International Journal of Human Research and Social Science Studies

ISSN(p): 3050-547X, ISSN(e): 3050-5488

Volume 03 Issue 04 April, 2026

DOI: https://doi.org/10.55677/ijhrsss/07-2026-Vol03I04

Page No : 259-271

Reformulating the Ethics of Attorney-Client Privilege from The Perspective of Personal Data Protection in The Digital Age

Irhammudin[1], Muhammad Djatmiko[2]

[1,2] Faculty of Law, Universitas Muhammadiyah Kotabumi, Lampung, Indonesia.

ABSTRACT: The development of digital technology has brought fundamental changes to the practice of the legal profession, particularly in the management and protection of client information. This transformation poses serious challenges to the principle of attorney-client privilege, which has long been the foundation of the relationship of trust between attorneys and clients. On the one hand, positive law and professional ethics in Indonesia explicitly require attorneys to maintain client confidentiality. On the other hand, the digitization of legal practice—through the use of electronic storage, online communication, and smart legal technology-expands the risk of data breaches that are not fully accommodated within the current framework of professional ethics. This situation highlights a normative gap between the attorney-client privilege and the dynamics of digital data protection. This study aims to analyze the concept of attorney-client confidentiality from the perspectives of legal professional ethics and personal data protection law, as well as to formulate the need for a reformulation of attorney confidentiality ethics that is adaptive to the digital era. This study employs a normative legal research method using legislative, conceptual, and comparative legal approaches. Legal materials were obtained through a literature review of legislation, professional codes of ethics, scholarly literature, and the practice of regulating lawyer's professional ethics in several other jurisdictions. The analysis was conducted qualitatively using systematic and prescriptive legal reasoning. The results of the study indicate that the regulation of attorney confidentiality in Indonesia remains oriented toward conventional legal practices and has not explicitly addressed attorney's digital responsibilities in protecting client data. The absence of clear regulations regarding technological competence and data security has the potential to weaken client confidentiality protections and create normative uncertainty for attorneys. This study emphasizes that attorneys' confidentiality obligations in the digital age must be understood as multidimensional obligations encompassing ethical, legal, and technological aspects. A reformulation of the legal profession's ethics must integrate the principles of digital confidentiality, technological competence, and data accountability to align with personal data protection regimes and developments in legal technology. With these updates, the legal profession is expected to maintain its integrity and public trust amidst the digital transformation of legal practice.

Corresponding Author:
Muhammad Djatmiko

Published Online:
April 22, 2026

KEYWORDS:
lawyers, professional confidentiality, legal professional ethics, personal data protection, digitization of legal practice.

Cite the Article: *Irhammudin, Djatmiko, M. (2026). Reformulating the Ethics of Attorney-Client Privilege from The Perspective of Personal Data Protection in The Digital Age. International Journal of Human Research and Social Science Studies, 3(4),259-271. https://doi.org/10.55677/ijhrsss/07-2026-Vol03I04*

1. INTRODUCTION

The legal profession occupies a strategic position within the judicial system as it serves as a bridge between individual interests and the mechanisms of law enforcement. In fulfilling this role, lawyers are burdened with ethical and legal obligations to maintain client confidentiality as the cornerstone of the professional relationship. Confidentiality is not merely a moral obligation but an institutional

prerequisite that enables clients to disclose facts and their interests honestly without fear of misuse of information. Without a guarantee of confidentiality, trust in the legal profession will erode, and ultimately undermine the legitimacy of the judicial system itself (Lubis et al., 2025).

In the context of Indonesian law, the attorney-client privilege has long been recognized and institutionalized through the Law on Attorneys and the Indonesian Code of Ethics for Attorneys. These provisions affirm that all information obtained by an attorney from a client through a professional relationship must be kept confidential. This normative formulation reflects the classical view that confidentiality is an inherent part of a lawyer's fiduciary duty to the client (Khairun et al., 2025). For years, this interpretation was relatively adequate because legal practice still relied on physical documents and direct communication, where risks could be personally controlled.

However, the development of digital technology has fundamentally changed the way attorneys work and manage client information (Setiarma, 2023). The use of electronic storage, online communication, cloud-based services, and smart legal technology has become an integral part of modern legal practice (Rafid & Nurita, 2025). This digitalization brings efficiency and convenience, but simultaneously expands the spectrum of risks to client confidentiality. Information that was previously stored in a limited manner is now within digital systems involving technological infrastructure and third parties, thereby increasing the potential for data breaches, unauthorized access, and misuse of information (Cindy et al., 2025).

These changes raise serious normative issues, as the ethical framework for the legal profession in Indonesia has not yet fully anticipated the implications of the digitalization of legal practice (Zuhdiantito, 2025). The Indonesian Code of Ethics for Lawyers is still formulated in general terms and oriented toward conventional practices, without providing clear guidance on lawyers' responsibilities in managing and protecting client data digitally *(Implementation of the Code of Professional Ethics for Lawyers in Daily Practice | Das Sollen: Journal of Contemporary Studies on Law and Society, n.d.*). Consequently, there is a gap between the ethical norms binding lawyers and the reality of legal practice, which is becoming increasingly complex and technology-driven.

On the other hand, the existence of a legal regime for personal data protection adds a new dimension to attorneys' confidentiality obligations. The Personal Data Protection Act affirms individuals' rights to the protection of their personal data as well as the obligations of data controllers and processors to ensure the security and accountability of such data management. In their professional relationship with clients, lawyers not only act as legal advisors but also as parties that control and process clients' personal data (Rinaldi et al., 2025). Thus, a breach of client confidentiality has the potential to result in both ethical consequences and public legal consequences.

This situation indicates that the duty of attorney-client confidentiality in the digital age can no longer be narrowly understood as merely a prohibition against disclosing client secrets. Confidentiality must be interpreted more broadly as an active obligation to manage technological risks and ensure comprehensive protection of client data. Without adequate normative reformulation, lawyers risk facing legal and ethical uncertainty in the practice of their profession, while clients' interests do not receive optimal protection.

Based on these issues, this study aims to re-examine the concept of attorney-client privilege from the perspectives of legal professional ethics and personal data protection law. This study seeks to assess the extent to which current regulations on the ethics of the legal profession are capable of addressing the challenges of the digitalization of legal practice, as well as to formulate the need for an update to the ethics of attorney-client confidentiality to align with technological developments and data protection requirements. With this approach, this study is expected to provide theoretical and normative contributions to strengthening the integrity of the legal profession in the digital age.

II. METHOD

This study is designed as a normative legal study focused on a conceptual and evaluative analysis of the duty of confidentiality of the legal profession in the context of the digitization of legal practice and the evolving personal data protection regime. The primary focus of the study is on the examination of legal norms, principles, and doctrines that form the ethical framework of the legal profession, as well as on the ability of these norms to adapt to technological changes that affect how lawyers manage client information (Permana, 2024). Given this nature, this study does not aim to test empirical facts but rather to construct a normative argument regarding the adequacy and relevance of professional ethical regulations in addressing contemporary legal challenges.

