The Easta Journal Law and Human Rights
Vol. 5, No. 01, October 2026, pp. 12 – 21
ISSN: 2985-7112, DOI: 10.58812/eslhr.v5i01

Criminal Law Analysis of the Use of Substitute Driver Identities in Electronic Traffic Law Enforcement (ETLE)

Feri Prasetyo[1], Waty Suwarty Haryono[2], Uyan Wiryadi[3]
[1,2,3] Universitas Krisnadwipayana Jakarta

Article Info

Article history:

Received Oct, 2026
Revised Oct, 2026
Accepted Oct, 2026

Keywords:

Law Enforcement;
Substitute Drivers;
Identity Misuse;
Criminal Liability;
Electronic Traffic Law Enforcement (ETLE)

ABSTRACT

The development of Electronic Traffic Law Enforcement (ETLE) as a form of digitalized traffic law enforcement has facilitated the handling of traffic violations. In practice, however, substitute driver identities have been misused to transfer responsibility for traffic violations to other people. This conduct not only undermines enforcement effectiveness but may also satisfy the elements of criminal offenses such as document forgery, use of forged documents, and electronic data manipulation. This study addresses two questions: What forms of criminal liability apply to perpetrators who misuse driver identities in the electronic traffic ticketing (ETLE) system? How are criminal law provisions concerning the use of substitute driver identities in ETLE applied in judicial practice? The research adopts normative legal research (doctrinal research). The findings indicate that perpetrators may be held criminally liable where they are proven to have committed an unlawful act intentionally, possess the capacity for responsibility, and have no applicable justification or excuse. Normatively, such conduct may be prosecuted under the provisions on document forgery in the Criminal Code, electronic data manipulation under the Electronic Information and Transactions Law, or other provisions concerning identity misuse and population administration, depending on the characteristics of the conduct. In judicial practice, judges have applied criminal law provisions to substitute driver identity cases by considering electronic evidence, documents, witness testimony, and facts established at trial. Nevertheless, the absence of provisions specifically criminalizing identity misuse during ETLE confirmation leaves legal application dependent on the interpretations of enforcement officials and judges, potentially producing inconsistent judgments. Regulatory reform, stronger law enforcement capacity, improved ETLE technology, and public education are therefore necessary to achieve legal certainty, justice, and effective electronic traffic law enforcement.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Name: Waty Suwarty Haryono
Institution: Universitas Krisnadwipayana Jakarta
Email: profwatyharyono@gmail.com

1. INTRODUCTION

In practice, the implementation of ETLE raises legal issues, particularly regarding the identification of traffic offenders. Not all violations are committed by vehicle owners. Vehicles may be used by other people, creating a distinction between

the registered owner and the driver who actually committed the violation. This situation creates opportunities for the misuse of driver identities [1], [2].

One form of misuse involves using a substitute driver's identity. Under this practice, the person who committed the violation refuses to acknowledge the act and instead uses another person's identity to avoid sanctions. This may involve forging documents or providing false information during the ETLE violation confirmation process. Such conduct goes beyond an ordinary traffic violation and enters the realm of criminal offenses [3].

From the perspective of criminal law, the use of a false identity may constitute document forgery as regulated under the Indonesian Criminal Code (KUHP). An essential element of this offense is the creation or use of a forged document with the intention of producing legal consequences. In the ETLE context, the use of a substitute driver's identity demonstrates an intention to evade legal responsibility and thus satisfies the element of intent [4], [5].

The principal issue concerns criminal liability. Criminal law requires that an offender be at fault before being held criminally liable [6]. ETLE cases may involve several parties: the vehicle owner, the actual driver, and the person using or creating the false identity. Determining which party should be held liable therefore requires in-depth legal analysis [7].

The evidentiary aspect is equally important. ETLE relies on electronic evidence in the form of camera recordings. Under criminal procedural law, electronic evidence is recognized as admissible evidence, subject to certain requirements [8]. When identity misuse occurs, the evidence must establish not only the traffic violation but also the forgery or use of a false identity. This requires careful evaluation of the relationship between the electronic evidence and the offender's identity [9]–[11].

From the standpoint of criminal law theory, this issue relates to the principle of fault, the principle of criminal liability, and the purposes of punishment. The use of a substitute driver's identity indicates a deliberate act intended to avoid legal sanctions. It is therefore necessary to examine how criminal law regulates and evaluates such conduct within the ETLE system. This study focuses on a criminal law analysis of the use of substitute driver identities in electronic traffic enforcement (ETLE). It also examines offenders' criminal liability and judges' legal considerations in relevant court decisions [12].

