AI Risk Management Framework (2023), which provides a set of voluntary but widely endorsed standards for managing risks related to AI deployment (NIST 2023). Although not legally binding, the framework is already shaping practice across public institutions, including courts, by encouraging systematic risk identification, mitigation strategies, and testing protocols before AI tools are integrated into adjudication or case management systems. By embedding cybersecurity preparedness into judicial contexts, the NIST guidelines aim to prevent vulnerabilities such as data manipulation or biased decision-making.

A significant development in Europe was the adoption of the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, in May 2024 (CEPEJ 2018; CoE 2024). These instruments represent the first legally binding international treaty on AI, establishing legal obligations for states to ensure that AI systems respect human rights, democratic values, and rule of law standards throughout their life cycle. The Convention introduces safeguards for transparency, accountability, and oversight of AI systems, and it extends explicitly to judicial institutions, thereby recognising courts as a sensitive domain where misuse of AI can have systemic consequences for democracy.

At the global level, the United Nations Office on Drugs and Crime (UNODC) has taken a complementary approach through the Global Judicial Integrity Network (Contini 2019). While not producing binding rules, it has initiated discussion on ethical guidance for the use of AI in courts. These discussions emphasise the risks of undermining judicial independence, the dangers of algorithmic bias, and the need for clear ethical frameworks to guide judges when confronted with AI-generated evidence or digital manipulation, such as deepfakes. The UNODS's soft-law approach complements binding instruments by promoting shared values and peer learning.

Finally, national responses such as Denmark's 2025 amendments to its copyright law illustrate how states are moving to adapt traditional legal instruments to technological realties. While narrowly focused, this initiative highlights how domestic legal systems can pioneer approaches that may later influence broader regional or international standards.

Nonetheless, existing responses often remain fragmented and lack comprehensive coordination. There is a growing need for a cohesive global strategy that integrates legal reform, digital forensics, AI auditability, and cross-border legal cooperation. This should include establishing clear standards for explainability and oversight of AI tools, deploying advanced capabilities for detecting deepfakes, and enhancing resilience through continuous training of judicial personnel.

STRATEGIES FOR RESILIENCE AND SAFEGUARDS

Addressing cybersecurity threats and the misuse of artificial intelligence in the judicial system requires a multi-layered and integrated strategy that goes beyond technical fixes and embedded resilience at structural, institutional, and cultural levels. Courts must invest in strengthening their digital infrastructure, implementing mandatory cybersecurity audits, adopting zero-trust architectures, and ensuring systematic cyber training for judicial staff (ENISA 2023). Regular audits are crucial to detect vulnerabilities before they are exploited, while targeted training addresses the persistent risk of human error, such as phishing and weak credential use, which remains one of the most common entry points for attackers.

In parallel, AI governance must prioritise transparency and accountability. This entails explainability obligations for AI tools used in judicial contexts, clear documentation of their functioning, and independent oversight mechanisms to prevent bias or "black box" decision-making (Sartor 2020, 24). Such safeguards are indispensable to uphold fairness, protect fundamental rights, and maintain trust in the digitalization of justice.

Good practices from European and international courts illustrate the importance of resilience planning. When the European Court of Human Rights suffered a cyber-attack coinciding with the *Demirtaş v. Turkey (No. 2)* judgement (Application no. 14305/17, judgement of 22 December 2020) (European Union 2021), contingency protocols under the Rules of Court enabled secured electronic filing (European Court of Human Rights 2018), and alternative submission channels, safeguarding access to justice. Similarly, the International Criminal Court, after detecting suspicious activity in its systems, collaborated with Dutch authorities to strengthen its cybersecurity framework and accelerate its migration to cloud-based infrastructure (Voelkerrechtsblog

2025). These cases highlight that effective judicial cybersecurity depends not only on prevention but also on institutional partnerships and adaptive modernization.

Building digital forensics capacities is equally essential. While the proliferation of manipulated evidence, particularly deepfakes, continues to grow, judicial systems must be able to authenticate the integrity of digital material (Venema and Geradts 2020, 15). Specialized forensic units should be equipped with advanced tools to detect digital tampering, verify metadata, and maintain the chain of custody of electronic evidence. Embedding these capacities directly into prosecutorial and judicial workflows will enhance both evidentiary reliability and the persuasiveness of evidence in court (Sandoval *et al*. 2024, 7).