A legal framework approach is employed as the initial foundation to examine the normative structure governing the legal profession and personal data protection in Indonesia. The analysis focuses on positive legal provisions that directly or indirectly regulate attorneys' confidentiality obligations, including the Attorney Act, the Indonesian Code of Ethics for Attorneys, and the Personal Data Protection Act. This approach enables the tracing of systemic relationships among norms, while also revealing the limitations of regulations that remain oriented toward conventional legal practice. Through a systematic reading of these regulations, this study identifies a normative gap between generally formulated ethical obligations and the need for client data management in a high-risk digital environment.

To deepen the normative analysis, this study employs a conceptual approach grounded in theoretical frameworks regarding legal professional ethics and personal data protection. This approach is used to examine foundational concepts such as fiduciary duty, confidentiality, professional loyalty, and the evolving concept of an attorney's responsibility in modern legal practice. In the digital

context, the conceptual approach serves to construct a new understanding of attorney confidentiality as a professional obligation that no longer relies solely on personal integrity but also on the ability to manage technological risks. Through this approach, the study formulates a conceptual framework that integrates ethical, legal, and technological dimensions in understanding the attorney's duty of confidentiality.

A comparative legal approach is employed to broaden the analytical perspective and avoid an isolated normative viewpoint. Through this approach, the study compares the ethical regulations governing the legal profession in Indonesia with the evolving practices and guidelines in several other jurisdictions that have already addressed the challenges of the digitalization of legal practice (Tahir et al., 2023). This comparison is not intended to adopt foreign models normatively, but rather to identify general principles that can serve as references in updating the professional ethics of lawyers in Indonesia. The comparative approach functions as an evaluative instrument that illustrates the position of national regulations within the spectrum of global legal professional ethics development.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation and official documents that are legally binding and relevant to attorneys' confidentiality obligations and the protection of personal data. Secondary legal materials include scientific literature, academic works, and reports from legal professional organizations that provide analysis, interpretation, and criticism of primary legal materials. Tertiary legal materials are used sparingly to ensure terminological accuracy and conceptual consistency (Firmanto et al., 2024). All legal materials were collected through a selective and systematic literature review, prioritizing sources with academic authority and direct relevance to the research issue.

The analysis of legal materials was conducted qualitatively using systematic and prescriptive legal reasoning. Legal norms and professional ethics were interpreted by considering the purpose of their establishment as well as the values underlying their regulation. Furthermore, a critical evaluation was conducted regarding the ability of these norms to address the challenges of legal practice in the digital age, particularly concerning the management and protection of client data. This analysis aimed to produce a normative framework that not only explains the existing legal conditions but also provides an argumentative foundation regarding the need for an update to the professional ethics of attorneys.

Using this methodology, this study aims to construct a coherent normative argument grounded in the integration of legal professional ethics theory and personal data protection theory. The approach used enables this study to make a theoretical contribution to the development of research on the ethics of the legal profession, while also offering relevant normative recommendations for updating the ethical regulations on attorney-client privilege to align with technological dynamics and the demands for client interest protection in the digital age.

III. RESULTS AND DISCUSSION

Attorney-Client Confidentiality as a Fiduciary Principle in the Legal Profession

Confidentiality is a fundamental principle that shapes the identity of the legal profession and serves as the foundation of the professional relationship between attorneys and clients (ADV.Dr.Maysarah.SH.MH et al., 2025). In legal practice, a client's openness toward an attorney can only be realized if there is a guarantee that all information provided will be protected and not used outside the interests of legal defense. Therefore, confidentiality cannot be viewed merely as an administrative obligation, but rather as an ethical prerequisite that enables the attorney's role to function effectively within the judicial system.

The attorney-client relationship is unique because it is built upon an information imbalance and a power dynamic. Clients are often in vulnerable situations—legally, economically, or psychologically—and thus heavily rely on the attorney's expertise and integrity. In such circumstances, attorneys gain access to information that is highly personal, strategic, and even potentially harmful to the client if disclosed to third parties. Confidentiality serves as a protective mechanism against such vulnerabilities, while also ensuring that attorneys will not abuse their professional position (Fisher, 2008).

From a professional ethics perspective, the duty to maintain confidentiality is rooted in the concept of fiduciary duty. The fiduciary principle positions the attorney as a trusted party acting in the client's best interests, setting aside personal interests or those of third parties (Jorgenson et al., 1997). This duty encompasses loyalty, good faith, diligence, and the protection of client information. Thus, a breach of confidentiality is not only a violation of ethical norms but also a betrayal of the trust that forms the foundation of the professional relationship (Dewanti & Lewoleba, 2025).

It is necessary to make a conceptual distinction between moral obligations, ethical obligations, and legal obligations in the context of attorney-client privilege (M.Hum, 2023). Moral obligations are rooted in the values of honesty and personal integrity of the attorney as an individual. Ethical obligations are reflected in professional norms that govern the standards of conduct for attorneys as members of a professional corps. Meanwhile, legal obligations stem from laws and regulations that impose formal sanctions if these obligations are violated. These three layers of obligations are interrelated and form a unified set of norms that govern the practice of the legal profession.

In the context of a rule-of-law state, the existence of the duty of confidentiality also has a public interest dimension. A fair and effective judicial system requires optimal legal representation (Meliana, 2025). Optimal representation can only be achieved if the client is willing to disclose all relevant facts and information to the attorney without fear. If confidentiality is not guaranteed, clients

tend to withhold information or provide incomplete statements, which ultimately undermines the legal enforcement process itself. Thus, attorney-client privilege not only protects the individual interests of the client but also supports the functioning of the judicial system as a whole (McCarty et al., 2023).

Confidentiality also plays a crucial role in maintaining the social legitimacy of the legal profession. The legal profession earns public trust not merely through mastery of positive law, but through its ability to uphold high ethical standards. Lawyers are regarded as a respected profession because they are trusted to keep clients' secrets, even in high-pressure situations or conflicts of interest. When a breach of confidentiality occurs, the impact is not limited to the relationship between the attorney and the client but can damage the collective image of the profession.

In practice, the fiduciary principle requires attorneys to be proactive in protecting client information (Rauzi & Suriadiata, 2024). This duty is not passive or reactive; rather, it requires attorneys to take reasonable and proportionate steps to prevent unauthorized disclosure. The principle of due diligence is a crucial element, as negligence in maintaining confidentiality— even without malicious intent—can still be classified as a breach of professional duty.

Furthermore, the concept of fiduciary duty also emphasizes that confidentiality cannot be negotiated based solely on convenience or efficiency. In the face of modern practice pressures, such as demands for speed, cost efficiency, or the use of technology, attorneys remain obligated to ensure that the principle of confidentiality is not compromised (PRATOMO, 2025). In other words, innovation in legal practice must always be situated within the framework of protecting clients' interests as the top priority.

From a theoretical perspective, attorney-client privilege reflects a balance between private and public interests. On the one hand, the state has an interest in uncovering the truth and enforcing the law. On the other hand, the state also has an interest in guaranteeing everyone's right to an effective legal defense. Attorney-client privilege serves as the meeting point between these two interests, providing a safe space for clients to communicate honestly with their legal counsel (Kushwaha et al., 2024).