Based on the foregoing discussion, the author is interested in conducting research presented as a thesis entitled "Criminal Law Analysis of the Use of Substitute Driver Identities in Electronic Traffic Law Enforcement (ETLE)."

2. RESEARCH METHOD

This study employs normative legal research (doctrinal research), focusing on the examination of legal norms found in legislation, court decisions, and legal scholarship. It seeks to identify the legal rules, principles, and concepts relevant to the use of substitute driver identities in the electronic traffic enforcement (ETLE) system, thereby enabling an analysis of the forms of criminal liability and the application of the law in judicial practice [13].

This study is descriptive-analytical in nature, aiming to provide a systematic, factual, and accurate account of legal provisions and practices involving identity misuse in the ETLE system, while analyzing the resulting legal issues. Under this approach, the researcher not only describes applicable legal norms but also analyzes their implementation in court decisions to assess the consistency between theory and practice [14], [15].

3. RESULTS AND DISCUSSION

3.1 Forms of Criminal Liability for Perpetrators of Driver Identity Misuse in the Electronic Traffic Law Enforcement (ETLE) System

The electronic traffic ticketing system, or Electronic Traffic Law

Enforcement (ETLE), is an innovation in traffic law enforcement introduced nationally by the Indonesian National Police as part of bureaucratic reform and the digitalization of public services. The system uses artificial intelligence-based closed-circuit television (CCTV) cameras to detect traffic violations automatically, record vehicle registration plates, and send violation confirmation notices to vehicle owners registered in the integrated One-Stop Vehicle Administration System (SAMSAT) database. As a result, enforcement no longer requires direct interaction between police officers and offenders in the field, theoretically reducing illegal levies and bribery associated with conventional traffic ticketing [16], [17].

Under Indonesian criminal law, these acts do not exist in a legal vacuum. Various statutory instruments can be used to establish the criminal liability of individuals who misuse identities within the ETLE system, including the Criminal Code (KUHP), Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions (the ITE Law), Law Number 22 of 2009 concerning Road Traffic and Transportation (the LLAJ Law), and regulations on population administration. A thorough analysis of these forms of criminal liability is particularly important because rapid developments in information technology are not always matched by corresponding legal regulation [18]–[20].

Before analyzing criminal liability for identity misuse in ETLE, it is necessary to understand the theoretical framework of criminal liability under Indonesian law. Criminal liability (strafbaarheid van de dader) refers to the condition in which a person may be held responsible for a criminal act committed. In criminal law doctrine, liability requires the cumulative fulfillment of several elements [5], [7].

First, there must be a criminal act (*actus reus*), namely conduct that satisfies the statutory definition of an offense. In the context of ETLE identity misuse, such acts may include document forgery, the use of false identities, manipulation of electronic data, or the use of improper registration plates. Second, the offender must have the capacity to be held responsible, understood in Indonesian criminal law as having a sound mental condition and being capable of understanding the unlawful nature of the conduct. Third, there must be fault (*mens rea*), whether in the form of intent (*dolus/opzet*) or negligence (*culpa*). Identity misuse in ETLE is generally intentional because the offender desires and is aware of the consequences. Fourth, there must be no excuse that eliminates the offender's culpability, such as necessity (noodtoestand), insanity, or duress (overmacht) [5].

Under this framework, a person's misuse of another driver's identity in the ETLE system—whether through data falsification, shifting responsibility for a traffic ticket to an innocent person, or using a false registration plate—may in principle satisfy all the elements of criminal liability. The challenge is to identify precisely which statutory provisions are the most relevant and effective to apply [1], [3].

The Criminal Code (KUHP), as the lex generalis of Indonesian criminal law, contains several provisions relevant to the misuse of driver identities in the ETLE system [4].

First, document forgery under Article 263 of the Criminal Code is among the most relevant offenses. The provision prescribes imprisonment of up to six years for anyone who falsely produces or forges a document that creates a right, obligation, or discharge of debt, or serves as evidence of a matter, with the intention of using it or having

someone else use it. In the ETLE context, forgery may occur when an individual falsifies a driver's identity document, certificate, or vehicle ownership document to deceive officials or the system. Article 264 of the Criminal Code likewise regulates the forgery of authentic instruments, carrying a heavier penalty of up to eight years' imprisonment [4].