Finally, resilience cannot be achieved in isolation. Cross-border cooperation must be promoted through harmonization of cybercrime laws, mutual legal assistance frameworks, and real-time information sharing mechanisms (EUROJUST 2020, 4). Together, these strategies provide a robust foundation for securing the judiciary in a digital era.

Justice systems can no longer treat cybersecurity and AI governance as peripheral issues. They must be embedded in judicial modernization strategies from the outset. Building a resilient justice system in the digital age requires not only technological upgrades but also legal, institutional, and cultural changes. Public trust in courts hinges on the integrity of the processes and the authenticity of decisions. Without credible digital safeguards, judicial digitization risks becoming a liability rather than a reform. Conversely, by embracing secure and ethical innovation, judicial systems can reinforce their legitimacy and better serve societies in an era of rapid change.

CONCLUSIONS

The integration of digital technologies and artificial intelligence (AI) into judicial systems is both inevitable and transformative. From streamlining case management and improving access to justice to enabling remote hearings and predictive analytics, digital tools hold significant promise. However, this transformation comes with a paradoxical cost; the very systems designed to enhance efficiency and transparency can also become vectors for unprecedented risks to judicial integrity, due process, and the public's trust in the rule of law.

This article has shown that cyberattacks targeting the judiciary are no longer hypothetical or isolated incidents. They have disrupted courts across continents, compromised sensitive data, and exposed critical gaps in infrastructure, training, and digital preparedness. Meanwhile, the malicious use of AI, from deepfakes and algorithmic bias to disinformation campaigns, has introduced new ways to distort evidence, harass judicial actors, and manipulate the outcomes or legitimacy of legal proceedings.

The consequences of these threats are far-reaching. As the judiciary serves as the last bulwark of constitutional rights and democratic accountability, its vulnerability to cybercrime and AI misuse threatens not only individuals' access to justice but also the structural integrity of democratic governance itself. When judicial institutions are digitally compromised, their capacity to deliver impartial, consistent, and transparent decisions is severely impaired.

To address these challenges, judicial systems must adopt a proactive, system-wide approach that combines cyber resilience, ethical AI governance, and comprehensive judicial policy reform. Judicial policy is the mechanism through which technological safeguards are embedded into the institutional fabric of the courts. It provides the framework for mandating regular cybersecurity audits, introducing zero-trust infrastructure, expanding digital forensics capacities, and regulating the admissibility of AI-generated evidence. By integrating these elements into judicial policy, courts can move beyond ad hoc technical fixes and create sustainable, legally grounded protection.

At the same time, no single jurisdiction can tackle these issues in isolation. The inherently transnational nature of cyber threats and AI misuse calls for coordinated judicial policies that align with global and regional frameworks. Emerging frameworks such as the EU's AI Act and initiatives by UNODC and the Council of Europe offer building blocks for a shared judicial policy environment, where innovation is encouraged but bound by transparency, accountability, and human rights safeguards.

Ultimately, the legitimacy of the judiciary in the digital era will depend on technology but also on the strength of judicial policies that govern its use. By embedding secure digital practices, ethical AI standards, and cross-border cooperation mechanisms into judicial policy, courts can ensure that technological innovation becomes a powerful enabler of justice rather than a source of vulnerability.

REFERENCES

Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner [Angwin *et al*.]. 2016. "Machine bias." *ProPublica*. Last Accessed on September 3, 2025. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bleiberg, Jake. 2020. "Texas High Courts Hit by Ransomware Attack, Refuse to Pay." *AP News*. Last Accessed on September 3, 2025. https://apnews.com/article/hacking-tx-state-wire-technology-us-news-courts-474453285863aebab0a2fe239f493548

Buolamwini, Joy, and Timnit Gebru. 2018. "*Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*." *Proceedings of Machine Learning Research* 81: 1–15. https://proceedings.mlr.press/v81/buolamwini18a.html

Brown, David. 2024. "State and Local Courts Struggle to Fight Increasing Cyberattacks." *State Court Report.* Last Accessed on September 3, 2025. https://statecourtreport.org/our-work/analysis-opinion/state-and-local-courts-struggle-fight-increasing-cyberattacks?utm_source=chatgpt.com

