Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 127-132

A Conceptual Model for Information Security Assessment in Judicial Information Systems Based on Risk and Regulatory Requirements

Nikolay Koev
University of Library Studies and Information Technologies
Sofia, Bulgaria
4623497-2@unibit.bg

George Dimitrov
Faculty of Information Sciences, Computer Sciences Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
g.g.dimitrov@unibit.bg

Daniela Pavlova
Faculty of Information Sciences, Computer Sciences Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
d.pavlova@unibit.bg

Nikolay Penev
University of Library Studies and Information Technologies
Sofia, Bulgaria
4623496-2@unibit.bg

***Abstract*—The increasing digitalization of the judicial sector requires the implementation of complex information systems that ensure high levels of information security, especially when processing sensitive and classified data. However, the application of security requirements in such environments is often fragmented due to the complexity of regulatory frameworks and the lack of structured approaches for risk assessment. This paper proposes a conceptual model for information security assessment in judicial information systems based on risk and regulatory requirements. The model integrates fundamental principles of information security, including confidentiality, integrity, and availability, with applicable legal and organizational constraints. It provides a structured approach for identifying assets, assessing risks, ensuring compliance with regulatory standards, and selecting appropriate security measures. The proposed model is designed to support decision-making processes and improve the effectiveness of security implementation during the deployment of complex information systems in the judicial sector. The results demonstrate that the model enhances the consistency and traceability of security-related decisions and facilitates alignment with established security standards and legal requirements.**

Keywords—information security, judicial information systems, regulatory requirements, risk assessment.

I. INTRODUCTION

The implementation of electronic justice in the Republic of Bulgaria began gradually in 2017, following the entry into force of amendments to the Civil Procedure Code. Its practical deployment continued in the subsequent years, during which the Unified Information System of the Courts was also introduced. Electronic justice involves the use of information and communication technologies within the judicial system. The digitalization of judicial activities already encompasses electronic case files, electronic submission of documents, internal case management systems, electronic service of documents, videoconferencing hearings, and data exchange with other public authorities. In addition to paper-based case files, cases are now also maintained electronically; summonses and notifications are served electronically; parties can monitor their cases online through the Unified Portal for Electronic Justice; and they can submit and sign documents using electronic signatures. Research on the development of e-justice shows that these processes simultaneously affect access to justice, the efficiency of judicial administration, data protection, and the guarantees of a fair trial [1]-[5]. This dependence on digital infrastructure transforms information security into a strategic factor for the proper functioning of the judiciary.

The problem is not limited to the implementation of individual technical measures. Judicial information systems process personal data, procedural documents, metadata and logs related to the actions of participants, electronic signatures, and, in certain cases, classified information. At the same time, risk management practice in information security shows that courts, as organizational

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol3.120

units, operate with a high degree of institutional independence. They apply different security procedures and do not have a unified risk management instruction applicable to all courts. This has an adverse impact on the overall monitoring of risk and weakens the connection between the judicial system as a whole, its control mechanisms, and regulatory compliance [6], [7]. In this respect, prosecution offices are organized under the authority of the Prosecutor General and strictly follow the principle of subordination by implementing the instructions issued by the highest authority within the prosecution system.

International frameworks for risk management and information security provide well-developed principles for asset identification, impact analysis, risk treatment, and continual improvement [8]-[12]. However, for the judicial sector, these frameworks are not sufficient on their own, as they must be applied in an environment subject simultaneously to substantive legal, procedural, organizational, and technological constraints. Of particular importance are the rules concerning personal data protection, the protection of classified information, electronic identification, compliance with internal rules, and the statutory and subordinate legislative acts governing the activities of the judicial system [13]-[22].

This creates the research need for a model that does not treat risk assessment and regulatory compliance as separate procedures but as interrelated layers of the same decision-making process. The aim of this study is to propose a conceptual model for information security assessment in judicial information systems that identifies critical assets and processes, assesses risk in dimensions relevant to judicial activity, maps risk to applicable regulatory requirements, and supports the selection and prioritization of security measures. The proposed model provides a systematic approach to identifying assets and critical infrastructure, managing risk, ensuring compliance with applicable requirements, and maintaining traceability of actions for audit purposes. The scientific novelty of the approach lies in the integration of a risk layer and a regulatory layer into a single decision-making mechanism adapted to the judicial institutional environment [8]-[12], [13]-[22].

