

INTERNATIONAL JOURNALOF LAW AND CONSTITUTION STUDY

Journal home page: https://jurnal.asrypersadaquality.com/index.php/ijlacos

CRIMINAL LAW POLICY ETHICS AND PRIVACY CHALLENGES IN NEW CRIMINAL ENFORCEMENT DIGITAL RELETED TO CYBERCRIME

Humaira Hannani Hrp[1], Diana Sri Utami[2], Rina Solin[3], Muhammad Rahman Rizqi[4]

Faculty of Sharia and Law, Department of Islamic Criminal Law, State Islamic University of North Sumatera Utara, Indonesia

diana0205232044@uinsu.ac.id

Abstract

The rapid development of tecnology has reshaped Indonesia's criminal law landscape, demanding adaptive policies to address emeriging forms cyber crime. Implemention of the New Criminal Code (KUHP) marks a legal system renewal effort to adjust classical criminal norms with the reality of the digital world. This study traces the direction of the virtue of digital criminal law in facing the challenges of ethics and privacy in law enforcement of siber's crime. By referring to various academic studies and comparative analysis, this study highlights the tension between the authority of the state in the oversight of cyberspace and protection of individual privacy rights. In addition, it is also discused the ethical implications of law enforcement practices, especially related to data collection, digital forensics, and electronic proof. Through the latest normative cyber law enforcement must be accompanied by ethical accountability and privacy protection. In conclusion, the application of new Criminal Code needs to be integrated with the Protection Act of Personal Data and international Digital Ethics Standarda to create a balance between public security and civil liberties in the digital space.

Keywords: Digital Criminal Law, Cyber Crime, KUHP, Privacy, Legal Ethics

INTRODUCTION

The development digital technology in two decades last has brought transformation big towards life social, economy, and law. The world virtual become room new for activity human, starting from communication, transaction economy, until activity government which creates form interaction new simultaneously potential crime new (Sangalang && Farina, 2024). In the context criminal law, digitalization gives birth to various forms cybercrime such as spread data personal without permission, fraud online, attacks cyber, as well as manipulation information. This change demands the existence of a system criminal law which is responsive to the dynamics technology so that enforcement law remains effective in the era digital (Arifin & Handayani, 2024). Indonesia then responds to the phenomenon through the enactment of the Book Statute Criminal Law (KUHP) new year 2023 which starts effective year 2026. KUHP new this reflects effort renewal law national to adjust provisions criminal with development crime modern, including crime cyber (Fajriansyah, Siregar & Panggabean, 2025).

The renewal becomes important because KUHP old legacy colonial no longer adequate for reach crime which is based on information technology (Indradjaja, Suseno Atmaja, 2024). Through articles-articles new and harmonization with the Law Information and Electronic Transactions (UU ITE), law criminal Indonesia strives to expand the scope enforcement law in space digital. However, modernization law this also raises problem ethical and juridical which is complex. In practice, enforcement digital law often intersects with the right privacy citizen, especially in activities digital surveillance, wiretapping, and collection electronic data by apparatus (Mak, Ho Beaumont, 2025). Tension between authority state in guarantee security digital and right individual to defend privacy becomes dilemma main in various country, including Indonesia (Cinar & Vanberg, 2022). Besides that, misuse personal data as well as weakness mechanism supervision towards institution enforcement law also strengthens concern will violation right basic in space digital (Yilma, 2023). Challenge ethics and privacy this increasingly prominent when technology law forensic digital used without guideline ethical which is clear. In this case, ethics criminal law digital must ensure that every action investigation and enforcement law done proportionally, transparent, and respect right individual (Winter & Ruggeri, 2022). A number of research also emphasizes the importance of building balance between effectiveness

enforcement law and protection right privacy society in handling crime cyber (Hendrawan, Rahmadhan & Hiahdar, 2025).

Therefore, writing this strives to examine the direction policy criminal law digital Indonesia in the context of the enactment of the new KUHP, by highlighting problem ethics and privacy as two aspects crucial in enforcement law cyber. Analysis done juridical normative by including approach conceptual and comparison law, for understand how policy law criminal can develop adaptively without sacrificing value justice and protection right basic human (Hasamuddin, Efendi Hamdi, 2024). Through study this, is hoped emerge understanding which is more comprehensive about how system criminal law digital Indonesia can run in line with principles-principles ethics and protection privacy in the era globalization technology.

