LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT

ISSN: 1581-5374 E-ISSN: 1855-363X
VOL. 23 , NO. 08(2025)

Legal Security in the Digital Age: Navigating the Challenges of Electronic Trials and the Transformation of Justice

Nouiri samia[1]
Associate professor, Class A, University of 8 May 1945- Guelma, Faculty of Law and Political Science, Law Department, Environmental Legal Studies Laboratory- Algeria
nouiri.samia@univ-guelma.dz

MERDJAL Aicha[2]
Associate professor, Class A, Institute of Law, Law Department, Governance Horizons Laboratory for Sustainable Local Development, University Center of Barika –Algeria
aicha.merdjal@cu-barika.dz

Received:12/03/2025 Accepted:18/05/2025 Published:29/06/2025

Abstract:

The rapid digitalization of society has irrevocably transformed the administration of justice, a process dramatically accelerated by the global COVID-19 pandemic. The transition from physical courtrooms to virtual proceedings and from paper-based records to digital files promises enhanced efficiency, accessibility, and transparency. However, this seismic shift concurrently introduces profound challenges to the foundational principle of legal security. This article examines the complex interplay between digital innovation and the stability of legal rights. It analyzes the multifaceted challenges posed by electronic trials, the admissibility of digital evidence, the digital divide, and cybersecurity threats to judicial systems. The central thesis argues that while technological adoption is inevitable and offers significant benefits, it must be guided by a robust legal and ethical framework to preserve due process, ensure equitable access to justice, and maintain public trust in the rule of law. The article concludes by proposing a multi-pronged strategy for balancing innovation with the safeguarding of fundamental rights, advocating for a human-centric approach to the future of digital justice that reinforces, rather than erodes, legal security.

1. Introduction

The principle of legal security, or legal certainty, is a cornerstone of the rule of law, ensuring that laws are clear, predictable, and stable, thereby allowing individuals and entities to regulate their conduct with a reasonable degree of confidence in the legal consequences of their actions. For centuries, this principle has been upheld through established judicial processes, physical courtrooms, and tangible legal records. However, the dawn of the digital age has begun to test the resilience of these traditional structures. The global shift towards digital governance, communication, and commerce has now fully permeated the justice sector, compelling a re-evaluation of how legal security can be maintained in an environment characterized by rapid and relentless technological change.

The COVID-19 pandemic served as an unprecedented catalyst, forcing judicial systems worldwide to adopt remote technologies to maintain operations. Virtual hearings, electronic filing, and digital case management systems transitioned from niche concepts to mainstream necessities overnight[1]. This forced evolution demonstrated the potential of technology to enhance the efficiency and accessibility of justice. Yet, it also exposed significant vulnerabilities and raised critical questions about the impact on fundamental legal principles. As Judge Roy Ferguson of Texas noted after a viral incident involving a lawyer appearing as a cat on Zoom, the legal profession showed remarkable dedication to keeping the justice system functioning, but these lighthearted moments belie the high-stakes reality for defendants whose lives and liberties are on the line[2].

This article contends that the transition to digital justice and electronic trials, while offering undeniable potential, presents a complex array of challenges to the core tenets of legal security. These challenges are not merely technical; they are deeply intertwined with procedural fairness, constitutional rights, and social equity. If not carefully managed, the drive for digital efficiency could inadvertently lead to a new form of justice that is less equitable, less transparent, and less secure. The core of the problem lies in balancing the immense potential of technological innovation with the unwavering need to protect the fundamental rights of all individuals and maintain unwavering public trust in the judiciary.

To explore this critical issue, this paper will proceed in several parts. First, it will delve into the principle of legal security and its inherent tension with the disruptive nature of digital technology. Second, it will analyze the promises and perils of the electronic courthouse, focusing on the digital divide and the potential erosion of procedural rights. Third, the paper will examine the unique challenges associated with the admissibility and integrity of digital evidence. Fourth, it will address the critical issue of cybersecurity and the protection of sensitive judicial data. Finally, the article will conclude by synthesizing these challenges and proposing a holistic framework for fostering legal security in the digital age, ensuring that the future of justice is both innovative and just.