II. Materials and Methods

The study is conceptual and applies a combined qualitative approach based on three groups of sources. The first group includes standards and frameworks for risk management and information security: NIST SP 800-39, NIST SP 800-30 Rev. 1, ISO/IEC 27001:2022, ISO/IEC 27005:2022, ISO 31000:2018, the NIST Cybersecurity Framework 2.0, and NIST SP 800-61 Rev. 3 [8]-[12], [23], [24]. The second group includes scientific publications on information security, risk assessment practices, and the digital transformation of courts [1]-[7], [25], [26]. The third group includes applicable European and national regulatory acts [13]-[22].

To improve the transparency and reproducibility of the conceptual procedure, the development of the model followed a four-step analytical process. First, the relevant literature on e-justice, information security risk management, and cybersecurity in judicial systems was reviewed. Second, international standards and frameworks were examined in order to identify recurring risk management components, including asset identification, impact assessment, risk treatment, monitoring, and continual improvement. Third, applicable European and Bulgarian regulatory requirements were mapped to the identified security dimensions. Fourth, the resulting model was analytically applied to three representative judicial scenarios: electronic submission of procedural documents, administration of electronic case files, and storage, archiving, and destruction of judicial information after the expiry of statutory retention periods.

The scope of the model includes the information assets, processes, and resources in the judicial system that are related to the creation, processing, exchange, storage, and archiving of classified and other sensitive information. For the purposes of the model, assets are grouped into six classes: information assets; application and infrastructure assets; authentication instruments; evidentiary materials; organizational roles; and related external services. The conceptual model is based on the principles of confidentiality, integrity, and availability, supplemented by the principles of "need to know", defense in depth, and least privilege. For each class, security criteria are defined that extend the classical triad with three additional dimensions: authenticity, traceability, and legal admissibility. These dimensions are particularly important in the judicial environment, since the validity of electronic actions, the provability of procedural actions, and the reliability of digital evidence have direct procedural significance [10], [11], [15], [16], [18], [19], [21], [22], [26].

III. Results and Discussion

A. Architecture of the Proposed Model

The proposed model contains six consecutive stages: defining the scope and management roles; identifying and classifying assets; assessing risk; mapping regulatory requirements; selecting and prioritizing security measures; and monitoring, incident response, and improvement of the risk strategy. Within this structure, risk assessment is directly linked to regulatory compliance and practical security management so that each decision can be justified technically, organizationally, and legally. This turns the model into an applicable decision-making framework for the judicial institutional environment [8], [9], [23], [24].

The first stage defines the scope of the assessment by describing the judicial process, information flows, participating roles, and dependencies on external systems. Instead of treating the system only as a software product, the model describes it as a sociotechnical environment in which judges, court clerks, system administrators, lawyers, citizens, external authorities, and suppliers interact. This approach follows observations in the literature on the digital transformation of courts, according to which the effect of technology depends not only on the implemented

platform but also on working practices, management mechanisms, and organizational acceptance [3]-[5].

The second stage introduces an asset-oriented view of the judicial information system. In practical terms, this means describing not only databases, networks, and applications, but also electronic case files, metadata related to procedural actions, participant identifiers, certificates, event logs, archives, backups, interfaces to registers, and repositories for electronic evidence. This approach helps avoid a common weakness in organizational practice, where risk assessment focuses primarily on infrastructure while underestimating the importance of security procedures, sensitive information, and evidentiary materials [6], [7].

The third stage is risk assessment. In the model, risk is determined through a combined assessment of probability, impact, and conditions of use. For the judicial environment, impact is examined across five dimensions: technological, procedural, substantive legal, organizational, and reputational. For example, the temporary unavailability of the Unified Portal for Electronic Justice may appear to be a technically limited incident, but in certain situations it may prevent the submission of a document and thus produce procedural and legal consequences, such as the preclusion of a party's right to submit a response within the statutory time limit. Similarly, a breach of integrity in the logs may not directly damage the main database, but it may compromise the evidentiary reliability of the actions performed. This extended assessment allows risk to be measured more closely in relation to the actual function of the judicial system, rather than solely according to general IT criteria [1], [2], [13], [16], [19], [22].