Thus, attorney-client privilege as a fiduciary principle cannot be reduced merely to a formal obligation listed in codes of ethics or laws. This principle constitutes the moral and structural core of the legal profession, determining the quality of professional relationships, the effectiveness of legal defense, and the level of public trust in the judicial system. A strong understanding of the essence of this confidentiality serves as a crucial foundation for analyzing the new challenges arising from digital transformation in legal practice.

The Transformation of the Concept of Attorney-Client Confidentiality in the Digital Age

Advances in information technology have brought fundamental changes to how the legal profession conducts its practice. Whereas in the past, case management was synonymous with physical files, locked archives, and face-to-face communication, contemporary legal practice increasingly relies on electronic systems. Case documents are now stored in digital formats, communication takes place via email and instant messaging apps, and professional coordination occurs through online platforms. This transformation not only alters the technical aspects of an attorney's work but also directly impacts the meaning and application of the client confidentiality principle (Muhamad et al., 2025).

The shift from physical archives to electronic systems carries significant implications for the management of client information (Azahra & Putra, 2024). Physical archives have inherent access limitations, as they require physical presence and relatively easy-to-monitor spatial control. Conversely, digital systems enable remote access, rapid data replication, and integration with various devices and third-party services. These conditions enhance the efficiency of lawyers' work, yet simultaneously expand the potential risks of data breaches, whether due to human error or systematic cyberattacks (MM, 2025).

In the digital context, threats to confidentiality no longer stem solely from intentional acts but also from technical oversights and weak information system governance. Security configuration errors, the use of weak passwords, sending documents to the wrong address, or using personal devices for professional purposes are examples of risks that frequently occur in daily practice. These risks indicate that protecting confidentiality in the digital age requires a more comprehensive approach than merely individual ethical commitments (Rabiu et al., 2025).

Reliance on technology service providers is also a critical issue in the transformation of attorney confidentiality. Cloud-based storage, case management software, and online communication applications are generally managed by third parties beyond the attorney's direct control (Khan, 2023). Although these services offer convenience and efficiency, attorneys remain professionally responsible for the security of client data processed through these systems. This raises normative questions regarding the extent to which attorneys can delegate the management of sensitive information to others without compromising their duty of confidentiality.

These changes are driving a paradigm shift in understanding professional confidentiality. In the classical model, confidentiality relied heavily on the personal integrity of the attorney as an individual. Personal honesty, loyalty, and diligence were the primary keys to protecting client secrets. However, in technology-based practice, individual integrity alone is no longer sufficient. Confidentiality is now also determined by the reliability of the systems, procedures, and digital infrastructure used in professional practice.

This shift can be understood as a transition from personal trust to system-based trust. Clients not only trust the attorney as an individual, but also implicitly trust the technological systems used by that attorney (Davidson et al., 2022). This trust includes the assumption that client data is stored securely, accessed only by authorized parties, and protected from misuse (Munawarah et al.,

2025). If the system fails to meet these assumptions, client trust may collapse, even if the attorney personally has no malicious intent.

In this context, failures in digital systems can have ethical implications just as serious as intentional breaches of confidentiality. Data breaches resulting from cyberattacks, for example, still result in harm to clients and damage the reputation of the legal profession. Therefore, an ethical approach that focuses solely on the individual behavior of attorneys is insufficient to address the challenges of the digital age. Professional ethics must account for the technological dimension as part of the scope of professional responsibility (Cox, 2022).

Digital transformation also blurs the boundaries between a lawyer's professional and private spheres. The use of personal devices for work purposes, remote work, and high mobility in legal practice result in client data potentially being scattered across various devices and networks (Kurniawan et al., 2025). This situation complicates the monitoring and control of access to sensitive information. Without clear internal policies and disciplined use of technology, the risk of confidentiality breaches increases.

On the other hand, digitization also creates new expectations regarding the professionalism of attorneys. Modern clients expect legal services that are fast, efficient, and integrated with technology. However, these demands for efficiency must not come at the expense of the principle of confidentiality. The primary challenge for lawyers is finding a balance between leveraging technology and protecting clients' interests. This balance requires lawyers to critically assess technological risks and implement proportionate preventive measures.

The transformation of the concept of confidentiality in the digital age ultimately underscores that a lawyer's obligations are no longer limited to passively safeguarding secrets. Lawyers are required to actively manage risks, understand the characteristics of the technologies used, and ensure that their professional practices align with data protection principles (Bayya, 2022). Confidentiality has become a dynamic responsibility, evolving alongside technological advancements and new work patterns within the legal profession.

Thus, changes in the technological landscape have expanded the meaning of attorney confidentiality from a mere individual ethical obligation to a systemic obligation that encompasses technology governance. Understanding this transformation is a crucial foundation for assessing the adequacy of existing ethical regulations and for formulating the need to update the norms of the legal profession so that they remain relevant and effective in the digital age.

The Indonesian Code of Ethics for Lawyers and Its Limitations in the Digital Context

The Indonesian Code of Ethics for Lawyers is the primary normative instrument governing the standards of conduct for lawyers in the practice of their profession. It embodies the fundamental values of the legal profession, such as independence, loyalty, integrity, and confidentiality. The duty to maintain client confidentiality is explicitly formulated as one of the pillars of professional ethics, affirming that a lawyer must not disclose anything learned from a client due to their professional relationship. This formulation reflects the classical view of confidentiality as a personal obligation inherent to the attorney as an individual.

Normatively, the confidentiality provisions in the Indonesian Code of Ethics for Lawyers serve a strong protective function. They provide an ethical foundation for lawyers to resist pressure from external parties—including law enforcement officials or non-client interests—seeking to obtain confidential information. In this context, confidentiality is positioned as both a right and an obligation of the attorney, serving to protect the client's interests and uphold the dignity of the profession. However, this formulation emerged within a legal practice context still dominated by analog systems and has not yet accounted for the complexities of information management in the digital age.

One of the main limitations of the Indonesian Code of Ethics for Lawyers is the absence of explicit provisions regarding lawyers' responsibilities in managing electronic data (Rosdiana et al., 2025). The code of ethics does not provide guidance on data security standards, the use of information technology, or obligations regarding digital risk mitigation. Consequently, the duty of confidentiality is narrowly interpreted as a prohibition against intentionally disclosing information, without accounting for potential breaches resulting from technical negligence or system failures. In modern practice, such forms of breaches are becoming increasingly prevalent and have far-reaching consequences.

The absence of norms regarding digital responsibility also creates uncertainty in the enforcement of professional ethics. The Bar Council faces difficulties in assessing whether a data breach incident resulting from hacking or a system error can be classified as an ethical violation (Imelda et al., 2024). Without clear standards, assessments tend to rely on subjective interpretations, which could lead to inconsistencies in the enforcement of professional discipline. This situation weakens the role of the code of ethics as an instrument for regulating professional conduct.

Furthermore, the Indonesian Advocates' Code of Ethics has not yet incorporated technological competence as a component of an advocate's professionalism. The focus of professional ethics remains on mastery of substantive and procedural law, while the ability to understand technological risks is not positioned as a key element of competence (Adams et al., 2024). In fact, in digital-based practice, a lack of technological knowledge can cause serious harm to clients. Lawyers who use electronic systems without understanding their security implications risk breaching their duty of care, even if they have no intention of disclosing client secrets (Nasution & Husein, 2025).