2. The Principle of Legal Security in an Era of Digital Disruption

Legal security is the principle that the law should be sufficiently clear, stable, and predictable to allow individuals to foresee the legal consequences of their actions. It is a meta-principle that underpins other fundamental rights, including due process and the right to a fair trial. In a stable legal environment, the law is not subject to arbitrary or constant change, and its application is consistent and non-discriminatory. However, the digital era is defined by disruption. Technologies such as artificial intelligence (AI), machine learning, blockchain, and big data analytics are evolving at a pace that far outstrips the traditional, deliberative process of legislative and judicial development.

This rapid evolution creates a significant challenge for legal frameworks. As noted by Bart Custers, technology is becoming increasingly complex and less transparent, a phenomenon he terms the "black box problem"[3]. Self-learning AI systems, for instance, can evolve in ways that even their creators cannot fully explain, making it difficult to scrutinize their decisions for bias or error. When such systems are used in the justice system—for predictive policing, risk assessments in sentencing, or even judicial decision support—they introduce a level of opacity that is fundamentally at odds with the principle of transparency inherent in legal security. The inability to understand or challenge the logic of an automated decision strikes at the heart of procedural fairness.[1]

In response to this challenge, some scholars and policymakers have advocated for the concept of "Agile Lawmaking"[4]. This approach suggests that legal and regulatory frameworks must become more adaptive, iterative, and responsive to technological change, mirroring the 'agile' development methodologies used in the software industry. The goal is to create a legal system that can co-evolve with technology, preventing the law from becoming obsolete. While appealing in theory, this approach carries its own risks to legal security. A legal system that is constantly in flux, with regulations frequently updated in response to the latest technological iteration, can become unpredictable and difficult to navigate. It creates a tension between the need for adaptability and the demand for stability, a core component of legal certainty.[2]

The challenge is further compounded by the global nature of digital technology. Cybercrime, data flows, and online transactions often cross multiple jurisdictions, creating complex legal questions about which laws apply and how they can be enforced. This fragmentation of authority and the complexity of international cyber law are significant hurdles to establishing a predictable legal environment. Legislative instruments like the European Union's General Data

[1] Central Law. (2024, August 15). Importance and Challenges of Implementing Electronic Judicial Processes in Central America. Retrieved from https://central-law.com/en/importance-and-challenges-of-implementing-electronic-judicial-processes-in-central-america/

[2] - op.cit.

Protection Regulation (GDPR) and the proposed AI Act represent ambitious attempts to create a harmonized legal framework, but their global efficacy and their ability to keep pace with innovation remain open questions.

Ultimately, the digital disruption of the legal landscape forces a re-examination of the balance between innovation and regulation. A legal system that is too rigid risks becoming irrelevant and ineffective, while one that is too flexible risks sacrificing the predictability and stability that are essential for legal security. Navigating this tension requires a new paradigm for legal governance—one that is principled, forward-looking, and deeply committed to protecting fundamental rights amidst technological upheaval.[3]

[3] Custers, B. (2024). A fair trial in complex technology cases: Why courts and judges need a basic understanding of complex technologies. Computer Law & Security Review, 52, 105935. https://doi.org/10.1016/j.clsr.2024.105935

3. The Electronic Courthouse: Promises of Access and Perils of the Digital Divide

The transition to the electronic courthouse, characterized by virtual hearings and electronic case management, was greatly accelerated by the COVID-19 pandemic, which necessitated remote operations to maintain judicial functions. This shift carries the significant promise of modernizing the justice system, making it more efficient and accessible. Proponents argue that digital processes can reduce costs for litigants, eliminate geographical barriers, and streamline administrative tasks, thereby accelerating case processing. For individuals in remote or rural areas, or those with mobility issues, the ability to file documents and attend hearings from their homes represents a substantial improvement in access to justice.