Bryant, Miranda. 2025. "Denmark to Tackle Deepfakes by Giving People Copyright to Their Own Features." *The Guardian*. Last Accessed on September 1, 2025. https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence

Check Point Research. 2023. "*Cyber Security Report.*" *Check Point Research.* Last Accessed on September 3, 2025. https://www.checkpoint.com/resources/report-4fd2/report-cyber-security-report-2023

Check Point Research. 2025. "*Cyber Security Report.*" *Check Point Research.* Last Accessed on September 3, 2025. https://www.checkpoint.com/security-report/

Citron, K. Daniel, and Robert Chesney. 2019. "Deepfakes and the new disinformation war." *Foreign Affairs* 98 (1): 147–155.

Contini, Francesco. 2019."Artificial Intelligence: A New Trojan Horse for Undue Influence on Judiciaries?" *United Nations Office on Drugs and Crime.* Last Accessed on September 3, 2025. https://www.unodc.org/dohadeclaration/en/news/2019/06/artificial-intelligence_-a-new-trojan-horse-for-undue-influence-on-judiciaries.html

Council of Europe, European Commission for the Efficiency of Justice [CEPEJ]. 2018. *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. Adopted at

the 31st plenary meeting of CEPEJ, December 3–4. https://www.coe.int/en/web/artificial-intelligence/cepej-ai-ethics-charter

Council of Europe [CoE]. 2024. *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. CETS No. 225. Adopted in Vilnius, September 5. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Dixon, B. Herbert. 2018. "Cyberattacks on Courts and Other Government Institutions." *Judges' journal* 57 (3): 37 – 39.

Dixon, B. Herbert. 2022. "Response to 'The Court has been Hacked!'." *Judges' journal* 61 (1): 37–39.

ENISA. 2023. *ENISA threat landscape*. European Union Agency for Cybersecurity. Last Accessed on September 3, 2025. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

EUROJUST. 2020. "Overview Report – Challenges and best practice from Eurojust's casework in the area of cybercrime." *Criminal justice across borders.* DOI: 10.2812/691335

European Union. 2021. "EU Statement on the Cyberattack on the Website of the European Court of Human Rights." January 13, 2021. Brussels. Last Accessed on September 3, 2025. https://www.eeas.europa.eu/delegations/council-europe/eu-statement-cyberattack-website-european-court-human-rights_en

European Court of Human Rights. 2018. "*Practice Direction: Secured Electronic Filing*." *Strasbourg: European Court of Human Rights*. Last Accessed on September 3, 2025. https://www.echr.coe.int/documents/d/echr/PD_electronic_filing_ENG

Garret, L. Brandon, and Cynthia Rudin, 2023. "The right to a glass box: Rethinking the use of artificial intelligence in criminal justice." *Cornell Law Review* 109 (3): 561–600.

Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle [Garvie *et al.*]. 2016. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/

Kovacs, Eduard. 2022. "French Ministry of Justice Targeted in Ransomware Attack." *SecurityWeek.* Last Accessed on September 3, 2025. https://www.securityweek.com/french-ministry-justice-targeted-ransomware-attack

Lawless, Jill. 2025. "UK Judge Warns of Risk to Justice After Lawyers Cited Fake AIGenerated Cases in Court." *Associated Press*. Last

Accessed on September 3, 2025. https://apnews.com/article/uk-courts-fake-ai-cases-46013a78d78dc869bdfd6b42579411cb

Liger, Quentin, and Mirja Gutheil. 2023. *The Use of Pegasus and Equivalent Surveillance Spyware.* Policy Department for Citizens' Rights and Constitutional Affairs. European Parliament

Los Angeles County Superior Court. 2024. "*Court Systems Return to Full Functionality (NR 07-29-2024)*." *Press release.* Last Accessed on September 3, 2025. https://www.lacourt.org/newsmedia/uploads/142024729163959NR07-29-2024-COURTSYSTEMSRETURNTOFULLFUNCTIONALITY(1).pdf

Matić Bošković, Marina. 2024a. "Impact of Artificial Intelligence on Practicing Judicial Profession." *Sociološki pregled* 58 (3): 481–499.