These limitations indicate that the Indonesian Code of Ethics for Lawyers still reflects a conservative approach to professional

ethics. Ethics is understood as a static set of prohibitions and obligations, rather than as a normative framework that adapts to social and technological changes. In this context, professional ethics lags behind the reality of increasingly digitized legal practice. Consequently, a gap exists between the prevailing ethical norms and the factual challenges faced by attorneys in their daily practice. From a normative perspective, this gap can be characterized as a regulatory void (normative gap). Lawyers are ethically and legally obligated to maintain client confidentiality, but they are not provided with adequate guidelines on how to fulfill this obligation in a digital environment. This gap has the potential to place lawyers in a vulnerable position, as they may be held accountable for breaches of confidentiality without having clear operational standards to guide their professional conduct.

Furthermore, the limitations of the Indonesian Code of Ethics for Lawyers also impact client protection. Clients generally lack the capacity to assess the extent to which the technological systems used by attorneys are secure and reliable. They place their full trust in legal professionals, assuming that attorneys have taken the necessary steps to protect their data. If the code of ethics does not mandate minimum digital protection standards, clients' interests risk not being optimally protected (Bazla et al., 2024).

From the perspective of the evolution of global professional ethics, current trends point to a shift toward risk-based ethics and systemic accountability. Professional ethics no longer merely regulate individual behavior but also require the profession to manage risks arising from the use of technology and modern work organizations ((, n.d.). Compared to these developments, the Indonesian Code of Ethics for Lawyers remains oriented toward a traditional ethical model that is less responsive to digital dynamics.

Therefore, the need to update the Indonesian Code of Ethics for Lawyers has become increasingly urgent. This update is not intended to replace the profession's core values, but rather to expand and adapt them to the context of contemporary legal practice. Confidentiality remains a core principle, but it must be interpreted more broadly, encompassing obligations regarding electronic data management, information system security, and attorneys' technological competence.

An analysis of the limitations of the Indonesian Code of Ethics for Lawyers serves as a crucial foundation for further discussions regarding the role of lawyers within the personal data protection regime. With the existence of general and legally binding data protection regulations, lawyers are no longer merely subject to internal ethical norms but also face public legal obligations demanding higher accountability in the management of client data.

Attorneys as Controllers and Processors of Personal Data in Professional Practice

Developments in personal data protection regulations have significant implications for the practice of the legal profession. In the context of the attorney-client relationship, nearly all professional activities involve the processing of personal data, including sensitive data. Identity information, legal history, financial status, business strategies, and even personal facts relevant to the case are an integral part of a lawyer's work. Therefore, lawyers effectively occupy a strategic position as the party controlling and processing clients' personal data.

The lawyer's role as a data controller can be understood through their authority to determine the purposes and methods of processing client data. Lawyers decide what data is collected, how that data is used in legal defense, to whom the data may be disclosed, and how long the data is retained. In modern practice, this authority also encompasses the selection of technological tools used to store and process data, including the use of third-party services such as cloud storage or case management software. Thus, a lawyer's responsibility does not end with the legal substance of a case but extends to the governance of clients' personal data (Candra, 2025).

This position carries significant legal consequences. Violations of client data security can no longer be viewed merely as breaches of internal professional ethics but also as violations of public legal obligations (Putri et al., 2026). Data breaches, unauthorized access, or the use of data beyond agreed-upon purposes have the potential to give rise to legal liability, whether in the form of administrative sanctions or claims for damages. In this context, attorneys face the potential for dual liability: ethical liability before the professional organization and legal liability before the state.

This situation creates complex normative challenges. On the one hand, lawyers are bound by an absolute duty of professional confidentiality to protect their clients' interests. On the other hand, the personal data protection regime demands transparency, accountability, and compliance with data processing principles. The tension between these two regimes arises, for example, when there is an obligation to report data breach incidents to authorities or data subjects. Lawyers must navigate these obligations without violating the principle of confidentiality that is central to their profession.

In practice, harmonizing confidentiality obligations with data protection requires an integrative approach (Waruwu & Siswoyo, 2024). Professional confidentiality cannot be used as an excuse to disregard data security obligations, just as personal data protection must not be applied mechanically to the point of sacrificing clients' rights to an effective legal defense. Attorneys are required to balance these two interests by applying the principles of due diligence and proportionality in data management.

Accountability is a key element in understanding a lawyer's responsibilities as a data controller. Accountability does not merely mean taking responsibility after a breach occurs, but also includes the obligation to demonstrate that adequate preventive measures have been implemented. In this context, lawyers are required to have internal policies regarding data management, security procedures, and mechanisms for monitoring the use of technology. Without a clear accountability framework, data protection obligations risk becoming a formality without substance.

Another implication of the lawyer's role as a data controller is the need to redefine the standard of professional care (Manullang & Habeahan, 2026). Professional care is no longer limited to legal analysis and defense strategies but also encompasses digital risk

management. A lawyer who is negligent in protecting client data—for example, by using an insecure system or ignoring security updates—may be deemed to have failed to meet professional standards, even if there was no intent to harm the client. In this context, technical negligence carries the same ethical and legal weight as substantive negligence.

Furthermore, the attorney's role as a data controller also has implications for relationships with third parties. In modern practice, attorneys frequently collaborate with technology consultants, IT service providers, or legal tech platforms. Such collaboration does not transfer the attorney's primary responsibility regarding client data. The attorney remains responsible for ensuring that involved third parties comply with adequate data protection standards (Butar-butar & Esther, 2026). A third party's failure to protect data may still result in professional liability for the attorney.

From a client protection perspective, recognizing lawyers as data controllers strengthens the client's position as a data subject who has rights over their personal information. Clients have the right to know how their data is managed, stored, and protected (Fiona & Rizqiyah, 2025). However, within the context of the professional relationship, the fulfillment of these rights must be carried out while maintaining the effectiveness of legal defense and the confidentiality of case strategies. This requires normative sensitivity in applying data protection principles without disrupting the lawyer's primary functions.

Thus, the lawyer's role as a controller and processor of personal data underscores that the duty of professional confidentiality has expanded into a broader realm of legal responsibility. Lawyers are no longer merely required to maintain client confidentiality ethically but must also manage client data responsibly in accordance with legal data protection standards. This integration of professional ethics and data protection regimes forms a crucial foundation for updating the paradigm of lawyer confidentiality in the digital age.

A Comparative Analysis of Digital Professional Ethics Regulations for Lawyers Across Countries

A comparative approach to analyzing the professional ethics of lawyers is essential for understanding how various legal systems respond to the challenges of client confidentiality in the digital age. Although the principle of confidentiality is a universal value in the legal profession, the ways in which countries regulate and enforce it show significant variations, particularly in responding to developments in information technology. This comparison is not intended to facilitate a direct transplantation of laws, but rather to identify normative principles that can be adapted to the context of the Indonesian legal system.

In common law countries, the regulation of attorney professional ethics tends to be more dynamic and based on the principle of ". Client confidentiality is viewed as an obligation that must be safeguarded through reasonable and proportionate efforts, including the use of technology (He, 2023). This approach emphasizes that attorneys are obligated to take rational preventive measures to prevent unauthorized access to client information. Thus, professional ethics not only prohibit the intentional disclosure of secrets but also require attorneys to actively manage digital risks.