However, the rapid and often ad-hoc implementation of these technologies has exposed a deep-seated issue: the digital divide. The term refers to the gap between those who have ready access to modern information and communication technology and those who do not. This divide is not merely about access to a device or an internet connection; it also encompasses digital literacy, the skills required to navigate digital platforms effectively. Research conducted during the pandemic highlighted how these disparities disproportionately affect marginalized communities. A study based on extensive observations of virtual courtrooms in New Jersey found that the move to virtual settings placed an added weight on already-shaky court foundations, particularly in diverse counties with high working-poor populations of color. These communities, often facing the "twin pandemics" of police hyper-surveillance and COVID-19, were least equipped to navigate the complexities of the digital justice system[4].

This digital inequity poses a direct threat to the constitutional right to a fair trial and the principle of equality of arms. A defendant who lacks a stable internet connection, a private space to confer with their lawyer, or the technical skills to operate a video conferencing platform is at a significant disadvantage. The nuances of in-person communication—body language, tone, and the ability to have discreet, real-time conversations with counsel—are often lost in a virtual setting. This can impede a defendant's ability to fully participate in their own defense and can affect a judge's or jury's perception of their credibility. The study by Nir and Musial raises critical questions about whether virtual courtrooms amplify existing structural challenges and racial inequities that pervaded the criminal justice system long before the pandemic.[5]

---

[4] -] Toyi, A. R., & Hamidun, E. Z. P. (2025). Establishing Legal Certainty in the Digital Era: Challenges and Solutions. Estudiante Law Journal, 7(2), 444-460. Retrieved from https://ejurnal.ung.ac.id/index.php/eslaw/article/view/31630.

[5] -] Toyi, A. R., & Hamidun, E. Z. P. (2025). Establishing Legal Certainty in the Digital Era: Challenges and Solutions. Estudiante Law Journal, 7(2), 444-460. Retrieved from https://ejurnal.ung.ac.id/index.php/eslaw/article/view/31630

Furthermore, the reliance on virtual proceedings raises concerns about due process. Issues such as poor video or audio quality, the inability to properly confront witnesses, and the difficulty in ensuring that jurors are not subject to external influences can all compromise the integrity of a trial. While many courts and legal professionals have shown incredible dedication in adapting to these new realities, the fundamental question remains: can a virtual proceeding ever fully replicate the procedural safeguards of a physical courtroom? The pre-COVID system was already fraught with inequities, including failures to protect speedy trial rights and documented disparities in sentencing and plea bargaining. The uncritical adoption of technology without addressing these underlying problems risks entrenching them further in a new, digital guise.[6]

Therefore, while the electronic courthouse offers a path toward a more efficient and seemingly accessible justice system, its implementation must be approached with caution. Ensuring legal security in this context requires more than just providing technology; it demands a concerted effort to bridge the digital divide through public investment in infrastructure and digital literacy training. It also necessitates the development of clear legal standards and protocols for virtual proceedings that explicitly protect the procedural and constitutional rights of all participants. Without these safeguards, the electronic courthouse could become another barrier to justice for the most vulnerable members of society, thereby undermining the very legal security it purports to enhance.[7]

[6]- Grimm, P. W., & Brady, K. M. (n.d.). Admissibility of Electronic Evidence. United States Courts. Retrieved from http://www.flmb.uscourts.gov/judges/tampa/mcewen/GrimmBradyEvidAdmissChart.pdf.

[7] - op.cit.

4. The Evidentiary Challenge: Ensuring the Integrity and Admissibility of Digital Evidence

The shift to digital justice extends beyond the courtroom environment to the very nature of evidence itself. In the modern legal landscape, evidence is increasingly born-digital or digitized—emails, text messages, social media posts, GPS data, and sensor logs are now routine components of both civil and criminal litigation. While this proliferation of digital information offers unprecedented opportunities for fact-finding, it also presents formidable challenges to established evidentiary principles, directly impacting legal security by questioning the reliability and authenticity of the information upon which legal judgments are based.