1.Basic Concept of Digital Criminal Law and Cybercrime

Digital criminal law refers to the adaptation of traditional criminal norms and institutions to regulate, prevent, and prosecute unlawful acts that occur in the digital space or utilize information technology as the primary means. Essentially, it connects fundamental principles of criminal law - such as the principle of legality, the elements of the act (*actus reus*), and guilt (*mens rea*) - with the technical reality of cyberspace, which has specific characteristics like **s**peed of dissemination, anonymity, and transnational nature (Sangalang & Farina, 2024; Nieto Martin, 2022). The classification of cybercrimes frequently used in literature differentiates between crimes that are dependent on the technology itself (*cyber-dependent crimes*) (e.g., hacking, spreading malware) and crimes that are enabled or magnified by technology (*cyber-enabled crimes*) (e.g., online fraud, distribution of illegal material). This classification helps determine the legal approach, whether it requires a new technology-specific norm or an adaptation of general criminal rules to new *modi operandi* (Sangalang & Farina; Winter & Ruggeri, 2022). Operationally, the main challenges in applying the concept of digital criminal law include proof (*how to prove the digital act*), attribution (determining the perpetrator behind the virtual identity), and the continuity of the digital evidence chain (*chain of custody*).

Electronic evidence is vulnerable to alteration, encryption, and cross-server traces, thus requiring clear digital forensic standards to be admissible in court (Husamuddin et al., 2024; Zainal & Handayani, 2024). Furthermore, the transnational nature of many cybercrimes necessitates international cooperation, mutual legal assistance treaties, and the harmonization of norms to prevent a legal vacuum in

enforcement (Nieto Martin, 2022; Winter & Ruggeri, 2022). In terms of policy, several authors emphasize the need for a combination of substantive regulation (*criminalization of specific digital harms*) and the strengthening of procedural aspects (digital investigation rules, forensic standards, Mutual Legal Assistance).

In the context of Indonesia, the development of the new Criminal Code (KUHP) and sectoral regulations like the Electronic Information and Transactions Law (UU ITE) and data protection regulations indicate a direction toward norm harmonization. However, its implementation still requires technical and procedural alignment to effectively face the ever-changing *modi operandi* of cybercrimes (Fajriansyah et al., 2025; Hendrawan et al., 2025).

2 Principles ethics law and right privacy in law criminal

Right privacy constitutes one of right fundamental which gets pressure strong in era digital because capacity technology to collect, analyze, and store data personal large scale. Normatively, protection privacy not stands alone; it must be read together with principles-principles ethics enforcement law, such as legality, proportionality, necessity, transparency, and accountability. Principles-principles this demands that every intervention towards privacy must have basis law which clear, goal which legitimate, way which minimal possible, as well as mechanism supervision which effective (Mak, Ho & Beaumont, 2025; Cinar & Vanberg, 2022). In practice investigation cyber, dilemma ethical arises when apparatus needs access to data to prevent crime or collect evidence, while action that risks targeting data which not relevant or violates right party third. Experience country other shows that response security which broad, for example collection mass metadata or monitoring without time limit, can cause violation right basic if not equipped limit law and control judicial (Hale-Ross, 2019; Winter & Ruggeri, 2022).

Therefore ethics enforcement emphasizes need for mechanism permission (warrants), limitation goal, recording action wiretapping/access, and audit independent. Principle privacy also demands application policy technical such as data minimisation, encryption end – to - end when possible, as well as policy retention data which clear. Besides that, role authority protection data independent becomes crucial to supervise suitability practice enforcement law with right privacy and gives channel remedial for victim violation (Mak er al., 2025; Yilma, 2023). In context criminal international and post-national criminal justice, author also shows that without

standard ethical which strong, efforts transnational to prosecute crime can erode protection right individual in various jurisdictions (Nieto Martin, 2022).

Finally, integration between ethics law and right privacy not just problem limitation action apparatus, but also problem legitimacy social from enforcement law that itself: society more likely supports action which viewed fair, proportional, and transparent. Therefore policy law criminal digital effective must combine norm substantive (what which prohibited), rule procedural (how investigation done), as well as rule ethical and supervision which ensures right privacy remains respected (Husamuddin et al., 2024; Hendrawan et al., 2025).