A hallmark of the common law approach is the emphasis on the concept of reasonableness (Siregar, 2025). Attorneys are not required to achieve absolute security, but are obligated to demonstrate that they have made reasonable efforts in accordance with professional standards and technological advancements. Assessments of ethical violations are made by considering the context, including the type of data being handled, the scale of the legal practice, and the foreseeable level of risk. This approach provides normative flexibility while promoting responsibility-based professionalism.

Furthermore, common law countries tend to link confidentiality obligations with technological competence obligations. Mastery of relevant technology is viewed as part of a lawyer's professional competence. Ignorance of technological risks is not considered a valid excuse in the event of a breach of confidentiality *(Trust, Because You Can't Verify, n.d.)*. Thus, professional ethics serve as an instrument to ensure that lawyers continuously update their knowledge and skills in line with the evolution of legal practice.

In countries with a civil law tradition, particularly in Continental Europe, the regulation of attorney professional ethics is increasingly integrated with the personal data protection regime (Cervi, 2022). Professional confidentiality is not positioned as a standalone norm, but rather as part of the system protecting the right to privacy and personal data. This approach positions lawyers as legal subjects with specific obligations regarding data management, subject to relatively detailed and binding standards.

This integration results in a strong emphasis on the principle of accountability. Lawyers are required not only to protect client data but also to demonstrate compliance with data protection standards (Abella et al., 2025). These obligations include documenting internal policies, conducting risk assessments, and overseeing third parties involved in data processing. In this context, professional ethics serve as a bridge between the moral obligations of attorneys and public legal obligations regarding data protection.

The civil law approach also demonstrates a tendency to adopt normative minimum data security standards. These standards are not always formulated technically, but they provide a clear framework of obligations regarding the protection of sensitive data. With these standards in place, lawyers have more concrete guidelines for managing digital risks, while clients gain the assurance that their data is systematically protected.

A comparison between the common law and civil law approaches reveals a normative convergence in responding to digital challenges. Both acknowledge that professional confidentiality can no longer be maintained solely through individual commitment but requires adequate technological governance. The difference lies in the level of detail and enforcement mechanisms. Common law tends to provide principle-based flexibility, while civil law places greater emphasis on compliance with structured standards.

For Indonesia, the key lesson from this comparative approach is the importance of developing adaptive professional ethics without

losing the character of the national legal system. A model that is too rigid risks being unresponsive to technological developments, while a model that is too flexible may create normative uncertainty. Therefore, a balance is needed between general principles and clear operational guidelines in the regulation of legal professional ethics.

The relevance of the comparative approach also lies in the recognition that the legal profession operates in a global environment. Cross-border legal practice, the use of international technology platforms, and cross-border data exchange demand internationally compatible ethical standards. By adopting globally recognized principles of digital ethics, the legal profession in Indonesia can strengthen its competitiveness and credibility at the international level.

However, the adaptation of global principles must take into account the factual and institutional conditions in Indonesia. Differences in the level of technological infrastructure, the scale of legal practice, and the capacity of professional organizations demand a contextual approach. The reformulation of professional ethics must be designed to be realistically applied by lawyers with diverse practice backgrounds, without compromising client protection.

Thus, comparative analysis indicates that updating the professional ethics of lawyers in the digital age is an inevitability faced by various legal systems. The experiences of other countries provide a valuable reference framework, but the success of reform depends heavily on the ability to adapt these principles to the national context. This discussion serves as an important foundation for analyzing more specific ethical challenges related to the use of smart legal technology and artificial intelligence in legal practice.

Ethical Challenges of Using Legal Technology and Artificial Intelligence in the Legal Profession

The use of legal technology and artificial intelligence in the legal profession is a logical consequence of the digital transformation of the legal sector. These technologies offer efficiency, accuracy, and ease in case management, ranging from legal document searches and contract analysis to case outcome predictions. However, behind these benefits lie a number of complex ethical challenges, particularly regarding client confidentiality and the professional responsibilities of attorneys.

One of the main challenges is the increased risk of confidentiality breaches resulting from the use of technology-based systems (Gemawaty & Yuliani, 2024). Legal tech generally operates by processing large volumes of data, including sensitive client data. The use of cloud-based systems, integration with third-party platforms, and cross-jurisdictional data processing increase the potential for unauthorized access and data breaches. In this context, attorneys are no longer the sole guardians of client confidentiality, as the data also resides within a technological ecosystem involving numerous actors.

The use of artificial intelligence raises additional issues regarding transparency and control. The algorithms used in AI systems are often complex and cannot be fully explained in simple terms. The lack of clarity regarding how algorithms work raises ethical questions about the extent to which attorneys can be held accountable for the analysis results generated by such systems. Overreliance on technological recommendations has the potential to reduce lawyers' professional autonomy and blur the line between technological assistance and legal decision- making.

The next challenge relates to the principle of professional competence. The use of legal tech requires lawyers to have a basic understanding of the technology being used, including its risks and limitations. Ignorance or negligence in understanding how the system works can lead to errors in the management of client data or the inappropriate use of analysis results. From a professional ethics perspective, a failure to develop technological competence can be viewed as a breach of the duty of professional care.

Additionally, the use of artificial intelligence raises issues regarding accuracy and bias. AI systems are built on specific data and models that are not always neutral. Bias in training data can produce unfair or inaccurate recommendations, which may ultimately harm clients. Attorneys who use such systems without critical evaluation risk violating their duty to provide an objective and balanced defense. In this context, an attorney's ethical responsibility cannot be delegated to the technology being used.

Another equally important issue is the relationship between the use of legal tech and client consent. Clients have the right to know how their data is used and processed, including the use of artificial intelligence-based technology (Adela et al., 2025). A lack of transparency in this regard can erode client trust and potentially violate the principles of fairness and honesty in professional relationships. Attorneys are required to explain the use of technology in a proportionate manner without compromising the confidentiality of legal strategies.

The use of technology also raises challenges regarding accountability when errors or violations occur. In situations where data breaches or analytical errors are caused by system failures, the question of who is responsible becomes crucial (Fathur, 2020). From a professional ethics perspective, attorneys remain the primary party responsible to clients, regardless of the involvement of technology or third parties. This principle affirms that technology serves as a tool, not as a substitute for professional responsibility.

On the other hand, rejecting the use of technology is not a realistic solution. A total ban on legal tech could actually hinder access to justice and place the legal profession at a competitive disadvantage. Existing ethical challenges must be addressed through adaptive, risk-based regulations, not through a prohibitive approach. Professional ethics must provide a framework that enables the responsible use of technology (Sulianta, 2025).

In this context, it is important to emphasize the need for the principle of digital due diligence. This principle requires lawyers to conduct a risk assessment before using specific technologies, consider their impact on client confidentiality, and ensure the presence of adequate security mechanisms. Digital due diligence also includes periodic evaluations of the technologies used and a willingness to adapt practices as risks evolve.