Second, fraud under Article 378 of the Criminal Code may apply when a person intentionally uses a false name or false status, deception, or a series of lies to induce another person to surrender property, grant credit, acknowledge a debt, or cancel a receivable. An identity misuse scheme intended to transfer liability for a traffic ticket to another person and thereby cause that person material loss may fall within this category of fraud. The applicable maximum prison sentence is four years [4], [5].

Third, the provisions on identity-related fraud under Article 378 in conjunction with Article 55 of the Criminal Code concerning participation (deelneming) are also relevant when identity misuse is committed jointly or when another party assists or facilitates the forgery. For example, an individual who helps someone alter vehicle ownership information in the SAMSAT or National Police Traffic Corps (Korlantas Polri) database may be held liable as a participant or an accomplice [4], [7].

Fourth, Article 406 of the Criminal Code on damage to property may apply to misuse schemes involving physical damage to or tampering with ETLE cameras or system infrastructure. Although this is less common, it is a form of misconduct that should be anticipated [4].

Articles 274 and 275 of the Road Traffic and Transportation Law regulate road use that disrupts traffic order and safety. More broadly, abuse of the ETLE system that interferes with traffic law enforcement may also be regarded as a violation of traffic order [20].

It should be noted that criminal provisions under the Road Traffic and Transportation Law generally prescribe lighter penalties than the Criminal Code or the ITE Law. Nevertheless, the Road Traffic and Transportation Law has the advantage of being a lex specialis directly governing traffic offenses, making its application more specific and targeted. In practice, prosecutors frequently combine charges under this law with provisions of the Criminal Code or the ITE Law to establish a more comprehensive basis for criminal prosecution [20].

Law Number 23 of 2006 in conjunction with Law Number 24 of 2013 concerning Population Administration (the Population Administration Law) also contains relevant provisions, particularly when identity misuse in ETLE involves the forgery of population documents such as identity cards (KTP), family cards (KK), or other civil registration documents [21], [22].

Under Indonesian criminal law, the form of fault significantly affects the classification of an offense and the degree of criminal liability. In ETLE identity misuse cases, an analysis of culpability indicates that almost all the methods described above involve intent (dolus/opzet) rather than negligence (culpa). This means offenders consciously intend the outcome of their actions and know that their conduct is unlawful [5], [7].

More specifically, in many ETLE identity misuse cases, the offender acts with *opzet als oogmerk* (direct intent as a purpose), rather than merely *opzet bij zekerheidsbewustzijn* (intent based on awareness of certainty) or *opzet bij mogelijkheidsbewustzijn* (intent based on awareness of possibility). This is because the offender's direct objective is to transfer traffic-ticket liability to another person or manipulate the system for personal gain [5].

The classification of fault is important because it affects sentencing severity. In delivering a judgment, judges consider not only whether the elements of an offense have been established but also the offender's degree of fault, the impact on victims and the public, and any mitigating or aggravating circumstances. Fully intentional ETLE identity misuse, particularly when repeated or organized, warrants appropriately severe punishment to deter further offenses and protect the integrity of law enforcement [5].

An often-overlooked aspect is the perspective of victims of ETLE identity misuse. People whose identities are misused may suffer various losses: financial losses from fines imposed for violations they did not commit; administrative losses through traffic violation records that may affect driver's license renewal; and non-material losses from damage to their reputation and dignity [2].

Within Indonesian criminal law, victims have the right to seek restitution or compensation under the mechanisms provided by Law Number 31 of 2014 concerning Witness and Victim Protection, as well as through a civil claim brought alongside criminal proceedings (voegen). In addition, during prosecution, the prosecutor may include a compensation claim for the victim as part of the requested court order [23].

From an institutional perspective, the National Commission on Human Rights (Komnas HAM) and the Ombudsman of the Republic of Indonesia may also become involved where ETLE identity misuse entails poor public services or human rights violations, for example when someone is arrested or harshly sanctioned because their identity has been misused without an adequate mechanism for clearing their name [24].

Although various legal instruments are available to prosecute perpetrators of ETLE identity misuse, law enforcement faces several practical challenges [12].

The first challenge concerns evidence. Proving information technology-related crimes requires specialized technical expertise that law enforcement officials at every level may not possess. Digital forensic experts are needed to analyze digital traces, system logs, and metadata to establish that someone has manipulated information in the ETLE system. Indonesia still has limited human resources and digital forensic infrastructure, particularly outside major cities [10], [25].

