

THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN RELATION TO THE RIGHT TO PRIVACY IN CASES OF SEXUAL CONTENT DISSEMINATION

Safaruddin Harefa

Faculty of Law, Universitas Tanjungpura

Jl. Prof Dr H. Hadari Nawawi, Bansir Laut, Pontianak Tenggara, Kota Pontianak, Kalimantan Barat, Indonesia 78124

E-mail: safaruddinharefa@hukum.untan.ac.id

Article	Abstract
<p>Article History: Submitted: September 2025 Reviewed: March 2026 Accepted: April 2026 Published: April 2026</p> <p>Keywords: Digital Rights; Electronic Evidence; ITE Law, Pandeglang Decision; Privacy Rights.</p>	<p><i>The rapid advancement of digital technology has transformed the nature of crime and evidence, requiring legal systems to accommodate electronic forms of proof. This study analyzes the admissibility of electronic evidence in Indonesian criminal procedure law and its implications for the protection of privacy, particularly in cases involving the dissemination of sexual content. Using a normative juridical approach, this research examines statutory frameworks, including the ITE Law and its 2024 amendment, the 1945 Constitution, Law No. 20 of 2025 on the new Criminal Procedure Code, and Law No. 27 of 2022 on Personal Data Protection. It also employs a case study of the Pandeglang District Court Decision No. 71/Pid.Sus/2023/PN Pdl to assess the gap between <i>das sollen</i> and <i>das sein</i>. The findings indicate that Indonesia has normatively established a clear legal basis recognizing electronic evidence as valid and binding. However, judicial practice, particularly in cases decided prior to the enactment of the new KUHAP and the Personal Data Protection Law, tends to prioritize evidentiary validity over the protection of victims' privacy. The Pandeglang case demonstrates that although electronic evidence was lawfully admitted, the absence of procedural safeguards created risks of re-victimization and undermined the victim's dignity. This study concludes that while the issue of admissibility has been resolved under the current legal framework, challenges remain in ensuring privacy protection in judicial practice. Therefore, courts must adopt rights-sensitive approaches, including closed hearings, anonymization, and proportional use of evidence, to balance evidentiary effectiveness with the protection of fundamental rights in the digital era.</i></p>

A. Introduction

The digital era has fundamentally transformed the nature of crime and evidence, requiring legal systems to adapt to new forms of violations and corresponding modes of proof. In Indonesia, the enactment of Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), later amended by Law No. 19 of 2016 and most recently by Law No. 1 of 2024 (Second Amendment), represents a decisive step towards integrating electronic evidence into the national legal framework. Normatively (*das sollen*), the law recognizes electronic

information and electronic documents, including their printouts, as valid legal evidence with equal probative value to traditional forms of evidence regulated in the Code of Criminal Procedure (*KUHAP*).¹

This recognition aligns Indonesia with global trends in evidentiary law, particularly in acknowledging the increasingly indispensable role of digital evidence in prosecuting cybercrime and technology-facilitated offenses. Furthermore, this development is reinforced by the enactment of Law No. 20 of 2025 concerning the new Code of Criminal Procedure (*KUHAP*), which was ratified on 17 December 2025. The new *KUHAP* explicitly accommodates electronic evidence as part of the formal evidentiary system. As stipulated in Article 235 paragraph (1), the recognized forms of evidence include: (a) witness testimony; (b) expert testimony; (c) documents; (d) defendant's statement; (e) physical evidence; (f) electronic evidence; (g) judicial observation; and (h) any other material that may be used for evidentiary purposes in court proceedings, provided that it is obtained lawfully.

Beyond the recognition of admissibility, the ITE Law and its amendments reflect principles aimed at ensuring both the reliability of evidence and the protection of fundamental rights.² Article 5 of the ITE Law, reaffirmed under Law No. 1 of 2024, explicitly stipulates the legal standing of electronic documents. Furthermore, Indonesian constitutional law, particularly Article 28G of the 1945 Constitution, guarantees the right of every person to protection of self, personal dignity, and private data.³ International human rights commitments, including the International Covenant on Civil and Political Rights (ICCPR), further embed privacy and fair trial rights within the state's legal obligations. From a normative perspective, therefore, Indonesia possesses a doctrinal foundation that aspires to harmonize effective law enforcement with the protection of privacy and digital rights.⁴

Empirically (*das sein*), however, judicial practice demonstrates a more complex and sometimes problematic reality. The Pandeglang District Court Decision No.

¹ Ariansyah and Lucky Eka Khalis Aulia ES, "Reconstruction of the Position of Electronic Documents as Evidence in Civil Case Evidence Based on Deep Ecology," *Judex Laguens* 3, no. 1 (2025): 95–112, <https://doi.org/10.25216/ikahi.3.1.4.2025.95-112>.

² Mustalim Lasaka, "Ius Constituendum of Electronic Evidence Arrangement in Criminal Procedure Law," *Jurnal Legalitas* 16, no. 2 (2023): 154–166, <https://doi.org/10.33756/jelta.v16i2.20306>.

³ Adisti Puspa Setyawan, Antonius Sambodo Adi A, I Dewa B S Wirantaya, Pina Mustika, and William Gomarga, "Indonesia's Electronic Information and Transactions Law: History, Impact, and Challenges," *Journal Research of Social Science, Economics, and Management* 4, no. 12 (2025): 2154–2165, <https://doi.org/10.59141/jrssem.v4i12.899>.

⁴ Abdul Kadir Zaylani Muhtar, Muh. Risnain, and Zunnuraeni, "The Right to Life Based on The International Covenant on Civil and Political Rights And Its Application In Indonesian National Law," *Mataram Journal of International Law* 2, no. 2 (2024): 125–144, <https://doi.org/10.29303/majil.v2i2.5031>.

71/Pid.Sus/2023/PN Pdl⁵ illustrates this tension. In this case, the defendant recorded sexual activities with the victim without consent and disseminated the content through Instagram direct messages. The prosecution introduced electronic evidence such as WhatsApp transcripts, screenshots, Instagram account data, and flash drives containing explicit images. The court accepted this evidence as lawfully obtained and therefore admissible, convicting the defendant under Article 45 paragraph (1) jo. Article 27 paragraph (1) of the ITE Law.