3 Theory policy law criminal (politics criminal, ultimum, remedium, etc.)

Theory policy law criminal (politics criminal) focuses attention on how state chooses instrument law its for prevent and prosecute act which harms society. In literature politics criminal, goal main is determine when and how far criminalization needed, as well as choose form sanction which proportional towards harm which wants to be eliminated (Nieto Martín, 2022). Principles-principles central which often made guide policy criminal include principle legality (*nullum crimen, nulla poena sine lege*), principle proportionality, principle *ultimum remedium* (criminal law as way last), and principle minimization intervention state towards freedom individual (Sangalang & Farina, 2024; Hasamuddin et al., 2024). *Ultimum remedium* affirms that law criminal should be applied only after effort non-criminal (regulation administrative, sanction civil, compliance technology) assessed not adequate to handle danger. In context crime cyber, principle this demands analysis *cost-benefit*: whether criminalization a mode digital more effective than rule technical or sanction administrative, and whether threat which caused by it enough serious to sacrifice freedom certain (Nieto Martín, 2022; Winter & Ruggeri, 2022).

Policy which prioritizes *ultimum remedium* also suggests gradation sanction, so that Action minor which motivated by negligence or economic not automatically subject to punishment criminal heavy. Besides that, politics criminal modern emphasizes importance precision norm (precision) so that not occurs criminalization which too broad or vague. In realm digital, threat ambiguity law increasingly big because term technical and pattern crime changes fast; therefore maker policy needs to formulate element offense which specific and measurable so that not causes effect chilling towards freedom expression and innovation technical (Sangalang & Farina, 2024; Fajriansyah et al., 2025).

Theory policy criminal also highlights aspect procedural, namely that effectiveness rule substantive depends on rule investigation, proof, and mechanism cooperation international. Standard forensic digital, protection chain evidence, as well as instrument cooperation extraterritorial such as Mutual Legal Assitance becomes part not separable from policy which effective to handle act criminal cross border (Hasamuddin et al., 2024; Nieto Martín, 2022). Literature also suggests approach multidisciplinary: combination norm law, technology prevention, Cooperation public-private, and Education digital literacy as sequence policy integrated to reduce room Movement crime cyber (Arifin & Handayani, 2024; Winter & Ruggeri, 2022).

4 Study literature related KUHP new and regulation protection data personal.

A number of studies latest discuss direction reform KUHP and how provision new potentially accommodate challenge crime cyber. Research current shows that KUHP new strives to include norms-norms which more relevant with reality digital so that gives basis substantive for prosecution cybercrime, simultaneously doing harmonization with regulation sectoral such as Statute Information and Electronic Transactions (UU ITE) (Fajriansyah et al., 2025; Indradjaja et al., 2024). However, literature also gives note critical: several authors reminds risk formulation article which still bersifat general so that can be misused or interpreted broad by apparatus enforcement law (Devi Anjheli, 2022/2023). In aspect protection data personal, study comparative in Asia emphasizes that statute protection data (Personal Data Protection/PDP) must run side by side with policy criminal. (Mak et al. 2025) emphasizes importance principle technical such as data minimisation, goal collection which clear, as well as rule retention data which limited.

Without harmonization which clear between KUHP, UU ITE, and UU PDP, apparatus enforcement could just obtain access broad towards data personal without mechanism supervision adequate, so that damages right privacy and causes potential misuse (Mak et al., 2025; Çınar & Vanberg, 2022). Study comparison also shows mechanism examination judicial and supervision independent as element key to balance need enforcement and protection privacy. Experience country other, including study case related response towards communication terrorism in England, presents lesson important: access intelligence which not limited by control law which adequate risks eroding freedom civil; conversely, procedure permission (*warrants*), audit, and transparency can maintains legitimacy action state (Hale-Ross, 2019; Yilma, 2023).

Several writings assesses policy national latest, such as draft Statute Cyber Security and Resilience, from perspective security-versus-privacy. Evaluation this affirms need for regulation which clear concerning authority access data by body security, procedure confidentiality, as well as guarantee remedial for citizen who become victim violation data (Seri Mughni Sulubara et al., 2025; Hendrawan et al., 2025). Critique other highlights need increase capacity investigator and judge in aspect forensic digital so that norm new not becomes useless because weakness implementation technical (Indradjaja et al., 2024; Arifin & Handayani, 2024). Synthetically, study literature recommends several things for policy which coherent: (1) clarifies norm KUHP related cyber so that fulfills principle legality and measurable; (2) synergizes KUHP with UU PDP and UU ITE to regulate access and usage data by apparatus; (3) enforces procedure investigation digital which guarantees chain evidence and right suspect; as well as (4) strengthens mechanism supervision independent and cooperation international. Approach this viewed necessary to ensure that modernization law criminal not sacrifices right privacy and principle ethics fundamental in enforcement law (Fajriansyah et al., 2025; Mak et al., 2025; Nieto Martín, 2022).