Ethical challenges regarding the use of artificial intelligence are also linked to the potential shift in the lawyer's role. If technology is used predominantly in analysis and decision-making, there is a risk that the lawyer's role will be reduced to that of a mere system operator. This contradicts the very nature of the legal profession as one grounded in human judgment, ethics, and moral responsibility. Therefore, professional ethics must affirm that the final decision in legal matters must remain in the hands of the attorney.

Thus, the use of legal technology and artificial intelligence presents a complex ethical dilemma. On one hand, technology offers significant benefits for the efficiency and quality of legal services. On the other hand, technology expands the spectrum of risks to client confidentiality and professional integrity. These challenges demand a reformulation of professional ethics capable of accommodating technological innovation without sacrificing the fundamental values of the legal profession.

Reformulating Attorney Confidentiality Ethics in the Digital Age and Normative Recommendations

The development of digital technology has fundamentally transformed the landscape of the legal profession. This transformation is not merely technical but also normative, as it touches upon the core values of the legal profession: confidentiality, trust, and professional responsibility. In this context, the attorney's duty of confidentiality can no longer be understood narrowly as an individual moral obligation but must be interpreted as a multidimensional obligation encompassing ethical, legal, and technological aspects simultaneously.

Reformulating the ethics of attorney-client confidentiality has become an urgent necessity because current ethical norms remain oriented toward conventional legal practice (Saputra et al., 2026). The Indonesian Code of Ethics for Attorneys, while affirming the duty to keep confidential everything learned from a client, has not provided operational guidance on how this duty is to be carried out in a digital environment. Consequently, there is a disconnect between general ethical norms and increasingly complex, technology-driven professional practices.

From a normative perspective, attorney confidentiality in the digital age must be redefined as an active obligation, not merely a passive one. In the analog era, confidentiality could be maintained by restricting physical access to documents and communications. However, in the digital era, confidentiality demands proactive measures such as implementing security systems, managing technological risks, and continuously monitoring the digital infrastructure used. It is not enough for attorneys to simply "not disclose" client secrets; they must also ensure that the systems they use do not allow for accidental leaks.

This reformulation demands explicit recognition of the concept of digital confidentiality as an integral part of professional ethics. Digital confidentiality encompasses the obligation to protect client data throughout the entire electronic processing cycle, from collection, storage, and use to the destruction of data. This principle requires attorneys to understand the of client data flows and identify potential risk points that threaten confidentiality (Fauziah et al., 2026). Thus, confidentiality is no longer viewed as a static state but as a dynamic and ongoing process.

Furthermore, the reformulation of confidentiality ethics must incorporate the principle of technological competence as an explicit professional obligation. Technological competence does not mean that attorneys must become information technology experts, but rather that they must possess an adequate understanding of the technologies used in legal practice. This understanding includes awareness of cybersecurity risks, the ability to select trustworthy technology service providers, and basic knowledge of risk mitigation measures. Without this competence, attorneys risk committing professional negligence that directly impacts clients' interests.

In the context of national law, the reformulation of confidentiality ethics must be aligned with the personal data protection regime. The Personal Data Protection Act has introduced the concepts of data controller and data processor responsibilities, which are substantively relevant to the practice of the legal profession. Lawyers, in their relationship with clients, act not only as legal advisors but also as parties that control and process clients' personal data. Therefore, the ethical duty to maintain client confidentiality must be understood as part of the legal obligation to protect personal data securely and responsibly.

Integration between professional ethics and personal data protection law is also crucial to prevent a dualism of responsibility. Without clear integration, lawyers may find themselves in a vulnerable position, where a single act could be assessed differently under the ethical regime and the public legal regime. A reformulation of the code of ethics that adopts personal data protection principles will provide normative certainty while strengthening client protection.

From an institutional perspective, professional bar associations play a strategic role in driving the reformulation of confidentiality ethics. Updates to the code of ethics must be undertaken through a participatory approach involving practitioners, academics, and technology experts (Anam et al., 2025). This approach is essential to ensure that the resulting norms are not only theoretically ideal but also practical in daily practice. A code of ethics that is too abstract will be difficult to implement, while one that is too technical risks becoming obsolete quickly due to technological advancements.

In addition to updating ethical norms, professional organizations must also develop technical guidelines and minimum operational standards regarding data security. These guidelines may include requirements for the use of strong passwords, communication encryption, internal access management, and security incident response procedures. These standards are not intended to standardize all legal practice but to establish measurable and enforceable minimum thresholds for ethical compliance.

The next normative recommendation pertains to professional education and training. A reformulation of the ethics of confidentiality

will not be effective without an accompanying increase in digital ethics literacy among lawyers. Legal education, both at the university level and in continuing professional education, must incorporate material on cybersecurity, personal data protection, and the ethics of using legal technology. Thus, lawyers are prepared from the outset to face ethical challenges in the digital age.

In the long term, the reformulation of attorney confidentiality ethics also contributes to strengthening the legitimacy of the legal profession. Amid the public's growing reliance on technology and concerns about data misuse, the legal profession has an opportunity to reaffirm its role as a guardian of public trust. Ethics that are adaptive to digitalization will demonstrate that the legal profession is capable of evolving without abandoning its fundamental values.

In conclusion, it can be asserted that attorney-client privilege in the digital age cannot be maintained through a static, normative approach. Technological changes demand a shift in perspective regarding ethical obligations—from individual obligations toward systemic obligations that encompass both humans and technology. A reformulation of confidentiality ethics that integrates digital confidentiality, technological competence, and data accountability is a crucial normative step to maintain the integrity of the legal profession. With these updates, the legal profession in Indonesia will be better prepared to face the challenges of the digital age while maintaining client trust as the cornerstone of legal practice.

IV. CONCLUSION

Client confidentiality is a fundamental principle in the legal profession that serves to maintain the relationship of trust between attorneys and clients and underpin the integrity of the judicial system. Within the framework of Indonesian positive law, this obligation has been established as both an ethical norm and a binding legal norm. However, the development of digital technology has significantly altered the way lawyers manage client information, thereby expanding the risks of confidentiality breaches that cannot be fully addressed by current professional ethical regulations.

Research findings indicate that the Indonesian Code of Ethics for Lawyers still interprets the duty of confidentiality within the framework of conventional legal practice and has not provided adequate normative guidance regarding the management of client data in a digital environment. The digitization of legal practice—including the use of electronic storage, online communication, and AI-based legal technologies—places client data within a complex technological ecosystem vulnerable to security breaches. Under such conditions, an ethical approach relying solely on the individual integrity of attorneys is no longer sufficient.

This study asserts that the attorney's duty of confidentiality in the digital age must be understood as a multidimensional obligation that comprehensively encompasses ethical, legal, and technological dimensions. Attorneys are not only obligated not to disclose client secrets but are also responsible for ensuring that the systems and technologies used in their professional practice are capable of adequately protecting client data. From this perspective, confidentiality is no longer passive but demands active measures such as risk management and the implementation of data security standards.

Furthermore, this study found that personal data protection regimes provide a relevant legal foundation for strengthening attorneys' confidentiality obligations in the digital age. In their relationship with clients, attorneys can be positioned as controllers and processors of personal data; thus, breaches of data security not only have ethical implications but also potentially give rise to legal liability. However, the lack of clear integration between professional ethical norms and personal data protection laws creates a normative gap that could potentially weaken the protection of clients' interests.