While the admission of such evidence reflects conformity with the normative framework, it simultaneously exposes a significant gap in protecting the victim's rights. The very evidence used to establish the defendant's guilt, explicit recordings and images, represents a direct intrusion into the victim's bodily privacy.⁶ The judicial process, by reproducing and scrutinizing such materials, risks perpetuating re-victimization and undermining the constitutional guarantee of privacy. Moreover, the court's reasoning primarily emphasized procedural validity and evidentiary authenticity, but gave limited consideration to proportionality and victim-sensitive safeguards, which are crucial in cases involving sexual content.

This divergence between *das sollen* and *das sein* highlights a fundamental problem: while the law provides for both admissibility of electronic evidence and protection of privacy, judicial application tends to prioritize evidentiary value over human rights safeguards.⁷ In effect, the reliability of proof is affirmed, yet the victim's dignity and digital rights remain vulnerable. The 2024 Second Amendment to the ITE Law attempted to recalibrate this balance by reaffirming lawful acquisition and proportionality as conditions for admissibility. However, as the Pandeglang decision demonstrates, the translation of these normative commitments into judicial reasoning remains limited.

Therefore, the background of this study rests on the need to critically analyze how courts interpret and apply the admissibility of electronic evidence in light of the right to privacy. The Pandeglang case underscores the gap between normative aspirations and empirical realities, raising urgent questions about the adequacy of current practices in safeguarding both evidentiary integrity and human rights protection. This research seeks to address that gap by examining the judicial treatment of electronic evidence in cases of sexual content

⁵ Pengadilan Negeri Pandeglang, "Putusan Nomor 71/Pid.Sus/2023/PN Pdl," 2023, <https://putusan3.mahkamahagung.go.id/direktori/putusan/zaee3fd389af4eac978731303333437.html>.

⁶ Sergey Vasiliev, "The Role and Legal Status of the Prosecutor in International Criminal Trials," November 26, 2010, <https://doi.org/10.2139/ssrn.1715465>.

⁷ Harkrisnowo *et al.*, *Law and Justice in a Globalized World: Proceedings of the Asia-Pacific Research in Social Sciences and Humanities, Depok, Indonesia, 7–9 November 2016: Topics in Law and Justice* (London: CRC Press/Balkema Taylor & Francis Group, 2018), 71.

dissemination, thereby contributing to the discourse on digital rights and evidentiary law in Indonesia's evolving legal system.

B. Method

This research adopts a normative juridical approach, focusing on the study of laws, principles, and doctrines relevant to the admissibility of electronic evidence and the protection of privacy rights. The normative juridical method is employed to analyze the applicable legal framework, including the 1945 Constitution, the Criminal Procedure Code, the ITE Law and its amendments, particularly Law No. 1 of 2024, as well as judicial precedents such as Decision No. 71/Pid.Sus/2023/PN Pandeglang. This approach enables the research to assess the coherence between *das sollen* (what the law prescribes) and *das sein* (how the law is applied in practice), thereby highlighting normative gaps and doctrinal challenges in safeguarding digital rights.⁸

The research is descriptive-analytical in specification, relying on secondary data sources. Primary legal materials include statutory provisions and court decisions, while secondary materials consist of scholarly literature, commentaries, and academic writings on electronic evidence and human rights. Data collection is conducted through library research, while data analysis applies a qualitative normative method by interpreting legal texts and judicial reasoning.⁹ The analysis seeks to evaluate whether existing legal norms are adequate to protect the right to privacy in cases involving electronic evidence, and to propose a more balanced normative framework for future application.

C. Analysis and Discussion

1. The Admissibility of Electronic Evidence under the ITE Law

a. Normative Framework of Electronic Evidence in Indonesian Law

The enactment of Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) has significantly reshaped Indonesia's evidentiary landscape. This reform marks the most comprehensive attempt to date to harmonize the probative value of electronic information with the

⁸ Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020), 44.

⁹ Jan M Smits, "What is Legal Doctrine? In the Aims and Methods of Legal-Dogmatic Research," dalam R. van Gestel, H. Micklitz, dan E. L. Rubin (eds.), *Rethinking Legal Scholarship* (Cambridge: Cambridge University Press, 2017), 207–228.

principles of criminal procedure, human rights, and technological reliability.¹⁰ In substance, the 2024 Amendment confirms that electronic information and electronic documents, along with their printouts, are not only admissible but also hold an evidentiary position equivalent to conventional written evidence, provided that their authenticity and integrity can be demonstrated.¹¹

This recognition addresses the long-standing doctrinal tension in Indonesian procedural law. Under the previous regime, the Criminal Procedure Code (*KUHAP*) adhered to the negative *wettelijk bewijsstelsel*, which exhaustively enumerated admissible forms of evidence, while the ITE Law expanded that catalogue by expressly recognizing electronic information and documents. However, this tension has been formally resolved with the enactment of Law No. 20 of 2025 concerning the New Criminal Procedure Code, which explicitly includes electronic evidence as one of the recognized means of proof. Nevertheless, it is important to note that the case under discussion arose prior to the entry into force of the new *KUHAP*. Accordingly, this analysis still reflects the earlier doctrinal framework, while simultaneously acknowledging that, under the current legal regime, the probative value of electronic evidence is no longer supplementary but has become explicitly normative and binding upon courts in adjudicating cases involving digital footprints.

The normative foundation under Law No. 1 of 2024 further refines the conditions for admissibility. First, it emphasizes authenticity, requiring that electronic evidence be generated, transmitted, or stored through a system that is reliable and verifiable. This provision addresses longstanding concerns regarding the mutability of digital data, which can be easily altered, deleted, or fabricated. Second, the amendment stresses lawful acquisition, stipulating that evidence must be obtained in compliance with procedural safeguards. Evidence derived from unlawful interception or unauthorized access is deemed inadmissible, thereby aligning Indonesia's evidentiary regime with the principle of due process. Third, the law incorporates proportionality as an implicit standard, particularly relevant in cases involving sensitive personal data, such as sexually explicit recordings or private communications.¹²

¹⁰ Muzakkir and Taufik Hidayat, "Juridical Review Article 27A of Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Information and Electronic Transactions," *Jurnal Hukum Samudra Keadilan* 19, no. 2 (2025): 238–249, <https://doi.org/10.33059/jhsk.v19i2.10650>.