The primary challenge lies in authentication. Traditional evidentiary rules were developed for tangible objects and documents, where authenticity could be established through physical custody (chain of custody), witness testimony, or forensic examination of physical characteristics. Digital evidence, by contrast, is intangible and easily altered, copied, or fabricated without leaving obvious traces. Establishing that a piece of digital evidence is what it purports to be—that an email was actually sent by the alleged author, that a digital photograph has not been manipulated, or that a system log is an accurate record of events—requires a new set of skills and tools. Courts have struggled to apply old principles to new forms of evidence, leading to inconsistencies in how digital evidence is treated across jurisdictions.[8]

This creates a significant risk to legal security. If the standards for admitting digital evidence are too lax, courts risk making decisions based on fraudulent or unreliable information. Conversely, if the standards are too stringent, valuable and probative evidence may be excluded, leading to unjust outcomes. The core issue is ensuring that the process of admitting digital evidence is both rigorous enough to ensure reliability and flexible enough to accommodate the vast array of new technologies. This requires a satisfactory foundation for a judge to determine that a reasonable jury could find the evidence authentic[5].

The preservation of digital evidence presents another critical challenge. Digital data is fragile and can be easily degraded, deleted, or overwritten. Proper preservation requires specialized forensic techniques to capture a 'snapshot' of the data in a way that is verifiable and complete. The failure to do so—a concept known as spoliation—can have severe legal consequences. However, the obligation to preserve data can be complex in an age of cloud computing, ephemeral messaging apps, and dynamic databases. Determining who is responsible for preserving data, what data must

[8] - U.S. Court System Hack Raises Risk for Sensitive Federal Court Filings. (2025, August 13). Smith, Law, PLLC. Retrieved from https://www.smithlaw.com/newsroom/publications/u-s-court-system-hack-raises-risk-for-sensitive-federal-court-filings

be preserved, and for how long are all questions that the law is still struggling to answer definitively, creating uncertainty for litigants.[9]

Furthermore, the sheer volume of digital evidence in many cases—terabytes or even petabytes of data—creates practical challenges for discovery and review. The process of identifying, collecting, and analyzing this data can be enormously expensive and time-consuming, creating an imbalance of power between well-resourced litigants (such as corporations or the state) and those with limited means. This disparity can undermine the principle of equality of arms, as one party may be unable to effectively challenge the digital evidence presented by the other, not because the evidence is sound, but because they lack the resources to scrutinize it properly.

To address these challenges, the legal system must develop clearer and more consistent standards for the authentication, preservation, and presentation of digital evidence. This includes investing in the training of judges, lawyers, and law enforcement in digital forensics and e-discovery. It also involves exploring the use of technology itself—such as blockchain for creating immutable records or AI for assisting in the review of large datasets—to enhance the integrity of the evidentiary process. Without such adaptations, the evidentiary foundation of our justice system risks becoming unstable, eroding the legal security that comes from knowing that judicial outcomes are based on reliable and authentic facts.[10]

[9] - op.cit.

[10] - U.S. Court System Hack Raises Risk for Sensitive Federal Court Filings. (2025, August 13). Smith, Law, PLLC. Retrieved from https://www.smithlaw.com/newsroom/publications/u-s-court-system-hack-raises-risk-for-sensitive-federal-court-filings.

5. Cybersecurity and the Protection of Judicial Data: A New Frontier for Legal Security

The digitization of court records and proceedings introduces a new and critical vulnerability: cybersecurity. Judicial systems are repositories of vast amounts of sensitive information, including personal data of litigants, sealed case files containing trade secrets, national security information, and confidential judicial deliberations. The transition from secure physical archives to networked digital systems makes this data a high-value target for a range of malicious actors, from individual hackers and organized crime syndicates to state-sponsored intelligence agencies. A breach of judicial data not only compromises the privacy and safety of individuals but also threatens to undermine the integrity of the entire justice system and erode the public's trust in its ability to function securely.