The second challenge is interagency coordination. The ETLE system involves numerous institutions—including the National Police Traffic Corps, SAMSAT, population and civil registration offices (Disdukcapil), and banking institutions—each with its own systems and databases. Investigating ETLE identity misuse requires cross-agency database access, which is frequently obstructed by bureaucracy and system incompatibility [2], [17].

The third challenge is a regulatory gap. Although the ITE Law, the Criminal Code, and the Road Traffic and Transportation Law provide an adequate legal basis, no regulation specifically governs the criminal offense of identity misuse in electronic traffic ticketing. This absence of specific provisions can create legal uncertainty during investigations and prosecutions [3].

Several recommendations can be offered to address these challenges. First, implementing regulations specifically governing offenses within the ETLE system should be issued promptly, whether in the form of government regulations, National Police Chief regulations, or a separate law if necessary. Second, the National Police should strengthen investigators' digital

forensic expertise to handle technology-based identity misuse. Third, the ETLE system should incorporate more robust driver identity verification mechanisms, for example through integration with more accurate facial recognition technology. Fourth, a clear and effective complaint mechanism should be established for citizens whose identities have been misused in ETLE, ensuring adequate protection of victims' rights [17].

3.2 Application of Criminal Law Provisions to the Use of Substitute Driver Identities in the Electronic Traffic Law Enforcement (ETLE) System in Judicial Practice

The application of criminal law provisions to offenses involving substitute driver identities in the Electronic Traffic Law Enforcement (ETLE) system is an emerging legal issue accompanying the digitalization of traffic law enforcement in Indonesia. Unlike conventional ticketing, which involves direct interaction between police officers and offenders, ETLE uses electronic cameras to record traffic violations automatically by identifying vehicles through their motor vehicle registration numbers (NRKB). Consequently, violation confirmation notices are sent to the owners listed in vehicle registration records rather than to the drivers who actually committed the violations. This creates opportunities for identity misuse by transferring responsibility to another person who did not commit the offense [3].

A recurring practical problem is that ETLE camera recordings do not always clearly identify drivers' faces. In such cases, law enforcement officials must gather additional evidence through witness examinations, vehicle data matching, mobile phone examinations, other CCTV footage, or electronic evidence establishing the offender's presence at the time of the violation. Thus, the application of criminal law to ETLE identity misuse depends heavily on the quality of digitally supported investigations [3], [25].

The application of criminal law in such cases must also respect the principle of geen straf zonder schuld, or no punishment without fault. This means a person may be punished only when legally and convincingly proven to have acted with the intent or negligence required by law. If someone's identity was merely borrowed without their knowledge that it would be used in an ETLE confirmation, that person cannot be held criminally liable because the element of fault is absent. By contrast, the person who deliberately uses that identity remains liable as the principal offender [6], [7].

In judicial practice, judges generally assess several essential factors before issuing a decision: the existence of an unlawful act, the offender's capacity for responsibility, the element of intent, and the absence of justifications or excuses. When all these elements are fulfilled, the defendant may be punished under the relevant provisions. Conversely, where the identity of the actual offender remains in doubt, the principle of *in dubio pro reo* requires a judgment favorable to the defendant [7].

Another practical problem is the absence of specific rules expressly criminalizing the use of substitute driver identities within the ETLE system. Accordingly, law enforcement officials continue to rely on interpretations of existing criminal provisions. This creates the possibility of differing legal applications across cases because investigators, prosecutors, and judges may construct different legal interpretations of the same conduct. Specific legal norms governing identity misuse in electronic law enforcement are therefore needed to provide legal certainty [2], [3].

The application of criminal law to the use of substitute driver identities also performs an important preventive function. Criminal penalties are intended

not only to punish offenders but also to generate a deterrent effect that discourages identity manipulation during ETLE procedures. The success of ETLE depends greatly on the public's honesty in providing accurate information to law enforcement. If identity manipulation is tolerated without firm enforcement, ETLE's primary goal of objective, transparent, and accountable traffic law enforcement will be difficult to achieve [12], [26].