¹¹ Enden Haetami, "The Strength of Electronic Evidence in the View of Islamic Law," *International Journal of Science and Society* 4, no. 4 (2023): 666–675, <https://doi.org/10.54783/ijssoc.v4i4.615>.

¹² Ahmed Moussa, "Electronic Evidence and Its Authenticity in Forensic Evidence," *Egyptian Journal of Forensic Sciences* 11 (2021): 20, <https://doi.org/10.1186/s41935-021-00234-6>.

From a normative perspective, these provisions demonstrate Indonesia's commitment to bridging the gap between technological realities and evidentiary doctrine. However, doctrinal recognition does not automatically translate into consistent judicial practice. The case of Decision No. 71/Pid.Sus/2023/PN Pandeglang illustrates how courts continue to grapple with the dual imperatives of evidentiary reliability and rights protection. In that case, the prosecution introduced electronic materials, WhatsApp chat transcripts, Instagram account data, and flash drives containing explicit screenshots, as proof of unlawful dissemination of sexual content. The court admitted these materials as lawful evidence, relying on their clear chain of custody and verifiable authenticity. On its face, this reasoning accords with the 2024 Amendment's emphasis on authenticity and lawful acquisition.¹³¹⁴

Yet a closer analysis reveals a tension between the formal validity of evidence and the substantive protection of privacy. The very act of reproducing intimate digital materials in court proceedings risks exacerbating harm to the victim's dignity and bodily integrity. The 2024 Amendment recognizes electronic evidence as valid, but it does not yet provide a detailed framework for privacy-sensitive adjudication, for instance, mechanisms to seal sensitive exhibits, anonymize victims, or limit access to explicit content during trial. As a result, while the Pandeglang decision upheld the admissibility of digital evidence, it offered only limited safeguards against secondary victimization.¹⁵

This highlights a normative-empirical gap between *das sollen* and *das sein*. *Das sollen*, embodied in the 2024 Amendment, aspires to balance evidentiary effectiveness with fundamental rights. *Das sein*, reflected in judicial practice, often privileges evidentiary utility over privacy protection. In other words, courts tend to treat digital materials primarily as proof of guilt, while underestimating their potential to inflict renewed harm on victims. This imbalance underscores the need for courts to interpret the ITE Law not merely as a tool for evidentiary expansion but as a normative mandate for rights-sensitive adjudication.

¹³ Indonesia Judicial Research Society, Maharani, Marsha, Inatsan Ashila, Bestha, Ismaya, Siti, Assyifa, Aisyah, Wicaksana, Dio Ashar, Barus, Naomi Rehulina, dan Nasir, Muhammad Ad'har, *The Role of Legal Empowerment by the Community in Strengthening Access to Justice for Women in Conflict with the Law in Indonesia* (Jakarta: Indonesia Judicial Research Society, 2023), 59-60.

¹⁴ Eko Riyadi, "Institutionalization of Human Rights Standards in Indonesia," dalam Aksel Tømte dan Eko Riyadi (eds.), *International Human Rights and Local Courts: Human Rights Interpretation in Indonesia* (Abingdon, Oxon; New York: Routledge, 2024), 73-74.

¹⁵ Uta Kohl, "The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy," *International and Comparative Law Quarterly* 72, no. 3 (2023): 737-769, <https://doi.org/10.1017/S0020589323000258>.

Comparative analysis reinforces this point. Many jurisdictions that recognize electronic evidence also impose strict procedural safeguards. For instance, courts in Europe apply the principles of necessity and proportionality before admitting intrusive digital materials, ensuring that the evidentiary value outweighs the potential rights violation. Similarly, U.S. jurisprudence emphasizes chain of custody and privacy-protective measures, particularly in cases involving minors or sexually explicit materials. By contrast, Indonesian courts have yet to articulate systematic criteria for balancing admissibility with privacy, leaving discretion largely to individual judges.¹⁶

In this regard, the 2024 Amendment offers a normative opening. Its provisions on lawful acquisition and integrity could be interpreted expansively to encompass privacy protection. For example, an “unlawful acquisition” may not only include hacking or unauthorized access but also the recording of intimate acts without consent. Likewise, the requirement of “integrity” could be linked to ensuring that evidence is not only unaltered technically but also untainted by rights violations. By adopting such interpretations, courts could align evidentiary doctrine more closely with constitutional guarantees under Article 28G of the 1945 Constitution, which enshrines the right to privacy and personal security.

The amendment underscores the necessity of digital forensics in verifying authenticity. In practice, however, Indonesian courts face uneven forensic capacity. Some judges may lack sufficient technical literacy to evaluate metadata, encryption, or digital signatures. Without consistent forensic support, courts risk admitting evidence whose authenticity is questionable or dismissing evidence that is technically sound but poorly presented. Thus, the normative recognition of electronic evidence in the 2024 Amendment must be matched with institutional investment in forensic expertise, standardized protocols, and judicial training.

The 2024 ITE Law represents a decisive normative advance in affirming the admissibility of electronic evidence. It provides a legal foundation that is both doctrinally sound and technologically responsive. Nevertheless, its implementation reveals persistent challenges: the risk of re-victimization in sensitive cases, the lack of explicit privacy safeguards, and the uneven capacity of courts to authenticate digital materials. The task ahead is not merely to recognize electronic evidence as valid but to operationalize that recognition in a manner consistent with constitutional rights, human dignity, and the

¹⁶ Zhanagul Balkibayeva, “Problems of Admissibility and Reliability of Metadata as Evidence,” *International Journal of Law and Policy* 2 (2024): 48–58, <https://doi.org/10.59022/ijlp.232>.

integrity of the justice system. Bridging the gap between *das sollen* and *das sein* requires judicial interpretation that views the 2024 Amendment not only as a technical instrument of proof but also as a normative framework for balancing evidentiary effectiveness with the protection of fundamental rights in the digital era.

b. Judicial Application in Decision No. 71/Pid.Sus/2023/PN Pandeglang

The Pandeglang District Court's Decision No. 71/Pid.Sus/2023/PN Pdl presents a significant case study in the application of the ITE Law, particularly regarding the admissibility of electronic evidence and its relation to fundamental rights. The court was tasked with evaluating whether electronic materials, namely WhatsApp chat transcripts, Instagram account data, screenshots, and flash drives containing digital images, could serve as lawful evidence in proving the unlawful dissemination of sexual content. The judgment demonstrates a careful balancing of evidentiary rules with the protection of human rights, even though the court did not explicitly frame its reasoning in terms of international human rights law.