METHOD

Research this constitutes research juridical normative (doctrinal) which focuses on study rule law, doctrine, and literature to analyze policy law criminal digital and issue ethics-privacy in enforcement KUHP new. Approach normative chosen because goal main is examine feasibility norm, coherence inter-regulation, as well as implication normative from practice enforcement law cyber based on principles-principles law criminal and ethics law. Method this common used in study law criminal digital to combine analysis text statute, doctrine, and study literature academic.

1 Research Approach

a. Approach Statute-law (*studytory/legislative approch*)

Analysis towards texts-texts law primary such as KUHP new, Statute Information and Electronic Transactions (UU ITE), as well as Statute Personal Data Protection (UU PDP). Approach this examines element offense, scope norm criminal, clause exception, as well as relation normative inter-regulation guna identify gap and potential overlap regulation.

b. Approach Conceptual (*doctrinal/theoretical approach*)

Deconstruct concepts-concepts key such as criminalization, ultimum remedium, proportionality, legality, and principle protection privacy. Approach this relates theory politics criminal with practice enforcement cyber to evaluate whether policy which exists adheres to principle basic law criminal modern.

c. Approach Case (*case approach/case study*)

Analysis case used to give illustration empirical atas problem implementation and implication right privacy in enforcement cyber. Case chosen based on relevance, impact national, and availability source primary secondary. For research this made study case most not two incidents big which reflects problem privacy and enforcement: (1) Attack ransomware towards Center Data National / National Data Center which impacted broad on service public. which exposes problem readiness technical and governance access data; and (2) Series of leak data big which attributed on actor anonymous "Bjorka" (e.g. Claim leak NPWP and data population), which highlights issue protection data public and trust society towards governance data state. Both events this chosen because illustrates tension between need security/enforcement and right privacy citizen.

2. Legal Sorces

Material law primary: Text KUHP new (articles-articles which relevant with act criminal cyber), Statute Information and Electronic Transactions (UU ITE), Statute Personal Data Protection (UU PDP), regulation implementing, and decision court which relevant. Material primary this becomes basis interpretation norm and determination element offense.

Material law secondary: Literature academic, book reference about law criminal cyber, book teaching law procedure criminal cyber, article journal (e.g. study KUHP new, evaluation UU ITE/UU PDP, and study comparative), as well as report institution research and articles news which makes chronology case. Example literature which becomes reference includes Sangalang Farina (2024), Arifin & Handayani (2024), Winter Ruggeri (2022), as well as journals-journals analytical latest. (Sangalang & Farina, 2024; Arifin & Handayani, 2024; Fajriansyah et al., 2025).

Material law tertiary: Dictionary law, encyclopedia, and index law which helps definition term and classification concept law.

3. Data Collection Technique

a. **Inventory regulation:** Collecting official copy KUHP new, UU ITE, UU PDP, and regulation related from site official government or publication law trusted. (Husamuddin et al., 2024).

b. **Study literature:** Search and collection book, journal, article scientific, and report research through library university, database journal, as well as portal publisher. Literature which mentioned in order used as reference main to build framework theoretic and argument. (Sangalang & Farina, 2024; Arifin & Handayani, 2024).

c. **Collection data case:** Chronology and fact technical related incident ransomware and leak data collected from report news credible, statement ministry/institution related, as well as publication academic which examines event that. Source news which used will listed as reference empirical for analysis.

4. Data Analysis Data

Analysis which done is descriptive qualitative and normative, with stages main as follows:

a. **Analysis text law (*textual legal analysis*):** Reading and interpreting provision KUHP, UU ITE, and UU PDP to identify element offense, scope authority enforcer, as well as exception or limitation law which regulates access towards data personal.

b. **Analysis conceptual:** Connecting finding normative with principles-principles politics criminal, *ultimum remedium*, proportionality, and principle protection privacy to assess consistency policy.

c. **Analysis case (*case analysis*):** Comparing fact empirical from incident which chosen with framework normative which already formulated to assess practice enforcement, policy access data, and impact towards right privacy. In analysis this used model comparison chronological, identification actor, mechanism access data, impact towards victim, and response policy.

d. **System normative:** Formulating conclusion policy which integrates analysis substantive and procedural, as well as giving recommendation policy which considers balance between security public and protection right privacy.