Table I summarizes the logic of the model by stages, key questions, and expected results. It shows that security assessment does not start from a checklist of controls but from the judicial function of the system and the type of assets that must be protected.

TABLE I. PHASES OF THE PROPOSED MODEL

Stage	Content and result
Scope and roles	Documentation of the process, the participants, the chronological and hierarchical sequence of activities, the roles of the participants involved, and the systems used.
Assets	Catalogue of information, technological, authentication, and evidentiary assets, including critical infrastructure.
Risk	Assessment of probability and impact in technological, procedural, legal, organizational, and reputational dimensions.
Regulatory mapping	Linking risk to applicable regulations, laws, ordinances, and internal rules.
Controls	Prioritization of technical, organizational, and procedural measures.
Monitoring	Indicators, incident readiness, audit, continuous monitoring of the process, and improvement.

The fourth stage is regulatory mapping. This is the main distinguishing feature of the proposed model. For each identified risk, a set of applicable regulatory requirements and internal rules is identified, defining the minimum acceptable level of protection. When personal data are processed, this includes the rules of the GDPR (General Data Protection Regulation), the Personal Data Protection Act, and the national cybersecurity framework; for authentication and signing, it includes eIDAS (electronic identification and trust services regulation) and the internal rules of the judiciary; for electronic procedural actions, it includes Ordinance No. 6 on the performance of procedural actions and certifying statements in electronic form; and for classified information, it includes the Classified Information Protection Act, the Rules for Implementation of the Classified Information Protection Act, and the Ordinance on the Security of Communication and Information Systems [13]-[22]. Regulatory mapping does not replace legal analysis; rather, it structures it so that it can be operationally used in risk management.

The fifth stage covers the selection of security measures. Here, the model applies a combined logic. On the one hand, measures are selected according to the level of risk; on the other hand, they are checked against the mandatory minimum requirements arising from the regulatory framework. This avoids two extreme scenarios: formal implementation of a control without a link to the actual risk, and low-cost risk optimization that does not meet the regulatory minimum. The groups of measures include access management, cryptographic protection, segregation of roles, chronological ordering of logs, administration, data storage, archiving and recovery, accreditation, secure administration, training, and supplier oversight [10], [11], [17], [19], [23]-[26].

The sixth stage introduces monitoring and improvement. In this stage, the model is linked to the principles of CSF 2.0 (Cybersecurity Framework) and the incident response guidance in NIST SP 800-61 Rev. 3, requiring the tracking of indicators for access, data modifications, policy violations, failures of system components, and incidents in exchanges with external systems [23], [24]. For the judicial environment, it is particularly important that these indicators be linked to predefined impact scenarios, such as unsuccessful electronic service of documents, compromise of an electronic signature, unauthorized extraction of a case file, or breach of the chain of custody of digital evidence.

B. Risk - Regulatory Criticality Matrix

This sequence supports the traceability of decisions and makes it easier to justify them before management, an audit body, or an external supervisory authority.

To make the model applicable in practice, risk is assessed not only by combining probability and impact, but also by introducing a regulatory criticality coefficient. Regulatory criticality reflects the extent to which a given risk affects compliance with laws, regulations, and internal rules. It is expressed numerically and indicates how critical a given event is in relation to regulatory requirements. It includes conflicts with legislation, non-compliance with internal rules, prescriptions issued following inspections by

supervisory authorities, and obligations related to the protection of sensitive information. The formula used is:

$$\text{Risk} = \text{Probability} \times \text{Impact} \times \text{Regulatory Criticality} \quad (1)$$

This approach is particularly useful in the public sector, where the acceptability of risk cannot be determined solely by operational efficiency [8]-[12], [17]-[22].

In practice, the matrix uses three levels of regulatory criticality: basic, increased, and critical. Criticality is basic when it concerns general organizational requirements that do not directly affect procedural validity. Criticality is increased when it concerns requirements related to personal data, case administration, electronic identification, traceability, and accountability. Regulatory criticality is critical when it concerns classified information, digital evidence, accredited systems, or actions that may lead to challenges to procedural lawfulness. This step enables more realistic prioritization and reduces the risk of formally equal treatment of vulnerabilities that differ in legal significance.