Based on the overall analysis, this study concludes that the reformulation of attorney confidentiality ethics is an urgent normative necessity. This reformulation must accommodate the principles of digital confidentiality, technological competence, and data accountability as integral parts of the legal profession's ethics. An adaptive ethical framework that keeps pace with technological advancements will strengthen the legitimacy of the legal profession, provide normative certainty for practitioners, and maintain public trust in the legal profession amidst the ongoing digital transformation.

V. RECOMMENDATIONS

Based on the findings of this study, strategic and normative measures are required to strengthen the protection of attorney–client confidentiality in an increasingly complex and high-risk digital environment.

First, the Indonesian Code of Ethics for Advocates must be explicitly reformulated to incorporate principles of digital confidentiality and technological responsibility. This reformulation should include clear provisions on electronic data management, minimum cybersecurity standards, and limitations on the use of legal technologies, including artificial intelligence, in legal practice.

Second, professional organizations of advocates should establish binding technical guidelines on client data protection. These guidelines must cover secure communication protocols, data storage systems, access control mechanisms, encryption standards, and incident response procedures for data breaches.

Third, the integration between professional ethics and personal data protection law must be strengthened at a normative level. Advocates should be clearly recognized as data controllers and/or processors within the legal framework, thereby subjecting them to accountability principles in data governance.

Fourth, continuous education and training in digital ethics and cybersecurity must be institutionalized as a professional obligation. Such capacity building is essential to ensure that advocates possess the technological competence necessary to assess, manage, and

mitigate risks associated with digital legal practice, including the ethical use of artificial intelligence.

Fifth, law firms and individual practitioners should adopt a systematic risk-based approach to managing client data. This approach requires proactive identification of vulnerabilities, regular evaluation of technological systems, and the implementation of mitigation measures proportionate to the level of risk involved.

Finally, future research is encouraged to examine the practical implementation of digital confidentiality in legal practice, including empirical studies on data protection compliance among advocates and the impact of legal technology on professional ethics.

REFERENCES

1. Abella, P., Dayu, N., & Marzadi, H. (2025). Analisis pelanggaran kode etik advokat dan perannya dalam meningkatkan profesionalisme profesi advokat. Journal of Development Economics and Digitalization, Tourism Economics, 2(1), 81–93. https://doi.org/10.70248/jdedte.v2i1.1754
2. Adams, T. L., Leslie, K., Myles, S., & Moraes, B. (2024). Regulating professional ethics in a context of technological change. BMC Medical Ethics, 25(1), 143. https://doi.org/10.1186/s12910-024-01140-x
3. Adela, N. N., Maharani, T. S., Rahmadina, N. S., Kurdi, S., Wardani, M., & Hafidzi, A. (2025). Hak privasi pengguna dalam era kecerdasan buatan: Tinjauan normatif hukum terhadap kesehatan mental. Interdisciplinary Explorations in Research Journal, 3(1), 75–82.
4. Anam, M. A., Mubarok, M. B. U., Fitria, A. S., Lailiyah, R. A., & Wahidullah. (2025). Etika profesi hukum dalam menghadapi tantangan era digital melalui perspektif integritas, tanggung jawab, dan independensi profesi. Al-Zayn: Jurnal Ilmu Sosial & Hukum, 3(3), 2715–2726. https://doi.org/10.61104/alz.v3i3.1707
5. Asrori, M. N. (2018). Tanggung jawab advokat dalam menjalankan jasa hukum kepada klien. Deepublish.
6. Azahra, M. F., & Putra, P. (2024). Implementasi arsip digital dalam efisiensi penyimpanan. Journal of Economic and Management (JEM) Terekam Jejak, 1(1), 1–13.
7. Bayya, A. K. (2022). Advocating ethical data management and security. International Journal of Computer Science Engineering Techniques, 8, 396–417. https://doi.org/10.32628/CSEIT225541
8. Butar-Butar, B. N., & Esther, J. (2026). Perlindungan hak asasi manusia dalam proses peradilan pidana melalui peran advokat. Jurnal Ilmu Pendidikan dan Sosial, 4(4), 609–620. https://doi.org/10.58540/jipsi.v4i4.1107
9. Candra, G. A. E. (2025). Peran teknologi informasi dalam meningkatkan pemberian bantuan hukum kepada klien oleh advokat dalam perkara perdata. Jurnal Komunikasi Hukum, 11(1), 150–163. https://doi.org/10.23887/jkh.v11i1.102229
10. Cervi, G. V. (2022). Why and how does the EU rule global digital policy: An empirical analysis of EU regulatory influence in data protection laws. Digital Society, 1(2), 18. https://doi.org/10.1007/s44206-022-00005-3
11. Cindy, C., Ivanka, K. A., Nasution, N. A., & Nurbaiti, N. (2025). Penerapan teknologi blockchain untuk meningkatkan keamanan dalam transaksi di era digital. Economist: Jurnal Ekonomi dan Bisnis, 2(1), 50–59. https://doi.org/10.63545/economist.v2i1.79
12. Cox, A. (2022). The ethics of AI for information professionals: Eight scenarios. Journal of the Australian Library and Information Association, 71(3), 201–214. https://doi.org/10.1080/24750158.2022.2084885
13. Davidson, K. M., Ostrom, B. J., & Kleiman, M. (2022). Client perspectives of holistic defense: Strengthening procedural justice through enhanced client trust. Justice System Journal, 43(1), 128–150. https://doi.org/10.1080/0098261X.2022.2062582
14. Dewanti, T. R., & Lewoleba, K. K. (2025). Analisis pelanggaran kode etik advokat terhadap penanganan perkara klien dalam kasus advokat Biy Palembang. Media Hukum Indonesia, 3(3). https://doi.org/10.5281/zenodo.15637950
15. Fauziah, Y. A., Susanto, D. A., & Utama, Y. P. (2026). Perlindungan hukum data kesehatan pasien di era digital. Jurnal Hukum dan Etika Kesehatan, 6(1), 1–19. https://doi.org/10.30649/jhek.v6i1.270
16. Fiona, & Rizqiyah, N. (2025). Perlindungan data pribadi klien pada era digital: Harmonisasi regulasi kenotariatan dan hukum perlindungan data pribadi. Jurnal Minuta, 7(2), 76–84. https://doi.org/10.24123/minuta.v7i2.7635
17. Fisher, M. A. (2008). Protecting confidentiality rights: The need for an ethical practice model. American Psychologist, 63(1), 1–13. https://doi.org/10.1037/0003-066X.63.1.1
18. He, Z. (2023). From privacy-enhancing to health data utilisation: The traces of anonymisation and pseudonymisation in EU data protection law. Digital Society, 2(2), 17. https://doi.org/10.1007/s44206-023-00043-5
19. Implementasi kode etik profesi advokat dalam praktik sehari-hari. (n.d.). Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat. https://journal.forikami.com/index.php/dassollen/article/view/799
20. Jorgenson, L. M., Hirsch, A. B., & Wahl, K. M. (1997). Fiduciary duty and boundaries: Acting in the client's best interest. Behavioral Sciences & the Law, 15(1), 49–62. https://doi.org/10.1002/(SICI)1099-0798(199724)15:1<49::AID-BSL253>3.0.CO;2-X