RESULTS AND DISCUSSION

RESULTS

Digital Criminal Law Policy In New Criminal Code (KUHP)

a. Scope norm KUHP new towards crime cyber and data personal

KUHP new shows direction renewal substantive which tries bridge gap between norm criminal classic and forms-forms crime which emerges in world digital. Generally, renewal this strives to recognize that a number of acts which previously difficult to reach by KUHP old, such as access without permission to system information, damage or alteration data electronic, and use data personal for purpose fraud, requires formulation offense which more explicit and character element offense which considers element technology (Fajriansyah, Siregar & Panggabean, 2025; Sangalang & Farina, 2024).

In practice, harmonization between KUHP new and regulation sectoral (especially UU ITE and UU PDP) becomes key. KUHP provides foundation criminal general, for example provision about act which results in loss or disturbance public. While UU ITE and UU PDP regulate element technical, mechanism sanction administrative, and obligation protection data which specific. Combination this allows prosecution which more integrated: KUHP handles aspect criminal general, while UU PDP/UU ITE regulates aspect related management and access data. However, several studies highlights potential overlap or conflict norm if element offense KUHP formulated too broad so that covers domain which should be regulated by UU sectoral (Hendrawan et al., 2025; Mak, Ho & Beamount, 2025).

Besides that, KUHP new tends to adopt approach category crime cyber, differentiates act which depends on technology (e.g. hacking, sabotage system) and act which enabled or magnified by technology (e.g. fraud electronic, spread content illegal). So that formulation element offense can be more specific and measurable in context digital (Sangalang & Farina, 2024; Winter & Ruggeri, 2022).

b. Analysis articles-articles: focus on element, scope and risk interpretation broad

Analysis normative towards articles-articles relevant shows three issue main: (1) Accuracy element offense; (2) Rule proof evidence electronic, and; (3) Limitation access data by apparatus. First, element offense which clear and

measurable very important to fulfill principle legality. KUHP new strives to establish element which considers action technical (e.g. "access without right", "altering data electronic"), however still there is risk language normative which is generic so that apparatus can interpret in a way broad in practice investigation. Risk interpretation broad this implies on freedom expression and innovation technology if norm used in a way broad towards activity which actually not contained criminal (Sangalang & Farina, 2024; Fajriansyah et al., 2025).

Second, rule proof evidence electronic becomes point critical. KUHP new needs to be oriented on standard forensic digital: clarity concerning how evidence electronic collected, verified, and maintained chain storage (*chain of custody*) so that can be accepted in trial. Literature technical and juridical emphasizes need for guideline investigation digital which detailed (e.g. *standard operating procedures for digital forensics*) as well as increase capacity investigator and expert forensic so that proof not easily falls because defect procedural (Hasamuddin et al., 2024; Arifin & Handayani, 2024).

Third, issue access data by apparatus: KUHP new needs to be integrated with provision UU PDP which regulates authority access, mechanism command judicial (*warrant*), and limitation purpose collection data. Without mechanism permission which strict and supervision independent, there is potential misuse authority; for example collection metadata massive or access towards data sensitive without reason proportional, which conflicts with principle protection privacy (Mak et al., 2025; Çınar & Vanberg, 2022).

c. Direction policy enforcement law in era digital

From review articles and policy, direction enforcement which appears can be summarized as follows:

a) Harmonization regulation: Enforcement which effective requires synergy KUHP, UU ITE, and UU PDP. KUHP provides sanction criminal main, while UU sectoral regulates mechanism access and responsibility organizer system electronic. Harmonization this also demands clarity division competency between apparatus enforcer and authority protection data (Fajriansyah et al., 2025; Mak et al., 2025).

b) Strengthening procedure investigation digital: Direction policy emphasizes formation standard forensic digital national, protocol *chain of custody*

evidence electronic, and requirement permission before access towards data sensitive. Thing this aligns with recommendation literature which emphasizes importance procedure technical which standardized so that proof digital can be trusted in court (Husamuddin et al., 2024; Winter Ruggeri, 2022).