Matić Bošković, Marina. 2024b. "Implications of EU AI Regulation for Criminal Justice." *Regional Law Review* 5: 111–120.

Matić Bošković, Marina, and Svetlana Nenadić. 2021. "*Impact of COVID-19 Pandemic on Criminal Justice Systems Across Europe." EU and comparative law issues and challenges series (ECLIC)* 5: 263–290.

Mitigo. 2025. "Legal Aid Agency Breach – One Rule for Us, Another for You?" *The Law Society – Communities: Risk & Compliance*. Last Accessed on September 3, 2025. https://communities.lawsociety.org.uk/risk-and-compliance/legal-aid-agency-breach-one-rule-for-us-another-for-you/6003388.article

Moyer, Bruce. 2021. "Washington Watch – Sealed Filings in Federal Cases May Have Been Compromised." *Federal Bar Association Blog*. Last Accessed on September 3, 2025. https://www.fedbar.org/blog/washington-watch-sealed-filings-in-federal-cases-may-have-been-compromised/

National Institute of Standards and Technology [NIST]. 2023. *AI Risk Management Framework.* U.S. National Institute of Standards and Technology. Last Accessed on September 3, 2025. https://www.nist.gov/itl/ai-risk-management-framework

NL Times. "Dutch government websites struggling with cyberattacks possibly from Russian hackers." *NL Times*. Last Accessed on September 3, 2025. https://nltimes.nl/2023/05/04/dutch-government-websites-struggling-cyberattacks-possibly-russian-hackers?utm_source=chatgpt.com

Pieterse, Heloise. 2021. "The Cyber Threat Landscape in South Africa: A 10-Year Review." *The African Journal of Information and Communication* 28: 1–21.

Quintanilla, D. Victor, Kurt Hugenberg, Margaret Hagan, Amy Gonzales, Ryan Hutchings, and Nedim Yel [Quintanilla *et al*.]. 2023. "Digital Inequalities and Access to Justice: Dialling into Zoom Court Unrepresented." In: Engstrom David Freeman, (ed.). *Legal Tech and the Future of Civil Justice*. 225–250. Cambridge University Press.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

Sandoval, Maria-Paz, Maria de Almeida Vau, John Solaas, and Luano Rodrigues [Sandoval *et al*.]. 2024. "Threat of deepfakes to the criminal justice system: a systematic review." *Crime Science* 13 (41). DOI: 10.1186/s40163-024-00239-1

Sartor, Giovanni. 2020. *The ethics of artificial intelligence: Issues and initiatives*. European Parliament Research Service. Last Accessed on September 3, 2025. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)634452

Stern, E. Rachel, Benjamin Liebman, Margaret Roberts, and Alice Wang [Stern *et al*.]. 2021. "Automating Fairness? Artificial Intelligence in the Chinese Courts." *Columbia Journal of Transnational Law* 59: 515–553.

Toskić Cvetinović, Ana, and Milica Tošić, 2022. "Application of Artificial Intelligence in Judiciary – Perspectives and Challenges." In: Jelena Kostić, amd Marina Matić Bošković (eds.). *Digitalization in Penal Law and Judiciary*, 317–341. Belgrade: Institute of Comparative Law, Institute of Criminological and Sociological Research,

UN Rapporteur. 2025. *Report of the Special Rapporteur on the independence of judges and lawyers, Margaret Sattertwaite – Artificial intelligence in judicial systems: promises and pitfalls*. A/80/169. UN General Assembly.

United Nations Office on Drugs and Crime [UNODC]. 2022. *Ethical principles for the use of artificial intelligence in the judiciary.* United Nations Office on Drugs and Crime. Last Accessed on September 3, 2025. https://www.unodc.org/ji

University of Chicago. 2025. "New Study Reveals Gaps in Common Types of Cybersecurity Training." *Department of Computer Science*. Last Accessed on September 3, 2025. https://cs.uchicago.edu/news/new-study-reveals-gaps-in-common-types-of-cybersecurity-training/

Venema, E. Agnes, and Zeno J. Geradts. 2020. "Digital Forensics, Deepfakes, and the Legal Process." *The SciTech Lawyer* 18 (4): 14–23.