A central aspect of the decision lies in the recognition of consent as a determinant of legality. The judges emphasized that recording or distributing sexual activities without the partner's knowledge or consent constitutes an unlawful act. This reasoning implicitly aligns with the right to privacy, the right to bodily integrity, and the right to sexuality, which are protected under both the Indonesian Constitution (Article 28G of the 1945 Constitution) and international human rights standards, particularly Article 17 of the ICCPR.¹⁷ Although the court did not cite these instruments, its acknowledgment that non-consensual recording constitutes a violation reflects the integration of rights-based principles into evidentiary reasoning. Such recognition is crucial, as it reframes electronic evidence not merely as neutral data, but as materials whose very creation and use may involve human rights violations.

The court further addressed the issue of authenticity and lawful acquisition, underscoring that electronic evidence must be procured in a manner that is verifiable, traceable, and legally accountable. This corresponds to the requirement under the 2024 Amendment to the ITE Law that electronic information is admissible only when obtained through legitimate procedures. By scrutinizing whether the evidence presented was

¹⁷ Law Commission, "Evidence in Sexual Offences Prosecutions: Consultation Paper 259," May 15, 2023, <https://www.lawcom.gov.uk/project/evidence-in-sexual-offence-prosecutions/>.

properly collected and preserved, the judges adhered to the principle of fair trial. They refrained from automatically accepting digital materials, instead evaluating the process of acquisition, chain of custody, and reliability.¹⁸ This reflects judicial awareness that the mere existence of digital data does not guarantee its integrity, as electronic materials are particularly vulnerable to alteration or manipulation.

In practical terms, this approach resonates with the principle of due process found in comparative jurisprudence. For example, the European Court of Human Rights has consistently held that the reliability of evidence, including the circumstances of its acquisition, forms part of the assessment of whether a trial is fair as a whole.¹⁹ By requiring proof that digital evidence was obtained in accordance with procedural safeguards, the Pandeglang court followed a similar trajectory, thereby reducing the risk of admitting tainted or unreliable materials. This methodology not only strengthens evidentiary reliability but also enhances public trust in judicial outcomes.

Importantly, the court's reasoning also touched upon broader notions of gender-based violence. The recording of sexual activity without consent, particularly when the victim was unconscious due to alcohol, can be categorized as a form of sexual violence and an infringement on bodily autonomy.²⁰ Although the decision was framed primarily through the ITE Law, it implicitly recognized the gendered dimension of digital crimes. The use of electronic evidence in this context thus intersects with the state's obligation to protect individuals from gender-based violations, a principle increasingly recognized in both domestic and international legal frameworks.²¹

Another notable contribution of the judgment is its implicit recognition of digital rights as part of fair trial guarantees. By requiring that electronic evidence be properly verified before admission, the court affirmed that individuals are entitled to access justice in a manner that respects both procedural fairness and digital integrity. Digital rights, though still lacking a universally agreed definition at the international level, generally encompass the ability to access, use, and create digital media while being protected from

¹⁸ Aga Naya Saputra and Ghina Salsabila Aven, "Legal Analysis of the Use of Electronic Evidence in Providing Evidence in Corruption Cases (Decisions in Indonesia)," *Legal Brief* 14, no. 3 (2025): 764–773, <https://doi.org/10.35335/legal.v14i3.1410>.

¹⁹ Yage Huang, "Authenticating Social Media Evidence in Chinese Criminal Procedure Law—A Comparative Study," *Indiana Journal of Global Legal Studies* 31, no. 2 (2024): 45–49, <https://www.repository.law.indiana.edu/etd>.

²⁰ Fajar Yaskur and Ifahda Pratama Hapsari, "The Existence of Sexual Violence Crime in Indonesia," *JUSTISI* 11, no. 1 (2024): 95–110, <https://doi.org/10.33506/js.v11i1.3748>.

²¹ Erna Dewi, "The Problems of Sexual Consent in Colleges Environment," *Migration Letters* 21, no. S3 (2024): 1376–1382, <https://migrationletters.com/index.php/ml/article/view/7474>.

misuse.²² In this sense, the decision reflects an emerging jurisprudential trend in Indonesia that situates electronic evidence not only within technical legality but also within a broader rights-based discourse.²³

Nevertheless, certain gaps remain. While the court took care to examine authenticity and consent, it did not fully articulate mechanisms for safeguarding the victim's privacy once the evidence was introduced. For instance, the public handling of sexually explicit materials in court may inadvertently contribute to secondary victimization. International best practices often include measures such as closed sessions, sealing of sensitive exhibits, or anonymization of victims' identities, practices that were not explicitly mandated in this case. The absence of such protections underscores the need for Indonesian courts to develop more robust privacy-sensitive protocols for handling intimate digital evidence.

The Pandeglang case illustrates both progress and limitations in judicial application of the ITE Law. On the one hand, the decision demonstrates consistency with the normative framework established by Law No. 1 of 2024, emphasizing authenticity, lawful acquisition, and accountability in the admission of electronic evidence. It also reflects human rights principles concerning privacy, bodily integrity, and fair trial, even if these were not expressly cited. On the other hand, the case highlights ongoing challenges in ensuring proportionality and preventing re-victimization, particularly in matters involving sensitive sexual content. The judgment therefore serves as a valuable precedent, while simultaneously signaling the urgent need for judicial guidelines that harmonize evidentiary rigor with the protection of fundamental rights in the digital age.

2. The Right to Privacy and Its Protection in Cases of Sexual Content Dissemination

a. Dimensions of Privacy: Data Privacy and Bodily Privacy

The right to privacy has become one of the most contested yet indispensable components of human rights in the digital age. It is not a monolithic concept but rather a multidimensional right that encompasses several aspects of individual autonomy and dignity. Within the Indonesian constitutional framework, Article 28G of the 1945 Constitution guarantees every person's right to protection of personal integrity, family, honor, dignity, and property, while also securing the right to be free from threats of fear to

²² María Tejerizo, "Digital Evidence and Fair Trial Rights at the International Criminal Court," *Leiden Journal of International Law* 36 (2023): 1–21, <https://doi.org/10.1017/S0922156523000031>.