The theory of criminal liability rests on the principle that an individual may be punished only upon committing an act that satisfies every element of a criminal offense and involves personal fault (schuld). This is known as the principle of *geen straf zonder schuld* (no punishment without fault). In the context of substitute driver identities in Electronic Traffic Law Enforcement (ETLE), establishing liability requires more than proving identity manipulation: the connection between the conduct, the offender's capacity for responsibility, the element of fault, and the absence of grounds excluding criminal liability must also be proven [7].

According to Moeljatno's theory of criminal liability, a person can be held responsible only after committing a criminal act involving fault that is blameworthy under the law. Such fault may take the form of intent (*dolus*) or negligence (*culpa*). In cases involving substitute driver identities in ETLE, intent is the predominant form of fault because the perpetrator knowingly submits another person's identity through the ETLE confirmation system to evade legal sanctions despite knowing that the person identified was not the driver who committed the violation [6].

According to Soerjono Soekanto, successful law enforcement is influenced by five factors: the law itself (legal substance), law enforcement officers, facilities and infrastructure, society, and culture. These factors are interconnected and determine the effectiveness of legal action against identity misuse in the ETLE system [24], [26].

a. Legal Factors (Legal Substance)

In terms of legal substance, the rules concerning substitute driver identities in ETLE remain fragmented. ETLE regulations primarily address procedures for enforcing traffic violations, while specific provisions governing identity forgery or manipulation in ETLE confirmations are not yet available. Consequently, law enforcement officials must rely on general criminal provisions of the Criminal Code, including false statements, forgery, or participation, as well as provisions of the ITE Law when manipulation occurs through electronic systems [3].

This situation demonstrates that a legal gap remains at the normative level. Consequently, the application of the law depends heavily on the interpretations of investigators, prosecutors, and judges. Such differences in legal construction may lead to inconsistent judicial decisions and diminish legal certainty [2].

b. Law Enforcement Factors

Law enforcement officers play an important role in the success of the ETLE system. Police investigators must possess digital forensic skills to identify actual offenders, especially when identities have been manipulated in the system. Public prosecutors must be capable of framing appropriate charges based on electronic evidence, while judges must be able to assess the validity of digital evidence in accordance with criminal procedural law [10], [25].

In practice, a common obstacle is the limited technical capacity of officials to uncover electronic data manipulation. Not all investigators have sufficient digital forensic competence, making it more difficult to prove identity misuse than conventional criminal offenses [17], [25].

c. Facilities and Infrastructure Factors

Effective enforcement through ETLE is strongly influenced by the quality of the technology used. ETLE cameras must capture sufficiently clear images for reliable driver identification. Integrated databases connecting police, population administration, and vehicle registration systems are also required to enable prompt and accurate identity verification [17].

In practice, camera footage may still be limited by weather conditions, lighting, camera angles, or heavily tinted windows. As a result, officials depend more heavily on vehicle owners' declarations during ETLE confirmations. Perpetrators exploit this weakness to substitute another identity for that of the actual driver [3].

d. Societal Factors

Public legal awareness is a decisive factor in ETLE's effectiveness. Some members of the public still consider replacing a driver's identity acceptable as long as the fine is paid. In fact, this constitutes information manipulation that obstructs law enforcement and contradicts the principle of honesty [26].

A weak culture of legal compliance means that ETLE's objective of achieving impartial law enforcement has not been fully realized. Accordingly, in addition to a repressive approach through criminal punishment, a preventive approach is needed to educate the public about the criminal consequences of identity misuse [26].

e. Cultural Factors

Indonesia's legal culture continues to be influenced by family ties and strong social tolerance. Many family members are willing to lend their identities to help relatives avoid legal consequences. From a criminal law perspective, this practice undermines equality before the law because legal responsibility is transferred to someone other than the actual offender [26].

A permissive culture regarding identity manipulation must be transformed into a legal culture that upholds honesty and accountability. ETLE is built on the expectation that the public will provide truthful information to the state. Without such a culture, the effectiveness of ETLE as a modern law enforcement system will continue to face obstacles [26].

Based on Soerjono Soekanto's theory of law enforcement, the application of criminal law to substitute driver identities in ETLE can be considered suboptimal because it remains affected by weaknesses in legal substance, limited official competence, uneven availability of technological facilities, low public legal awareness, and a legal culture that tolerates identity manipulation. Optimizing enforcement

therefore requires regulatory reform specifically criminalizing identity misuse in ETLE, strengthening the capacity of law enforcement officials in digital evidence, improving ETLE technology infrastructure, and expanding public legal education and awareness. ETLE could thus serve not only as an instrument for sanctioning traffic violations but also as a means of enforcing the law in a manner that promotes justice, legal certainty, and public benefit [17], [26].