Table II illustrates the way in which the model links typical judicial assets with regulatory focuses and groups of measures. What is important here is that the asset is not considered abstractly, but in relation to the process. For example, the electronic case file has a different protection profile from the system log, while the repository for digital evidence has a different protection profile from the public portal for inquiries. This differentiation is consistent with recent publications focused on cybersecurity in the judiciary and the protection of digital evidence [25], [26].

TABLE II. EXAMPLE MAPPING OF ASSETS, REGULATORY FOCUSES, AND MEASURES

Scenario	Regulatory focus and priority measures
Electronic submission	eIDAS, Ordinance No. 6, GDPR; strong identification, reliable administration, compliance with the statutory deadline, and confirmation of the statement.
Electronic case file	GDPR, Cybersecurity Act, Ordinance No. 1; role-based model, least privilege, confidentiality, integrity, and availability of information, and control of administrators.
Digital evidence and classified information	Classified Information Protection Act and the Ordinance on the Security of Communication and Information Systems; accreditation, cryptographic protection, compliance with the principles of "need to know" and "defense in depth", physical security, and personnel security.

C. Analytical Application of the Model

The first representative scenario is the electronic submission of documents and certifying statements. Here, the main risks are related to denial of authorship, unauthorized access, manipulation of the time of submission, incomplete documentation and administration, and unavailability of access to the electronic case file at a critical moment concerning compliance with a statutory deadline. The regulatory focus falls on requirements for electronic identification, authentication of authorship, technical formats, logging of actions, and protection of personal data [13], [15], [21], [22]. In this scenario, the model leads to the priority introduction of strong identification, synchronized time, reliable administration, mechanisms for confirmation of the submitted statement, redundant access channels, and procedures for proving a technical incident.

The second scenario is the management of the electronic case file. Here, the main object of protection is not only the content of the case file but also its history: who created, read, edited, forwarded, or signed a specific document and under which access rights. It is also necessary to verify whether the "need-to-know" principle has been observed, namely whether access to certain data with a specific classification level was performed by a user whose level of authorization corresponds to that classification level and who acted in the performance of official duties or a specifically assigned task. The risks include unauthorized internal access, unlawful extraction of data sets, changes without trace and manipulation of information, system unavailability after updates, and insufficient separation of roles. In this scenario, the model emphasizes the need for a detailed rights model, minimization of privileges, strict control over administrative actions, immutable logs, and periodic checks of consistency between organizational roles and technically granted rights [10], [11], [17], [20], [23], [25].

The third scenario is the storage and processing of digital evidence and information under a special protection regime. This is precisely where classical IT criteria are most insufficient unless they are supplemented by requirements for authenticity, chain of custody, accreditation, and documentary provability. Publications on digital evidence in judicial information systems emphasize that protection must cover not only the medium but also the process of receiving, indexing, accessing, copying, analyzing, and presenting evidence before the court [26]. The Classified Information Protection Act and the Ordinance on the Security of Communication and Information Systems additionally impose specific organizational and technical measures, including accreditation, cryptographic security, physical security, document security, and personnel security, with the aim of ensuring the protection and control of responsible officials and system users [18], [19]. In this scenario, the proposed model provides the greatest benefit by linking technical controls with the evidentiary value of the processed information.

D. Discussion

The advantage of the proposed model is that it overcomes the traditional separation between a compliance checklist and risk assessment. This is important because, in the judicial environment, formal compliance with a given requirement does not automatically guarantee that the risk has been managed appropriately, and a low technical

assessment of a given risk does not mean that its legal consequences are insignificant. The combined approach enables more precise justification of priorities, better documentation of decisions, and clearer allocation of roles and responsibilities among technical teams, administrative management, security officers, and legal experts [6]-[9], [23]-[25].