²³ Tareq Al-Billeh, Ali Al-Hammouri, Tawfiq Khashashneh, Mohammed Makhmari, and Hamad Kalbani, "Digital Evidence in Human Rights Violations and International Criminal Justice," *Journal of Human Rights, Culture and Legal System* 4, no. 3 (2024): 842–871, <https://doi.org/10.53955/jhcls.v4i3.446>.

do or not to do something that is a human right.²⁴ This provision, although broad, provides a normative foundation for recognizing privacy as a fundamental right that extends to both personal data and bodily integrity.

Data privacy refers to the protection of personal information from unauthorized access, misuse, or disclosure. In the context of sexual content dissemination, data privacy is implicated when private communications, digital images, or metadata are accessed and distributed without consent.²⁵ Modern information technologies enable intimate data to be stored, replicated, and transmitted in ways that amplify harm to victims once their information is leaked. The 2024 Amendment to the ITE Law acknowledges this risk by affirming that electronic information and documents are admissible as evidence only when lawfully obtained, which implicitly recognizes the individual's right to control their digital data. Internationally, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) reinforces this principle by prohibiting arbitrary or unlawful interference with privacy, family, or correspondence. Thus, data privacy is not merely a technical issue of information security but a substantive human right that demands state protection, especially when judicial processes rely upon sensitive personal data.²⁶

Bodily privacy, by contrast, relates to the sanctity of the individual's physical and sexual integrity. It encompasses the right to control one's body, including decisions about sexual activity and protection against non-consensual observation or recording. In cases of sexual content dissemination, bodily privacy is directly implicated when intimate acts are recorded without consent or when such recordings are shared publicly. The harm in such cases is not limited to reputational damage but extends to violations of autonomy, dignity, and psychological well-being.²⁷ Bodily privacy therefore functions as a shield against gender-based violence, recognizing that the unauthorized exposure of sexual activity constitutes not only a privacy violation but also a form of coercion and exploitation. The

²⁴ Syahwami Syahwami and Hamirul Hamirul, "The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia," *Enigma in Law* 2, no. 2 (2024): 75–84, <https://doi.org/10.61996/law.v2i2.56>.

²⁵ Katina Michael, Shannon Kobran, Roba Abbas, and Salah Hamdoun, "Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals," dalam *2019 IEEE International Symposium on Technology and Society (ISTAS)* (2019): 1–13, <https://doi.org/10.1109/ISTAS48451.2019.8937956>.

²⁶ Oluwatosin Reis, Nkechi Eneh, Benedicta Ehimuan, Anthony Anyanwu, Temidayo Olorunsogo, and Temitayo Abrahams, "Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement," *International Journal of Applied Research in Social Sciences* 6, no. 1 (2024): 73–88, <https://doi.org/10.51594/ijarss.v6i1.733>.

²⁷ Michael Friedewald, Rachel Finn, and David Wright, "Seven Types of Privacy," dalam *Privacy and Identity Management*, Lecture Notes in Computer Science (Springer, 2013), 3–32, https://doi.org/10.1007/978-94-007-5184-2_1.

Indonesian legal system, while often addressing such cases through the ITE Law, must also interpret these violations in light of broader human rights principles that prohibit inhumane or degrading treatment.

What makes sexual content dissemination uniquely harmful is the simultaneous violation of both dimensions of privacy. When explicit material is unlawfully circulated, the victim's data privacy is compromised through the loss of control over personal digital information, while bodily privacy is violated by the exposure of intimate aspects of their physical identity. This dual infringement magnifies the impact, creating a form of "digital victimization" that transcends traditional understandings of privacy breaches.²⁸ The combination of these violations illustrates why courts must interpret privacy rights holistically, ensuring that legal protections extend not only to abstract data but also to the lived reality of bodily autonomy.

From a judicial perspective, respecting these dual dimensions of privacy within legal proceedings requires a careful balancing act. Courts must admit electronic evidence to ensure accountability but must simultaneously adopt procedures that minimize the intrusion into victims' rights. This could include sealing sensitive files, anonymizing victims in public records, or conducting closed hearings when intimate materials are involved.²⁹ Although such practices are not yet systematically embedded in Indonesian jurisprudence, they align with international best practices, such as those developed by the European Court of Human Rights, which has consistently ruled that trials must not expose victims to unnecessary humiliation or secondary victimization.

The recognition of privacy as a fundamental right in Indonesia reflects the influence of global human rights norms. The ICCPR, the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), and the jurisprudence of international tribunals collectively emphasize that privacy is central to human dignity, equality, and personal security. By integrating these instruments into domestic reasoning, Indonesian courts can move beyond a narrow application of evidentiary law to a more rights-sensitive adjudication process.³⁰ Such integration would not only strengthen compliance with

²⁸ Martha Mccaughey and Jill Cermele, "Violations of Sexual and Information Privacy: Understanding Dataraid in a (Cyber)Rape Culture," *Violence Against Women* 28, no. 11 (2022): 3955–3976, <https://doi.org/10.1177/10778012211070316>.

²⁹ Radina Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence," *Computer Law & Security Review* 42 (2021): 105575, <https://doi.org/10.1016/j.clsr.2021.105575>.

³⁰ Sri Devina Hutagalung, Dea Ananda P Sitompul, Kezia Priskila Sinaga, Sigar P Berutu, and Alendra, "Analysis of Legal Protection of Women's Human Rights in Indonesia," *International Journal of Politics and Sociology Research* 11, no. 2 (2023): 316–325, <https://www.ijobsor.pelnus.ac.id>.

international obligations but also provide greater coherence in protecting victims of sexual content dissemination.