4. CONCLUSION

Misuse of driver identities in the electronic traffic ticketing (ETLE) system is a serious criminal offense that threatens the integrity of technology-based traffic law enforcement in Indonesia. Based on the legal analysis presented, perpetrators may be held criminally liable under various applicable legal instruments: Articles 263, 264, 378, and 242 of the Criminal Code on forgery and fraud; Articles 30, 32, and 35 of the ITE Law on unlawful access and electronic data manipulation; Article 280 of the Road Traffic and Transportation Law on the use of unauthorized registration plates; and Articles 77 and 93 of the Population Administration Law on the misuse and manipulation of population data. These provisions may be applied individually or cumulatively depending on the offender's modus operandi, with intent being the predominant form of fault across the identified methods. Accordingly, the Indonesian legal framework is normatively sufficient to reach such offenders, although its practical effectiveness continues to face serious challenges in digital evidence gathering, interagency coordination, and the availability of personnel skilled in cyber forensics [18], [20], [21], [27].

The application of criminal law to the use of substitute driver identities in the Electronic Traffic Law Enforcement (ETLE) system already has a legal basis in the Criminal Code (KUHP), Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, and the provisions on participation and criminal liability. Nevertheless, the absence of specific criminalization of identity misuse during ETLE confirmation means that the application of these provisions still depends on interpretations by law enforcement officials and judges, potentially producing divergent outcomes in judicial practice. Under the theory of criminal liability, perpetrators may be held responsible if their conduct is proven unlawful and intentional, they possess the capacity for responsibility, and no justification or excuse applies. Under the theory of law enforcement, the effectiveness of enforcement against this offense is still affected by insufficient legal substance, the quality of law enforcement personnel, ETLE infrastructure and technology, public legal awareness, and a legal culture that remains permissive toward shifting responsibility. Regulatory reform and a stronger law enforcement system are therefore needed to address identity misuse in ETLE more effectively and promote legal certainty, justice, and utility in electronic traffic law enforcement [28].

REFERENCES

[1] D. R. Cahyati, I. Januardy, and R. Sangalang, "Tilang Elektronik sebagai Mekanisme Pencegahan Kejahatan Lalu Lintas: Analisis Kriminologis atas Pertanggungjawaban Pemilik Kendaraan," *Al-Zayn J. Ilmu Sos. Huk.*, vol. 4, no. 2, pp. 4957–4971, 2026, doi: 10.61104/alz.v4i2.3701.

[2] K. A. Sidrajat, Syachdin, and Ansar, "Kepastian Hukum Administratif dalam Penerapan Electronic Traffic Law Enforcement (ETLE) terhadap Pemilik Kendaraan di Wilayah Polda Sulawesi Tengah," *Zaaken J. Civ. Bus. Law*, vol. 7, no. 1, pp. 98–114, 2026, doi: 10.22437/zaaken.v7i1.54418.

[3] Z. Andrian, "Criminal Liability for Traffic Violations Based on Electronic Recorded Evidence under Indonesia's Electronic Traffic Law Enforcement System," *J. Perad. Huk.*, vol. 4, no. 2, pp. 212–232, 2026, doi: 10.33019/jph.v4i2.630.

[4] A. Hamzah, *Hukum Pidana Indonesia*. Jakarta: Sinar Grafika, 2017. [Online]. Available:

https://jdih.kejaksaan.go.id/buku/view?id=1234

[5] E. O. S. Hiariej, *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka, 2016. [Online]. Available: https://library.iblam.ac.id/index.php?id=21315&p=show_detail

[6] Moeljatno, *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2008. [Online]. Available: https://simpus.mkri.id/opac/detail/5490

[7] C. Huda, *Dari Tiada Pidana Tanpa Kesalahan Menuju kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan: Tinjauan Kritis terhadap Teori Pemisahan Tindak Pidana dan Pertanggungjawaban Pidana*. Jakarta: Kencana, 2006. [Online]. Available: https://jdih.kejaksaan.go.id/buku/view?id=1423

[8] A. Chazawi, *Hukum Pembuktian Tindak Pidana Korupsi*. Malang: Bayumedia Publishing, 2011. [Online]. Available: https://inlislite.ebookbanyuwangi.id/opac/detail-opac?id=5139

[9] A. Hamzah, *Hukum Acara Pidana Indonesia*. Jakarta: Sinar Grafika, 2013. [Online]. Available: https://inlislite.ipdn.ac.id/opac/detail-opac?id=17472

[10] A. H. Samudra, S. Basu, and C. Saenz Perez, "Digital Challenge, Analogue Mind-set: Assessing Indonesia's Electronic Criminal Evidence Framework," *J. Indones. Leg. Stud.*, vol. 11, no. 1, pp. 257–298, 2026, doi: 10.15294/jils.v11i1.35378.