The model also has organizational value. Research on e-justice shows that the real benefit of digitalization depends on institutional readiness and capacity for change, acceptance of the system by internal users, and the balance between efficiency and procedural guarantees [1]-[5]. When security decisions are traceable and well justified, both the acceptance of new procedures and internal control are facilitated. This is especially important when common platforms are implemented across many courts, where organizational differences in information security may lead to different levels of protection.

A limitation of the present study is that the model is conceptual and has not been validated through large-scale empirical application in multiple courts. It does not replace technical audits, penetration testing, digital forensics in the analysis of evidentiary materials, or an individual legal assessment of a specific case. Its purpose is to provide a structured framework that reduces fragmentation in decision-making and makes the relationship between asset, risk, regulatory requirement, and security measure clearer. Future research may develop the model through quantitative scales, profiles for different types of courts, and empirical comparison among implemented systems. A promising direction is also the inclusion of indicators for the quality and usability of judicial data, as recent research shows that data management is becoming key to assessing efficiency and fairness in justice [27].

E. Indicators for Subsequent Control

To be usable in an institutional environment, the model also includes a minimum set of indicators for subsequent control. They are grouped into four categories: indicators for access and identification; indicators for integrity and administration; indicators for continuity and recovery; and indicators for regulatory compliance. The first category includes failed login attempts, use of privileged accounts, deviations in user behavior, and actions outside the usual role. The second category includes changes to electronic case files, events without a digital signature or with a non-corresponding timestamp, and missing logs. The third category includes failures of critical services, time to detect an incident, time to recover, and the availability of verified backups. The fourth category includes deviations from internal policies, incomplete records of processing activities, lack of evidence of training, or gaps in accreditation documentation [13], [14], [17], [19], [23], [24].

The use of indicators should not be reduced to formal reporting. They are meaningful only when linked to specific management decisions: reconsidering roles and rights, reviewing access to classified case files and other sensitive information, updating incident response procedures, providing additional user training, or changing the system architecture. From this perspective, the model functions as a cyclical mechanism for organizational learning rather than as a one-time assessment. Such a dynamic logic is consistent with risk management frameworks and the requirements of modern approaches to cybersecurity [8]-[12], [23], [24].

From a scientific perspective, this also enables better comparison among different judicial organizations. If assets, risks, regulatory focuses, and controls are described according to a unified scheme, it becomes possible to trace which problems recur most often, which measures have the strongest effect, and where the effective and improved organization of processes has the greatest impact on the level of security. In the long term, this opens the possibility of building sectoral profiles for judicial cybersecurity and empirically validating the model through comparable data from different institutions [7], [25], [27].

IV. Conclusions

The proposed conceptual model for information security assessment in judicial information systems integrates risk and regulatory requirements into a single decision-making framework. Its main advantage is that it treats the judicial information system as a sociotechnical and legally regulated environment in which security must protect not only data and infrastructure, but also the validity, traceability, and reliability of procedural actions.

The model is applicable when planning new systems, modernizing existing solutions, conducting internal checks, and preparing for audits in courts and prosecutor's offices, as well as in other administrative structures that process sensitive or classified information. By linking assets, risks, regulatory requirements, and control measures, it supports the consistency, justification, and traceability of decisions. This makes it a suitable basis for the development of institutional methodologies and for empirical verification in a real judicial environment.

The main contribution of the paper is the integration of risk assessment and regulatory compliance into a single decision-support model tailored to judicial information systems.

The model was not empirically validated through deployment in multiple courts, which is a limitation of the present study. Its verification was analytical and scenario-based. The purpose of this stage was to examine whether the proposed structure can consistently connect assets, risks, regulatory requirements, and security measures in typical judicial information system scenarios. Future research should focus on empirical validation through expert evaluation, pilot implementation, or comparative assessment across different judicial institutions.

REFERENCES

[1] A. Maralbaeva, "Evolution of e-Justice Platforms: from ICT in Courts Towards 'Digital Justice' Portal in Kyrgyzstan," International Journal for Court Administration, vol. 15, no. 1, art. 6, 2024, https://doi.org/10.36745/ijca.582.

[2] M. Fabri, "Will COVID-19 Accelerate Implementation of ICT in Courts?," International Journal for Court Administration, vol. 12, no. 2, art. 2, 2021, https://doi.org/10.36745/ijca.384.