The right to privacy must be understood through its dual dimensions: data privacy and bodily privacy. The former protects personal digital information from unauthorized use, while the latter safeguards individual autonomy over one's body and sexual identity. In cases of sexual content dissemination, both dimensions are inevitably implicated, producing compounded harm. The challenge for Indonesian courts lies in operationalizing these concepts within evidentiary procedures, ensuring that while electronic evidence is admitted to establish guilt, victims are not further harmed by the judicial process itself. Anchoring legal reasoning in both constitutional guarantees and international human rights norms will be essential in building a jurisprudence that affirms privacy not only as a formal entitlement but as a lived reality deserving of robust protection.

b. Privacy Protection and the Risk of Re-victimization in Judicial Practice

One of the most complex challenges in adjudicating cases of sexual content dissemination lies not merely in the determination of guilt but in ensuring that the judicial process itself does not inflict further harm upon the victim. The principle of privacy protection must therefore extend beyond the recognition of rights in abstract terms and into the very procedures of trial. When courts admit electronic evidence containing intimate or sexually explicit material, the risk of re-victimization becomes acute.³¹ Re-victimization refers to the phenomenon in which victims of crime suffer additional psychological, social, or legal harms as a result of the way their cases are handled by the justice system. In sexual content cases, the judicial process may inadvertently reproduce the trauma of exposure that the unlawful dissemination itself created.

In the Indonesian context, the 2024 Second Amendment to the ITE Law provides a legal foundation for the admissibility of electronic evidence, yet it offers limited procedural safeguards for handling sensitive content. This normative gap must be understood in light of the fact that the Pandeglang District Court Decision No. 71/Pid.Sus/2023/PN Pdl was rendered prior to the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). At the time of the decision, there was no explicit statutory basis mandating protective mechanisms such as closed hearings to safeguard personal data. From a contemporary

³¹ Afisa Afisa, Zuly Qodir, Akhmad Habibullah, and Unggul Sugiharto, "Analysis of the ITE Law on Digital Rights and Democratic Values in Indonesia," *The Journal of Society and Media* 8, no. 2 (2024): 424–444, <https://doi.org/10.26740/jsm.v8n2.p424-444>.

analytical perspective, however, Article 64 paragraphs (3) and (4) of the PDP Law now clearly recognize electronic information and/or documents containing personal data as valid evidence and allow court proceedings to be conducted in closed sessions where necessary to protect such data. Nevertheless, in the Pandeglang case, although the court accepted WhatsApp conversations and Instagram screenshots as lawful evidence, it did not articulate measures to prevent re-traumatization of the victim. This illustrates that, prior to the PDP Law, privacy protection in evidentiary proceedings was largely dependent on judicial discretion, and even under the current framework, its effective implementation remains a critical issue.

From a human rights perspective, privacy protection in judicial practice is inseparable from the guarantee of a fair trial. International jurisprudence, particularly from the European Court of Human Rights (ECHR), has emphasized that the fairness of a trial must be assessed not only in terms of evidentiary balance but also in terms of whether the procedure respects the dignity and integrity of participants. In cases involving sexual violence or intimate recordings, this has meant adopting privacy-sensitive measures such as closed hearings, redaction of sensitive materials, or limitations on public reporting. These measures aim to strike a balance: ensuring that evidence necessary to establish guilt is considered by the court while minimizing the risk that victims are subjected to further public exposure.

The Indonesian judiciary has yet to institutionalize such safeguards. Judges may occasionally order in-camera hearings for cases involving minors or state security, but the procedural rules do not explicitly require protective measures in cases of non-consensual sexual recordings. This gap is critical because it leaves victims vulnerable to systemic re-victimization. Scholars have pointed out that revictimization often manifests in subtle but damaging ways: victims may be forced to recount their trauma in detail multiple times, subjected to invasive cross-examination, or see their intimate images treated as ordinary exhibits rather than sensitive materials requiring special handling.³² Each of these practices undermines not only privacy but also broader commitments to gender equality and non-discrimination.

The risk of re-victimization is compounded by the digital permanence of evidence. Unlike traditional physical evidence, electronic evidence such as screenshots or videos can

³² International Commission of Jurists (ICJ), “Indonesia: Law No. 12 of 2022 on Sexual Violence Crimes and Online Gender-Based Violence Against Women,” September 1, 2023, https://www.icj.org/wp-content/uploads/2023/09/Briefing-Paper-on-OGBV_ENG.pdf.

be easily copied, stored, or leaked outside of court. If not handled with strict safeguards, sensitive materials may circulate beyond the courtroom, amplifying harm and making judicial proceedings themselves a vector of further privacy violations.³³ This underscores the importance of digital forensic protocols not only for establishing authenticity but also for ensuring secure handling and storage of evidence. The absence of such protocols in Indonesia heightens both legal and ethical risks.

Another dimension relates to societal stigma. In many cultural contexts, including Indonesia, victims of sexual content dissemination may already face social blame or ostracization. The prospect of having their case adjudicated in open court, with explicit details entered into public records, can deter victims from pursuing justice at all. This creates a chilling effect, where the fear of re-victimization through the legal process itself leads to underreporting and impunity for perpetrators. Privacy protection, therefore, is not only a matter of individual dignity but also of systemic justice: without adequate safeguards, the legal system fails to provide meaningful remedies for victims, undermining both deterrence and accountability.

To address these risks, judicial practice must evolve toward a rights-sensitive evidentiary framework. First, courts should adopt clear guidelines for handling intimate electronic evidence, including the possibility of closed hearings when necessary. Second, sensitive evidence should be sealed or redacted in court records to prevent public dissemination. Third, victims should be granted procedural accommodations, such as the right to testify remotely or through intermediaries, to minimize retraumatization. These measures would not weaken the probative force of evidence; rather, they would ensure that its use in court is consistent with constitutional protections of privacy and dignity.

Comparative experience offers valuable lessons. For example, in Canada and several European jurisdictions, “rape shield laws” restrict the admissibility of evidence relating to a victim’s sexual history or behavior, recognizing the potential for re-victimization. While Indonesia’s legal system has not adopted analogous statutes, the underlying principle, limiting evidentiary practices that expose victims to undue harm, could inform judicial discretion under the ITE Law. Similarly, international human rights law, particularly Article 2 and Article 17 of the ICCPR, obliges states not only to prohibit unlawful interference with privacy but also to ensure effective remedies when such rights are

³³ Erin Kenneally and Christopher Brown, “Risk Sensitive Digital Evidence Collection,” *Digital Investigation* 2, no. 2 (2005): 101–119, <https://doi.org/10.1016/j.diin.2005.02.001>.

violated. Ensuring privacy protection within judicial processes is therefore not discretionary but a legal obligation under Indonesia's international commitments.