c) Prioritizing principle proportionality and *ultimum remedium*: Policy enforcement directed to apply criminal law only if step non-criminal not adequate. For case which is administrative or violation compliance technical, sanction administrative or civil prioritized; criminal law used for case with impact serious or element intent heavy. Approach this aims to prevent criminalization excessive towards activity digital which not dangerous (Nieto Martín, 2022; Sangalang & Farina, 2024).

d) Protection privacy as instrument legitimacy: Policy enforcement realizes that legitimacy action apparatus depends on respect towards right privacy. Therefore, need existence mechanism supervision independent (e.g. authority protection data) as well as mechanism remedial for victim violation data so that trust public remains maintained (Mak et al., 2025; Çınar & Vanberg, 2022).

e) Cooperation international and public-private: Considering many modes cyber are cross border, policy enforcement emphasizes expansion cooperation with country other through Mutual Legal Assistance, as well as collaboration with organizer platform and sector private for response quick towards incident (*incident response*). Besides that, policy empowerment capacity national (training, center forensic digital) becomes agenda important (Nieto Martín, 2022; Arifin & Handayani, 2024).

d. Implementative Challenges And Policy Risks

Although the direction of the policy has been identified, the literature highlights several implementative challenges: (1) The technical capacity of the apparatus is still limited; (2) The harmonization gap between substantive law and technical rules; (3) The potential for the use of articles in a repressive manner if the element of the offense is not firm enough; and (4) The lack of a specific independent oversight mechanism in the context of data access by security institutions. Without improvements on these points, the new Criminal Code risks only becoming a symbolic framework without practical effectiveness

in tackling cybercrime while still protecting civil rights (Hasamuddin et al., 2024; Fajriansyah et al., 2025; Mak et al., 2025).

Ethical Challenges in Cyber Law Enforcement

The development of digital technology expands the scope of law enforcement, but at the same time raises new ethical problems. In the context of cyber law enforcement, the apparatus has the authority to conduct tracking, wiretapping, and the collection of electronic data for the sake of uncovering digital crimes. However, this authority often creates moral dilemmas and legal ethics, especially when dealing with individual privacy rights guaranteed by the constitution and various international instruments (Mak, Ho & Beaumont, 2025; Çınar & Vanberg, 2022).

This dilemma arises because law enforcement apparatuses are faced with two equally important interests: maintaining public security through law enforcement and maintaining citizens' freedom to communicate securely in the digital world. In practice, the boundary line between legitimate investigative action and privacy violations is often blurred. For example, the process of tracing an IP address or monitoring online conversations can be considered necessary for the purpose of evidence, but without a strict judicial authorization mechanism, this action could lead to human rights violations (Winter & Rugeeri, 2022; Hasamuddin et al., 2024).

The ethics of digital criminal law enforcement demands proportionality and legitimacy of state action. Proportionality means that every intervention against privacy must be balanced with the threat of the crime being handled. Meanwhile, legitimacy requires every action by the apparatus to have a clear and accountable legal basis. This principle is also in line with the theory of criminal policy that positions criminal law as *ultimum remedium*, which is the last resort used after other legal instruments prove inadequate (Nieto Martín, 2022; Sangalang & Farina, 2024).

From a moral perspective, cyber law enforcement also raises questions about the limits of *digital surveillance* authority by the state. The state needs to enforce the law and protect the public from threats of cybercrime such as data theft, online fraud, or *ransomware*, but on the other hand, overly broad surveillance can lead to *state overreach* that damages public trust. According to Yilma (2023), without independent oversight mechanisms and public transparency, the mass collection of data by law enforcement agencies can lead to systematic human rights violation practices. In the Indonesian context, this challenge is still visible in the

implementation of the ITE Law and the PDP Law which do not yet fully regulate data access procedures by the apparatus.

The lack of clarity regarding the technical limitations of wiretapping and the absence of digital enforcement ethical standards can lead to abuse of authority. Therefore, the development of a digital law enforcement system needs to be accompanied by a code of ethics for the cyber apparatus and internal audit mechanisms that ensure all enforcement processes respect the values of justice and citizens' privacy rights (Arifin & Handayani, 2024; Fajriansyah et al., 2025).