Recent events have demonstrated that this threat is not merely theoretical. Court systems at both the state and federal levels have been targeted by increasingly frequent and sophisticated cyberattacks[6]. These attacks can take many forms, including ransomware attacks that paralyze court operations by encrypting essential files, data breaches that expose sensitive information, and denial-of-service attacks that disrupt access to online services. In 2025, the U.S. judiciary announced that its electronic case management system (CM/ECF) had been breached, raising alarms about the security of highly sensitive, non-public documents filed in federal courts[7][8]. Such incidents reveal that even well-resourced judicial systems struggle to defend against a constantly evolving threat landscape.[11]

The challenge of securing judicial data is multifaceted. First, many court systems, particularly at the state and local levels, operate with outdated IT infrastructure and limited cybersecurity budgets. They often lack the resources and expertise to implement robust security measures, such as multi-factor authentication, end-to-end encryption, and continuous security monitoring. This leaves them vulnerable to even relatively unsophisticated attacks.[12]

Second, the very nature of the justice system requires a delicate balance between transparency and security. The principle of open justice dictates that court records and proceedings should be accessible to the public. However, in a digital environment, this accessibility can be exploited by malicious actors. For example, publicly accessible court records can be scraped en masse to gather personal information for identity theft or other nefarious purposes[13]. Balancing the public's right to access with the need to protect sensitive information in an electronic format is a complex policy and technical challenge that courts are still grappling with privacy policies for

[11]- Winn, P. A. (2004). Online court records: Balancing judicial accountability and privacy in an age of electronic information. Washington Law Review, 79(1), 307-346.

[12] Op.cit., p 308.

[13]- op.cit., p 309.

electronic case files, which mandate the redaction of personal identifiers, are a step in the right direction, but their effectiveness depends on consistent and flawless implementation[10].

Third, the human element remains a significant vulnerability. Phishing attacks, where court personnel are tricked into revealing their credentials, are a common vector for breaching security. A lack of cybersecurity awareness and training among judges, court staff, and lawyers can create openings for attackers. Ensuring that all participants in the justice system are vigilant and adhere to security protocols is a critical, yet often overlooked, component of a strong cybersecurity posture.

Protecting judicial data is, therefore, a fundamental aspect of ensuring legal security in the digital age. A justice system that cannot protect its own information cannot be considered secure. This requires a comprehensive approach that includes significant investment in modern, secure IT infrastructure; the development and implementation of clear cybersecurity policies and protocols; regular security audits and risk assessments; and continuous training for all court personnel. It also necessitates a shift in mindset, where cybersecurity is not seen as a purely technical IT issue, but as a core governance responsibility that is essential to the administration of justice and the preservation of the rule of law.[14]

[14]- Privacy Policy for Electronic Case Files. (n.d.). United States Courts. Retrieved from https://www.uscourts.gov/privacy-policy-electronic-case-files

6. Conclusion: Rebuilding Trust and Forging a Path to Secure Digital Justice

The digital transformation of the justice system is an irreversible and accelerating trend, bringing with it a paradigm shift that challenges the very foundations of legal security. The journey from paper to pixels, and from physical courtrooms to virtual spaces, is laden with both extraordinary promise and significant peril. As this article has demonstrated, the challenges are not merely technical but are deeply woven into the fabric of due process, procedural fairness, social equity, and the fundamental trust that underpins the rule of law. The uncritical pursuit of efficiency and modernization risks creating a system of justice that is faster and more convenient for some, but less just, less secure, and less equitable for all.

To navigate this complex transition successfully, a passive or reactive approach is insufficient. What is required is a proactive, human-centric strategy that places the principles of legal security at the forefront of the innovation agenda. This strategy must be built on several key pillars:

First, bridging the digital divide. The promise of access to justice through technology can only be realized if the digital divide is actively addressed. This requires more than just ensuring access to hardware; it necessitates a commitment to digital literacy, public investment in reliable internet infrastructure, and the design of user-friendly platforms that are accessible to people of all abilities and backgrounds. Courts must maintain non-digital options to ensure that no one is denied justice simply because they are on the wrong side of the digital gap.