In terms of doctrine, the principle of proportionality provides a normative anchor. Admitting electronic evidence in cases of sexual content dissemination is often necessary to establish guilt, but the extent of disclosure must be proportionate to the legitimate aim pursued. Courts must therefore weigh the evidentiary value of explicit materials against the harm caused by their exposure. In some cases, the probative purpose may be satisfied by metadata, expert testimony, or limited excerpts, rather than by full public display of sensitive recordings. This proportionality analysis ensures that the pursuit of justice does not come at the expense of victims' rights.

Ultimately, the challenge lies in bridging the gap between *das sollen* and *das sein*. *Das sollen*, embodied in the constitutional guarantee of privacy and the provisions of the 2024 ITE Law, mandates that electronic evidence be both valid and rights-sensitive. *Das sein*, however, reveals that judicial practice often defaults to a utilitarian approach, prioritizing evidentiary sufficiency over the lived experiences of victims. The Pandeglang decision demonstrates partial progress in emphasizing authenticity and consent but also underscores the absence of a systematic framework for protecting privacy in trial. Closing this gap requires both doctrinal innovation and institutional reform.

Privacy protection and the prevention of re-victimization are not peripheral concerns but central obligations of the justice system in handling cases of sexual content dissemination. Courts must move beyond formal admissibility toward practices that safeguard dignity, autonomy, and equality. Without such reforms, judicial processes risk reproducing the very harms they are meant to redress. Embedding privacy-sensitive procedures into evidentiary law will therefore be essential to ensuring that the promise of justice in the digital age does not translate into renewed suffering for victims.

D. Conclusion

This study demonstrates that Indonesia has normatively established a strong legal framework recognizing electronic evidence as valid and binding, particularly through the ITE Law and its 2024 amendment, which is further reinforced by the enactment of Law No. 20 of 2025 on the New Criminal Procedure Code and Law No. 27 of 2022 on Personal Data Protection. These developments signify that, under the current legal regime, electronic evidence is no longer contested in terms of admissibility, as it is explicitly recognized as a legitimate means of proof within the evidentiary system. However, the analysis of the

Pandeglang District Court Decision No. 71/Pid.Sus/2023/PN Pdl remains relevant from a retrospective and analytical perspective, given that the case was decided prior to the enactment of both the PDP Law and the New *KUHAP*. The decision illustrates that, while courts were able to accept and rely on electronic evidence in accordance with the ITE Law, the protection of privacy, particularly in cases involving sensitive sexual content, was not yet systematically integrated into judicial practice. This reveals a clear gap between *das sollen* and *das sein*, where evidentiary validity was prioritized over victim protection. Therefore, although the study of electronic evidence in this verdict is no longer relevant in light of the current legal framework, it remains as a critical juridical reflection, highlighting the necessity for courts to operationalize privacy safeguards, such as closed hearings, anonymization, and proportional use of evidence, so that the use of electronic evidence in the digital era not only ensures legal certainty but also upholds human dignity and fundamental rights.

References

Books

Harkrisnowo, *et al.*, *Law and Justice in a Globalized World: Proceedings of the Asia-Pacific Research in Social Sciences and Humanities, Depok, Indonesia, 7–9 November 2016: Topics in Law and Justice*, London: CRC Press/Balkema Taylor & Francis Group, 2018.

Indonesia Judicial Research Society, Maharani, Marsha, Inatsan Ashila, Bestha, Ismaya, Siti, Assyifa, Aisyah, Wicaksana, Dio Ashar, Barus, Naomi Rehulina, dan Nasir, Muhammad Ad'har, *The Role of Legal Empowerment by the Community in Strengthening Access to Justice for Women in Conflict with the Law in Indonesia*, Jakarta: Indonesia Judicial Research Society, 2023.

Muhaimin, *Metode Penelitian Hukum*, Mataram: Mataram University Press, 2020.

Riyadi, Eko, "Institutionalization of Human Rights Standards in Indonesia," dalam Tømte, Aksel, dan Riyadi, Eko (eds.), *International Human Rights and Local Courts: Human Rights Interpretation in Indonesia*, Abingdon, Oxon; New York: Routledge, 2024.

Smits, Jan M., "What is Legal Doctrine? In the Aims and Methods of Legal-Dogmatic Research," dalam van Gestel, R., Micklitz, H., dan Rubin, E. L. (eds.), *Rethinking Legal Scholarship*, Cambridge: Cambridge University Press, 2017.

Journal Articles

Afisa, Afisa, Zuly Qodir, Akhmad Habibullah, and Unggul Sugiharto, "Analysis of the ITE Law on Digital Rights and Democratic Values in Indonesia," *The Journal of Society and Media* 8, no. 2 (2024): 424–444, <https://doi.org/10.26740/jsm.v8n2.p424-444>.

Al-Billeh, Tareq, Ali Al-Hammouri, Tawfiq Khashashneh, Mohammed Makhmari, and Hamad Kalbani, "Digital Evidence in Human Rights Violations and International Criminal