Privacy Issues and Personal Data Protection

a. Relationship between the Criminal Code (KUHP), ITE Law, and PDP Law

Indonesia's digital criminal law policy shows an interconnected relationship between three main instruments: the new Criminal Code (KUHP), the ITE Law, and the PDP Law. The new Criminal Code functions as the general criminal legal umbrella, establishing the basic principles of criminalization and sanctions against acts that harm the public, including those occurring in the digital realm. The ITE Law serves as a sectoral rule that technically elaborates the forms of cybercrime, such as illegal content distribution, unauthorized access, or manipulation of electronic systems.

Meanwhile, the PDP Law provides special protection for individuals against the collection, storage, and dissemination of their personal data without consent (Hasamuddin et al., 2024; Mak et al., 2025). The relationship between the three must be understood as a complementary legal system. The Criminal Code emphasizes general criminal aspects and sanctions, the ITE Law provides operational provisions related to activities in cyberspace, while the PDP Law strengthens the ethical and human rights aspects in personal data protection. However, challenges arise when there is an overlap of authority and norms, especially related to investigation mechanisms and the imposition of sanctions. Several provisions in the new Criminal Code are still general in nature and may intersect with the articles of the ITE Law, for example regarding “unauthorized use of electronic systems” or “dissemination of personal data” which have been regulated more specifically in the PDP Law (Fajriansyah et al., 2025; Hendrawan et al., 2025).

International literature emphasizes the importance of harmonization between general criminal law and privacy rules. Without proper harmonization, law enforcement can become contradictory: on the one hand protecting the public from cybercrime, but on the other hand potentially violating individual privacy through overly intrusive investigation processes (Mak et al., 2025; Çınar & Vanberg, 2022). Therefore, an integrative policy approach, which unifies ethical standards, investigation procedures, and legal guarantees for privacy rights, becomes a priority in the reform of digital law enforcement in Indonesia.

b. Cases of privacy violation in *cybercrime* enforcement

One real example of privacy violation in Indonesia is related to the handling of the case of personal data *leakage* of citizens by parties claiming to be the anonymous hacker “Bjorka” in 2022 – 2023. This incident caused a wide debate regarding the limits of the state's responsibility for the protection of public data and the mechanism of law enforcement involving personal data (Hendrawan et al., 2025). In handling the case, police apparatus carried out investigations by accessing various digital data, but the process was criticized due to the absence of public information disclosure and the clarity of the legal basis for the forensic methods used. In addition, the *ransomware* attack on the National Data Center (PDN) in 2024 (which disabled some government services) also showed gaps in the security of public data and the weak oversight of access to state information systems.

The data breach at the PDN showed two important aspects: first, the weak cyber security system that caused the data of millions of citizens to be exposed; and second, the unpreparedness of the apparatus in enforcing the law quickly without violating privacy principles. In some cases, investigations were carried out by pulling data from third parties without explicit consent, which potentially conflicts with the principle of *data minimisation* in the PDP Law (Mak et al., 2025; Yilma, 2023). These cases show that privacy violations do not only originate from cybercrime itself, but can also emerge in the process of disproportionate law enforcement. Therefore, strengthening oversight mechanisms and *judicial review* becomes important so that law enforcement apparatus do not exceed the limits of authority.

The state must ensure that every investigative action against personal data is always based on a clear legal basis, a court order, and the principle of

public transparency (Winter & Ruggeri, 2022; Hale-Ross, 2019). Thus, privacy protection and the effectiveness of digital law enforcement are not two contradictory things, but must run in balance. When the apparatus works with strong ethical guidelines and respects individual rights, then the legitimacy of the state in enforcing the law in the digital era will increase. Conversely, if enforcement is carried out repressively without limitations, it does not only threaten citizens' privacy but can also reduce public trust in the legal system itself (Sangalang & Farina, 2024; Fajriansyah et al., 2025).

DISCUSSION

The results of this discussion shows that the success of digital criminal law policy depends on three pillars simultaneously: (1) Certainty and harmony of legal norms; (2) technical standards and reliable investigative capacity; and (3) strong oversight mechanisms and privacy rights guarantees. Without all three working together, the new Criminal Code (KUHP) risks becoming a substantive document that is less effective, while civil rights are actually threatened by unethical enforcement practices. With the recommendations above, it is hoped that cyber law enforcement in Indonesia can be more efficient, just, and have stronger public legitimacy.