[3] J. Björkdahl and C. Kronblad, "Getting on track for digital work: Digital transformation in an administrative court before and during COVID-19," Journal of Professions and Organization, vol. 8, no. 3, pp. 374-393, 2021, https://doi.org/10.1093/jpo/joab015.

[4] C. Kronblad and J. E. Pregmark, "When digitalization hit the court: Strategizing to turn turbulence into opportunities," Journal of Professions and Organization, vol. 12, no. 1, art. joae007, 2025, https://doi.org/10.1093/jpo/joae007.

[5] O. Oktal, O. Alpu, and B. Yazici, "Measurement of internal user satisfaction and acceptance of the e-justice system in Turkey," Aslib Journal of Information Management, vol. 68, no. 6, pp. 716-735, 2016, https://doi.org/10.1108/AJIM-04-2016-0048.

[6] M. Schmidt, "Information security risk management terminology and key concepts," Risk Management, vol. 25, art. 2, 2023, https://doi.org/10.1057/s41283-022-00108-8.

[7] M. Brunner, C. Sauerwein, M. Felderer, and R. Breu, "Risk management practices in information security: Exploring the status quo in the DACH region," Computers & Security, vol. 92, art. 101776, 2020, https://doi.org/10.1016/j.cose.2020.101776.

[8] National Institute of Standards and Technology, Managing Information Security Risk: Organization, Mission, and Information System View, NIST SP 800-39, 2011, https://doi.org/10.6028/NIST.SP.800-39.

[9] National Institute of Standards and Technology, Guide for Conducting Risk Assessments, NIST SP 800-30 Rev. 1, 2012, https://doi.org/10.6028/NIST.SP.800-30r1.

[10] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, 2022.

[11] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection - Guidance on managing information security risks, 2022.

[12] ISO 31000:2018, Risk management - Guidelines, 2018.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4 May 2016.

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333, 27 December 2022.

[15] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), OJ L 257, 28 August 2014.

[16] Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, OJ L, 27 December 2023.

[17] Cybersecurity Act, promulgated in State Gazette No. 94 of 13 November 2018, amended and supplemented in State Gazette No. 17 of 13 February 2026. [In Bulgarian].

[18] Classified Information Protection Act, promulgated in State Gazette No. 45 of 30 April 2002. [In Bulgarian].

[19] Ordinance on the Security of Communication and Information Systems, adopted by Council of Ministers Decree No. 28 of 24 February 2020, promulgated in State Gazette No. 18 of 28 February 2020. [In Bulgarian].

[20] Ordinance No. 1 of 8 January 2008 on Automated Information Systems in the Judiciary. [In Bulgarian].

[21] Rules on the Internal Procedure for the Use of Electronic Signatures and Electronic Identification by the Authorities of the Judiciary, adopted by the Plenum of the Supreme Judicial Council under item 39 of Protocol No. 10/16 March 2017, promulgated in State Gazette No. 32 of 21 April 2017. [In Bulgarian].

[22] Ordinance No. 6 of 3 August 2017 on the Performance of Procedural Actions and Certifying Statements in Electronic Form, promulgated in State Gazette No. 67 of 18 August 2017, amended and supplemented in State Gazette No. 53 of 1 July 2025. [In Bulgarian].

[23] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 2024, https://doi.org/10.6028/NIST.CSWP.29.

[24] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST SP 800-61 Rev. 3, 2025, https://doi.org/10.6028/NIST.SP.800-61r3.

[25] R. S. Alves, J. P. B. da Silva, L. A. Ribeiro Junior, and R. R. Nunes, "Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework," Computers & Security, vol. 157, art. 104584, 2025, https://doi.org/10.1016/j.cose.2025.104584.

[26] I. V. Țicovan and G. Sebestyen, "Solutions for enhancing the protection of digital evidence in judicial information systems," Romanian Journal of Information Technology and Automatic Control, vol. 35, no. 2, pp. 19-32, 2025, https://doi.org/10.33436/v35i2y202502.

[27] M. Ramos-Maqueda and D. L. Chen, "The data revolution in justice," World Development, vol. 186, art. 106834, 2025, https://doi.org/10.1016/j.worlddev.2024.106834.