- Justice,” *Journal of Human Rights, Culture and Legal System* 4, no. 3 (2024): 842–871, <https://doi.org/10.53955/jhcls.v4i3.446>.
- Ariansyah, and Lucky Eka Khalis Aulia ES, “Reconstruction of the Position of Electronic Documents as Evidence in Civil Case Evidence Based on Deep Ecology,” *Judex Laguens* 3, no. 1 (2025): 95–112, <https://doi.org/10.25216/ikahi.3.1.4.2025.95-112>.
- Balkibayeva, Zhanagul, “Problems of Admissibility and Reliability of Metadata as Evidence,” *International Journal of Law and Policy* 2 (2024): 48–58, <https://doi.org/10.59022/ijlp.232>.
- Dewi, Erna, “The Problems of Sexual Consent in Colleges Environment,” *Migration Letters* 21, no. S3 (2024): 1376–1382, <https://migrationletters.com/index.php/ml/article/view/7474>.
- Friedewald, Michael, Rachel Finn, and David Wright, “Seven Types of Privacy,” dalam *Privacy and Identity Management, Lecture Notes in Computer Science* (Springer, 2013), 3–32, https://doi.org/10.1007/978-94-007-5184-2_1.
- Haetami, Enden, “The Strength of Electronic Evidence in the View of Islamic Law,” *International Journal of Science and Society* 4, no. 4 (2023): 666–675, <https://doi.org/10.54783/ijsoc.v4i4.615>.
- Huang, Yage, “Authenticating Social Media Evidence in Chinese Criminal Procedure Law—A Comparative Study,” *Indiana Journal of Global Legal Studies* 31, no. 2 (2024): 45–49, <https://www.repository.law.indiana.edu/etd>.
- Hutagalung, Sri Devina, Dea Ananda P Sitompul, Kezia Priskila Sinaga, Sigar P Berutu, and Alendra, “Analysis of Legal Protection of Women’s Human Rights in Indonesia,” *International Journal of Politics and Sociology Research* 11, no. 2 (2023): 316–325, <https://www.ijobsor.pelnus.ac.id>.
- Kenneally, Erin, and Christopher Brown, “Risk Sensitive Digital Evidence Collection,” *Digital Investigation* 2, no. 2 (2005): 101–119, <https://doi.org/10.1016/j.diin.2005.02.001>.
- Kohl, Uta, “The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy,” *International and Comparative Law Quarterly* 72, no. 3 (2023): 737–769, <https://doi.org/10.1017/S0020589323000258>.
- Lasaka, Mustalim, “Ius Constituendum of Electronic Evidence Arrangement in Criminal Procedure Law,” *Jurnal Legalitas* 16, no. 2 (2023): 154–166, <https://doi.org/10.33756/jelta.v16i2.20306>.
- Mccaughey, Martha, and Jill Cermele, “Violations of Sexual and Information Privacy: Understanding Dataraid in a (Cyber)Rape Culture,” *Violence Against Women* 28, no. 11 (2022): 3955–3976, <https://doi.org/10.1177/10778012211070316>.
- Michael, Katina, Shannon Kobran, Roba Abbas, and Salah Hamdoun, “Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals,” dalam *2019 IEEE International Symposium on Technology and Society (ISTAS)* (2019): 1–13, <https://doi.org/10.1109/ISTAS48451.2019.8937956>.

- Moussa, Ahmed, “Electronic Evidence and Its Authenticity in Forensic Evidence,” *Egyptian Journal of Forensic Sciences* 11 (2021): 20, <https://doi.org/10.1186/s41935-021-00234-6>.
- Muhtar, Abdul Kadir Zaylani, Muh. Risnain, dan Zunnuraeni, “The Right to Life Based on The International Covenant on Civil And Political Rights And Its Application In Indonesian National Law,” *Mataram Journal of International Law* 2, no. 2 (2024): 125–144, <https://doi.org/10.29303/majil.v2i2.5031>.
- Muzakkir, and Taufik Hidayat, “Juridical Review Article 27A of Law Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Information and Electronic Transactions,” *Jurnal Hukum Samudra Keadilan* 19, no. 2 (2025): 238–249, <https://doi.org/10.33059/jhsk.v19i2.10650>.
- Putri, Ni Made Diana Kencana, “Analysis of Recognition from the Perspective of International Law and Implementation of Public Policies in Indonesia and Myanmar,” *Focus Journal Law Review* 3, no. 2 (2023), <https://doi.org/10.62795/fjl.v3i2.226>.
- Reis, Oluwatosin, Nkechi Eneh, Benedicta Ehimuan, Anthony Anyanwu, Temidayo Olorunsogo, and Temitayo Abrahams, “Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement,” *International Journal of Applied Research in Social Sciences* 6, no. 1 (2024): 73–88, <https://doi.org/10.51594/ijarss.v6i1.733>.
- Saputra, Aga Naya, and Ghina Salsabila Aven, “Legal Analysis of the Use of Electronic Evidence in Providing Evidence in Corruption Cases (Decisions in Indonesia),” *Legal Brief* 14, no. 3 (2025): 764–773, <https://doi.org/10.35335/legal.v14i3.1410>.
- Setyawan, Adisti Puspa, Antonius Sambodo Adi A, I Dewa B S Wirantaya, Pina Mustika, and William Gomarga, “Indonesia’s Electronic Information and Transactions Law: History, Impact, and Challenges,” *Journal Research of Social Science, Economics, and Management* 4, no. 12 (2025): 2154–2165, <https://doi.org/10.59141/jrssem.v4i12.899>.
- Stoykova, Radina, “Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence,” *Computer Law & Security Review* 42 (2021): 105575, <https://doi.org/10.1016/j.clsr.2021.105575>.
- Syahwami, Syahwami, and Hamirul Hamirul, “The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia,” *Enigma in Law* 2, no. 2 (2024): 75–84, <https://doi.org/10.61996/law.v2i2.56>.
- Tejerizo, María, “Digital Evidence and Fair Trial Rights at the International Criminal Court,” *Leiden Journal of International Law* 36 (2023): 1–21, <https://doi.org/10.1017/S0922156523000031>.
- Yaskur, Fajar, and Ifahda Pratama Hapsari, “The Existence of Sexual Violence Crime in Indonesia,” *JUSTISI* 11, no. 1 (2024): 95–110, <https://doi.org/10.33506/js.v11i1.3748>.

Internet

International Commission of Jurists (ICJ), “Indonesia: Law No. 12 of 2022 on Sexual Violence Crimes and Online Gender-Based Violence Against Women,” September 1, 2023, https://www.icj.org/wp-content/uploads/2023/09/Briefing-Paper-on-OGBV_ENG.pdf.

Law Commission, “Evidence in Sexual Offences Prosecutions: Consultation Paper 259,” May 15, 2023, <https://www.lawcom.gov.uk/project/evidence-in-sexual-offence-prosecutions/>.

Pengadilan Negeri Pandeglang, “Putusan Nomor 71/Pid.Sus/2023/PN Pdl,” 2023, <https://putusan3.mahkamahagung.go.id/direktori/putusan/zaee3fd389af4eac9787313033333437.html>.

Vasiliev, Sergey, “The Role and Legal Status of the Prosecutor in International Criminal Trials,” November 26, 2010, <https://doi.org/10.2139/ssrn.1715465>.