Second, developing robust legal and ethical frameworks. The law must evolve in concert with technology. This requires the development of clear, consistent, and principled standards for virtual proceedings, the admissibility of digital evidence, and the use of AI in the justice system. This framework must be grounded in the protection of fundamental rights, ensuring that principles like the right to a fair trial, the presumption of innocence, and the equality of arms are not degraded in the digital realm. As advocated by some, an "Agile Lawmaking" approach may be necessary, but it must be balanced with the need for legal stability and predictability.

Third, prioritizing cybersecurity and data protection. The security of judicial data is not an IT issue; it is a fundamental pillar of legal security. Judicial systems must be fortified against cyber threats through sustained investment, the adoption of best-practice security protocols, and the cultivation of a security-conscious culture among all legal professionals. The integrity of the justice system depends on its ability to protect the sensitive information entrusted to it.

Fourth, fostering transparency and accountability. As judicial processes become more automated and opaque, the need for transparency and accountability becomes more acute. The "black box" problem associated with complex algorithms must be countered with mechanisms for independent auditing, algorithmic impact assessments, and meaningful explanations for automated decisions. Public trust cannot be sustained in a system where justice is administered by inscrutable machines.

Fifth, investing in education and training. The digital transformation requires a corresponding transformation in the skills and knowledge of legal professionals. Judges, lawyers, and court staff must be equipped with the necessary training to understand the technological landscape, from the basics of cybersecurity to the complexities of digital evidence and AI.

In conclusion, the challenge of ensuring legal security in the digital age is not about choosing between technology and tradition. It is about harnessing the power of innovation in a way that reinforces, rather than erodes, the core values of our justice system. It is about building a future where technology serves justice, and not the other way around. This requires a sustained and collaborative effort from policymakers, judges, lawyers, technologists, and the public. By balancing innovation with a steadfast commitment to fundamental rights, we can forge a path toward a system of digital justice that is not only more efficient but also more equitable, transparent, and, ultimately, more secure.

References

[1] Central Law. (2024, August 15). Importance and Challenges of Implementing Electronic Judicial Processes in Central America. Retrieved from https://central-law.com/en/importance-and-challenges-of-implementing-electronic-judicial-processes-in-central-america/

[2] Nir, E., & Musial, J. (2022). Zooming In: Courtrooms and Defendants' Rights during the COVID-19 Pandemic. Social & Legal Studies, 31(5), 725-745. https://doi.org/10.1177/09646639221076099

[3] Custers, B. (2024). A fair trial in complex technology cases: Why courts and judges need a basic understanding of complex technologies. Computer Law & Security Review, 52, 105935. https://doi.org/10.1016/j.clsr.2024.105935

[4] Toyi, A. R., & Hamidun, E. Z. P. (2025). Establishing Legal Certainty in the Digital Era: Challenges and Solutions. Estudiante Law Journal, 7(2), 444-460. Retrieved from https://ejurnal.ung.ac.id/index.php/eslaw/article/view/31630

[5] Grimm, P. W., & Brady, K. M. (n.d.). Admissibility of Electronic Evidence. United States Courts. Retrieved from http://www.flmb.uscourts.gov/judges/tampa/mcewen/GrimmBradyEvidAdmissChart.pdf

[6] State and Local Courts Struggle to Fight Increasing Cyberattacks. (2024, June 5). State Court Report. Retrieved from https://statecourtreport.org/our-work/analysis-opinion/state-and-local-courts-struggle-fight-increasing-cyberattacks

[7] Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System. (2025, August 7). United States Courts. Retrieved from https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system

[8] U.S. Court System Hack Raises Risk for Sensitive Federal Court Filings. (2025, August 13). Smith, Law, PLLC. Retrieved from https://www.smithlaw.com/newsroom/publications/u-s-court-system-hack-raises-risk-for-sensitive-federal-court-filings

[9] Winn, P. A. (2004). Online court records: Balancing judicial accountability and privacy in an age of electronic information. Washington Law Review, 79(1), 307-346.

[10] Privacy Policy for Electronic Case Files. (n.d.). United States Courts. Retrieved from https://www.uscourts.gov/privacy-policy-electronic-case-files