[11] L. Wulandari, "Kekuatan Pembuktian Alat Bukti Elektronik dalam Perkara Pidana di Indonesia," *RETORIKA J. Law, Soc. Humanit.*, vol. 3, no. 1, pp. 33–46, 2024, doi: 10.69503/retorika.v3i1.1572.

[12] F. N. Djaya, Andika, and M. Radith, "Menegakkan Supremasi Hukum: Analisis Hukum Pidana, Sistem Peradilan, dan Peran Penegak Hukum," *J. Soc. Commun. Terekam Jejak*, vol. 1, no. 1, pp. 72–86, 2025, [Online]. Available: https://journal.terekamjejak.com/index.php/jsc/article/view/317

[13] J. Ibrahim, "Teori dan metodologi penelitian hukum normatif," *Malang Bayumedia Publ.*, vol. 57, no. 11, 2006.

[14] Amiruddin and Z. Asikin, *Pengantar Metode Penelitian Hukum*. Jakarta: Rajawali Pers, 2012. [Online]. Available: https://jdih.bpk.go.id/Dokumen/Monografi/F1F9B35D-3AEA-417D-BE44-401A01F41A98

[15] B. Sunggono, *Metodologi Penelitian Hukum*. Jakarta: Rajawali Pers, 2013. [Online]. Available: https://ekatalogperpus.bnn.go.id/index.php?id=642&keywords=&p=show_detail

[16] Chaerudin, S. A. Dinar, and S. Fadillah, *Strategi Pencegahan dan Penegakan Hukum Tindak Pidana Korupsi*. Bandung: Refika Aditama, 2008. [Online]. Available: https://jdih.bpkp.go.id/page/monografi/5469

[17] F. Tjahyono, D. Purwoko, and D. D. Kusumaningrum, "Dinamika Penerapan Electronic Traffic Law Enforcement (ETLE) dalam Rangka Mewujudkan Kamseltibcarlantas," *J. Litbang Polri*, vol. 28, no. 3, pp. 186–202, 2025, doi: 10.46976/litbangpolri.v28i3.323.

[18] Republik Indonesia, *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia, 2008. [Online]. Available: https://www.peraturan.go.id/files/UU%2B11%2BTahun%2B2008.pdf

[19] Republik Indonesia, *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia, 2016.

[20] Republik Indonesia, *Undang-Undang Nomor 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan*. Jakarta: Pemerintah Republik Indonesia, 2009.

[21] Republik Indonesia, *Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan*. Jakarta: Pemerintah Republik Indonesia, 2006. [Online]. Available: https://www.peraturan.go.id/files/uu23-2006.pdf

[22] Republik Indonesia, *Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan*. Jakarta: Pemerintah Republik Indonesia, 2013.

[23] Republik Indonesia, *Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban*. Jakarta: Pemerintah Republik Indonesia, 2014. [Online]. Available: https://peraturan.go.id/files/uu31-2014bt.pdf

[24] L. M. Friedman, *Sistem Hukum: Perspektif Ilmu Sosial*. Bandung: Nusa Media, 2011. [Online]. Available: https://balaiyanpus.jogjaprov.go.id/opac/detail-opac?id=282517

[25] Jovanza and T. Kartika, "The Admissibility of Digital Forensic Evidence in Proving Cybercrimes in Indonesia: An Analysis of the Principles of Authenticity and Chain of Custody," *IBLAM Law Rev.*, vol. 6, no. 3, pp. 15–25, 2026, doi: 10.52249/ilr.v6i3.714.

[26] S. Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Pers, 2014. [Online]. Available: https://slims.pknstan.ac.id/index.php?id=11381&p=show_detail

[27] Republik Indonesia, *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia, 2024.

[28] Indonesia, *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Pemerintah Republik Indonesia, 2023.