21. Khairun, I. L. L., Ardelia, T. A., Aprilia, S. N., & Imon, S. A. (2025). Strategi komunikasi advokat dalam membangun kepercayaan klien: Ditinjau dari pendekatan hukum. Media Hukum Indonesia, 3(2). https://doi.org/10.5281/zenodo.15511861
22. Khan, M. N. I. (2023). Legal documentation and case management: A systematic review of digitization trends and cybersecurity challenges in legal support roles. Review of Applied Science and Technology, 2(1), 1–25. https://doi.org/10.63125/21hf4w52
23. Kurniawan, T., Dj, A., Karim, A., Marifah, M., & Muniri, S. (2025). E-book hukum digital dan privasi data 2025.
24. Lubis, F., Harahap, N. I., Livia, D., Sembiring, T. H., Lubis, M. A., & Sitepu, A. R. (2025). Peran advokat dalam menegakkan keadilan. Bertuah Jurnal Syariah dan Ekonomi Islam, 6(1), 104–113.
25. Manullang, R. L., & Habeahan, B. (2026). Tinjauan yuridis peranan advokat dalam penyelesaian sengketa yang ditentukan oleh klien. Judge: Jurnal Hukum, 6(6), 2054–2063. https://doi.org/10.54209/judge.v6i06.2070
26. McCarty, D. L., Christian, D. D., & Stefurak, T. (2023). Adlerian-informed supervision: Protecting counselors from burnout and improving client outcomes in the juvenile justice system. Psychological Services, 20(2), 318–325. https://doi.org/10.1037/ser0000641
27. Meliana, Y. (2025). Dialektika sistem peradilan terhadap analisis kritis perbandingan litigasi virtual dan konvensional dalam perspektif hak pembelaan terdakwa. Jurnal Hukum Lex Generalis, 6(7). https://doi.org/10.56370/jhlg.v6i7.2183
28. M. Hum, S. (2023). Etika dan tanggung jawab profesi hukum di Indonesia. Sinar Grafika.
29. Muhamad, F., Basyarin, R., & Akhirah, N. (2025). Peran strategis profesi hukum di era society 5.0: Antara inovasi dan etika profesional. Journal Sains Student Research, 3(2), 642–654. https://doi.org/10.61722/jssr.v3i2.4391
30. Munawarah, I., Raffi, M., Agustin, N., & Haslinda, H. (2025). Menjaga privasi di cloud: Tantangan dan strategi perlindungan data pribadi di era digital. Prosiding Diseminasi Nasional Hasil Penelitian dan Pengabdian kepada Masyarakat, 2(1). https://doi.org/10.30998/dinamika.v2i1.8341
31. Nasution, S. A., & Husein, S. H. (2025). Pengaruh teknologi informasi terhadap kewajiban kerahasiaan dan perlindungan data pribadi klien dalam praktik notaris. Media Bina Ilmiah, 19(12), 6491–6500.
32. Permana, G. (2024). Urgensi perubahan pengaturan kelembagaan organisasi advokat untuk mewujudkan profesi advokat yang officium nobile (Master's thesis, Universitas Nasional). https://repository.unas.ac.id/id/eprint/10944/
33. Pratomo, M. A. (2025). Profesional di bawah sorotan algoritma: Etika, citra, dan pertarungan di era digital. PT MuhammadAriLaw Pustaka Nada.
34. Putri, R. M. S., Septiani, R., Putri, N. A. C., & Handoko, A. B. (2026). Etika profesi sebagai pilar pencegahan penyalahgunaan wewenang dalam penegakan hukum pidana. Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat, 4(2). https://journal.forikami.com/index.php/dassollen/article/view/1039
35. Rabiu, A. A., Merican, A. M. M. N., & Murshid, G. A. (2025). Ethics in the digital age: Exploring the ethical challenges of technology. Journal of Information Systems and Digital Technologies, 7(1), 29–50. https://doi.org/10.31436/jisdt.v7i1.555
36. Rafid, R., & Nurita, R. F. (2025). Dinamika pendidikan dan hukum di era digital: Tantangan dan peluang dalam menghadapi transformasi teknologi. MLJ Merdeka Law Journal, 6(1), 79–92.
37. Rauzi, F., & Suriadiata, I. (2024). Penyuluhan etika profesi hukum bagi calon advokat Ikatan Advokat Indonesia. Jurnal Ilmiah Pengabdian dan Inovasi, 2(4), 869–876. https://doi.org/10.57248/jilpi.v2i4.429
38. Rhode, D. L. (2003). Ethics in practice: Lawyers' roles, responsibilities, and regulation. Oxford University Press.
39. Rinaldi, F. A., Hidayati, A. D., Putri, L. N. A., Ramadhani, R., Abigail, K. J., Sumardiana, B., & Abidah, S. Q. (2025). Kemahiran bantuan hukum pendampingan advokat berkomunikasi dengan klien. Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research, 2(2), 3678–3687. https://doi.org/10.32672/mister.v2i2.3223
40. Rosdiana, R., Arda, A., & Yanti, D. (2025). Legal issues in the oversight and enforcement of advocate professional ethics in Indonesia. Hakim: Jurnal Ilmu Hukum dan Sosial, 3(1), 1072–1089. https://doi.org/10.51903/hakim.v3i1.2300
41. Saputra, M. I., Nugeraha, P. R., Maulana, M. R., & Pratama, M. R. (2026). Orientasi materi versus integritas profesi advokat: Tantangan penegakan kode etik dalam praktik hukum. Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat, 4(2). https://journal.forikami.com/index.php/dassollen/article/view/1059
42. Setiarma, A. (2023). Disrupsi teknologi hukum terhadap jasa advokat dalam pandangan hukum pembangunan Mochtar Kusumaatmadja. Reformasi Hukum, 27(2), 80–88. https://doi.org/10.46257/jrh.v27i2.622
43. Siregar, M. A. (2025). Buku ajar perbandingan hukum pidana. Serasi Media Teknologi.
44. Tahir, R., Astawa, I. G. P., Widjajanto, A., Panggabean, M. L., Rohman, M. M., Dewi, N. P. P., Deliarnoor, N. A., Abas, M., Ayu, R. F., Meinarni, N. P. S., Hs, F., Sumartini, N. W. E., Sugiharti, D. K., & Paminto, S. R. (2023). Metodologi penelitian bidang hukum: Suatu pendekatan teori dan praktik. PT Sonpedia Publishing Indonesia.
45. Trust, because you can't verify: Privacy and security hurdles in education technology acquisition practices. (n.d.). Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3658644.3690353

46. Waruwu, S., & Siswoyo, A. A. (2024). Data pribadi sebagai aset bisnis: Sinergi hukum rahasia dagang dan perlindungan data. Lex Lectio Law Journal, 3(2), 118–129. https://doi.org/10.61715/jll.v3i2.118
47. Zuhdiantito, A. (2025). Urgensi pembaharuan hukum terhadap undang-undang jabatan notaris berbasis praktik persaingan tidak sehat antar notaris di era disrupsi digital (Thesis, Universitas Islam Indonesia). https://dspace.uii.ac.id/handle/123456789/57822