This differs from previous reseacrh that has highlighted digital issues in the context of the Electronic Information and Transactions Law and the Personal Data Protection Law. For example, reseacrh by Afifah Rizqy Widianingrum (2024) focused more on the implementation of legal policies for handling cybercrime in the digital era. Meanwhile, research by Zainuddin Kasim (2023) emphasized criminal law policies for combinating cybercrime in Indonesia. Unlike these studies, this article specifically examines the direction of digital criminal law policy in addressing ethical and privacy cahllenges in the New Criminal Code regarding crybercrime.

CONCLUSION

This writing shows that the new Criminal Code (KUHP) marks an important step toward the renewal of Indonesian criminal law that is responsive to digital reality: the new Criminal Code begins to recognize forms of crime rooted in information technology and opens space for enforcement against cybercrimes that were previously difficult to handle by the old Criminal Code (Sangalang & Farina, 2024; Fajriansyah et al., 2025). However, the current position of digital criminal law is complementary: the Criminal Code functions as the framework for general criminal substance while the ITE Law and the PDP Law play a sectoral role that regulates

technical aspects, administrative sanction mechanisms, as well as personal data protection. The analysis found significant implementative barriers. First, there is a gap in the harmonization of norms and terms between the Criminal Code, the ITE Law, and the PDP Law which causes legal uncertainty and the potential for broad interpretation by the apparatus.

Second, digital forensic procedures and standards for proving electronic evidence have not been well institutionalized, thereby reducing the reliability of the enforcement process. Third, the technical capacity of the apparatus, mechanisms for access oversight, data, and remedial pathways for victims are still weak, conditions that risk harming privacy rights and the legitimacy of law enforcement. Consequently, without technical and normative improvements, the new Criminal Code has the potential to become a symbolic framework that is less effective or, worse, used repressively against civil liberties. Normatively, these findings affirm that the effectiveness of cyber enforcement is not just about criminalization, but about the combination of substantive norms, reliable investigative procedures, ethical guarantees, and oversight mechanisms that protect privacy, a balance that is a pre-condition for public legitimacy toward criminal policy.

REFERENCES

Anjheli, D. (2023). *Digital privacy and phishing crime in Indonesia: Critical evaluation of the effectiveness of the ITE Law and the PDP Law. Staatsrecht: Journal of Constitutional Law and Islamic Politics.*

Arifin, Z., & Handayani, E. P. (2024). *Cybercrime: Investigating law enforcement and its countermeasures. Yogyakarta: Deepublish Digital.*

Çınar, Ö. H., & Vanberg, A. D. (Eds.). (2022). *The right to privacy revisited: Different international perspectives. London: Routledge.*

Fajriansyah, A., Siregar, R. A., & Panggabean, M. L. (2025). *Criminal law reform in the digital era: Analysis of the new Criminal Code (KUHP). Jurnal Hukum Mimbar Justitia, 11(1).*

Hale-Ross, S. (2019). *Digital privacy, terrorism and law enforcement: The UK's response to terrorist communication*. London: Routledge.

Hendrawan, A. R., Ramadhan, B. D. A., Hiahdar, B. A., & Triana, T. (2025). Legal protection for victims of digital crime in the perspective of the ITE Law and the Criminal Code (KUHP). *Causa: Journal of Law and Citizenship, 7*(2).

Husamuddin, M. Z., Efendi, S., Hamdi, S., et al. (2024). *Criminal procedure law & cybercrime: Textbook*. Jakarta: PT. Media Penerbit Indonesia.

Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementation of investigation against cybercrime in the perspective of comparative law: Indonesia and the United Kingdom. *Jurnal Ilmiah Penegakan Hukum, 6*(2).

Mak, A., Ho, C. H., & Beaumont, P. (Eds.). (2025). *Privacy and personal data protection law in Asia*. Oxford: Hart Publishing.

Martín, A. N. (2022). *Global criminal law: Postnational criminal justice in the twenty-first century*. Cham: Springer.

Sangalang, R. S., & Farina, T. (2024). *Cyber criminal law: Reference book*. Jakarta: PT. Media Penerbit Indonesia.

Sulubara, S. M., Tasril, V., & Nurkhalisah, N. (2025). *Legal protection against cybercrime from ransomware attacks and evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's defense*. *Aliansi: Journal of Law, Education and Social Humanities, 5*(1).

Winter, L. B., & Ruggeri, S. (Eds.). (2022). *Investigating and preventing crime in the digital era: New safeguards, new rights*. Cham: Springer.

Yilma, K. (2023). *Privacy and the role of international law in the digital age*. Oxford: Oxford University Press.