Voelkerrechtsblog. 2025. "International Courts and Tribunals under Cyber-Threat – What Responses to Attacks on International Courts and Tribunals?" Last Accessed on September 3, 2025. https://voelkerrechtsblog.org/international-courts-and-tribunals-under-cyber-threat/?utm_source=chatgpt.com

World Economic Forum. 2025. "Emerging Technologies – Deepfake legislation: Denmark moves to protect digital identity." July 30, 2025. Last Accessed on September 3, 2025. https://www.weforum.org/stories/2025/07/deepfake-legislation-denmark-digital-id/

Yoon, H. Albert. 2023. "Technological Challenges Facing the Judiciary." In: Engstrom David Freeman, ed. *Legal Tech and the Future of Civil Justice*, 349–367. Cambridge University Press.

Марина Матић Бошковић[*]

Институт за криминолошка и социолошка истраживања, Београд

Јелена Костић[**]

Институт за упоредно право, Београд

ПРАВОСУЂЕ ПОД ОПСАДОМ: САЈБЕР ПРЕТЊЕ И ЗЛОНАМЕРНА УПОТРЕБА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ПРАВОСУЂУ[***]

Резиме

Како правосудни системи све више интегришу дигиталне технологије и вештачку интелигенцију (ВИ), они постају ефикаснији, али истовремено и знатно рањивији на сајбер претње и манипулације засноване на ВИ. Овај рад истражује растуће ризике од сајбер напада усмерених ка правосуђу, као и злонамерну употребу ВИ у судским поступцима, који представљају озбиљну претњу судском интегритету, правичности, поверењу јавности и ширем оквиру правосудне политике. Чланак анализира кључне рањивости у области сајбер безбедности, укључујући нападе рансомвером на судске базе података, манипулацију доказима путем *deepfake* технологије, алгоритамску пристрасност у аутоматизованом доношењу одлука и дезинформационе кампање које користе ВИ. Употреба ВИ као алата у правним контекстима, кроз лажне манипулације предметима, аутоматизовано хаковање и дигитални надзор, изазива дубоку забринутост у погледу права на правично суђење, независности судства и приступа правди. Ови изазови непосредно утичу на

[*] Имејл: m.m.boskovic@roldevelopmentlab.com; ORCID 0000-0003-1359-0276

[**] Имејл: j.kostic@iup.rs ORCID 0000-0001-6032-3045

[***] Овај рад је резултат истраживања које подржава Министарство науке, технолошког развоја и иновација кроз Споразум о реализацији и финансирању научних истраживања СРО у 2025 са Институтом за криминолошка и социолошка истраживања (бр. 451-03-136/2025-03/200039) и кроз пројекат "Прилагођавање правног оквира друштвеним и технолошким променама са посебним фокусом на вештачку интелигенцију, који спроводи у 2025. години Институт за упоредно право и који финансијски подржава Министарство науке, технолошког развоја и иновација (бр. 451-03-136/2025-03/200049).

правосудну политику, јер захтевају нове механизме заштите и прилагодљиве моделе управљања који могу очувати непристрасност и одговорност у све дигиталнијем правосудном окружењу. Анализом стварних случајева и међународних регулаторних приступа, рад предлаже стратегије за јачање сајбер безбедности судства и заштиту примене ВИ. Препоруке обухватају унапређење дигиталне форензике, транспарентност ВИ, независне механизме ревизије и прекограничну правну сарадњу у борби против сајбер претњи и злоупотребе ВИ у правосуђу. Од суштинског је значаја да се ове мере интегришу у правосудне политике на националном и наднационалном нивоу како би се обезбедила отпорност реформи. Како судови настављају дигиталну трансформацију, проактиван и отпоран безбедносни оквир постаје неопходан за очување владавине права у ери све софистицираних сајбер претњи и ВИ-заснованих правних манипулација. Овај рад наглашава хитну потребу за глобалним правним и технолошким механизмима заштите како би се правосудни системи заштитили од дигиталне експлоатације и сајбер напада потпомогнутих ВИ.

Кључне речи: сајбер безбедност, сајбер претње, правосудна политика, манипулације ВИ, дигитална форензика

* This manuscript was submitted on September 8, 2025, and accepted by the Editorial Board for publishing on December 8, 2025.