GLOBAL ENGINEERING INSIGHTS
Vol. 1 No. 2 (November 2026)

Legal and Regulatory Framework for Information Technology-Based Lawful Interception in Indonesia: Authorization Procedures, Digital Privacy, and Civil Liability

I Kadek Edi Dharmawan[1]*
Muhammad Abkur Anggarullah[2]
* Business Law Study Program, Pelita Ibu University, Indonesia
Corresponding mail id : ikdkedi.dharmawan@gmail.com

Abstract
Indonesia now holds two pieces of a modern interception regime but not the piece that connects them. Law No. 27 of 2022 on Personal Data Protection gives individuals enforceable data rights, and Law No. 20 of 2025 on the Code of Criminal Procedure, in force since January 2026, recognizes interception as a coercive measure. Article 136(2) of the latter, however, leaves the entire procedure to a separate interception statute that has not been enacted. The gap matters in practice. Amnesty International documented spyware imports by Indonesian state agencies between 2017 and 2023, the June 2024 ransomware attack on the Temporary National Data Center disrupted 239 government users, and the 2024 Salt Typhoon intrusion showed that lawful interception systems themselves are prime targets. This article asks how Indonesian law allocates interception authority, which IT governance controls are needed to make interception auditable, and what civil remedies exist for people who are intercepted unlawfully. Using normative legal research with statutory, conceptual and comparative approaches, supported by a Scopus-indexed literature base and a coding of nine safeguards across five statutes, the study finds that no statute sets prior independent approval, maximum duration, security and logging duties, deletion or notification for interception generally. It also shows that the right to compensation in Article 12 of the Personal Data Protection Law falls outside the law-enforcement exemption in Article 15, and that Article 15 of the Telecommunications Law presumes operator fault. The article proposes a five-layer Regulatory Governance Model for Lawful Digital Interception (RG-LDI) linking authorization, access control, a tamper-evident audit trail, data protection and civil remedies through a single warrant identifier.

Keyword: *lawful interception, digital privacy, civil liability, IT governance, audit trail, personal data protection, Indonesia*

I. INTRODUCTION

In May 2024, Amnesty International's Security Lab published evidence that highly invasive spyware and other surveillance products had been imported into or deployed in Indonesia between 2017 and 2023, by private companies and by state bodies that included the National Police and the National Cyber and Crypto Agency (BSSN) [1]. Much of the equipment passed through brokers in Singapore, and the supply chain was hard to trace. A month later, on 20 June 2024, a Brain Cipher ransomware attack took down the Temporary National Data Center (PDNS 2) in Surabaya. By 26 June the government reported that 239 user institutions were affected, including 30 ministries and agencies, 15 provinces, 148 regencies and 48 cities, while only 43 users that kept backup copies there escaped disruption [2]. The attackers reportedly demanded a ransom of USD 8 million [3]. Fig-1 summarizes the reported impact.

A third event, outside Indonesia, ties these two together. In late 2024 United States authorities confirmed that the China-linked group known as Salt Typhoon had broken into several major telecommunications providers and reached the systems those companies use to carry out court-ordered wiretaps [4], [5]. The very infrastructure built for lawful interception became the point of entry. Security researchers had warned for years that mandated access creates new vulnerabilities [6]. Salt Typhoon turned that warning into a documented incident.

Read together, the three events define the problem this article addresses. Indonesian state agencies already hold intrusive interception tools, the state has struggled to secure its own data infrastructure, and interception systems are now known to be attractive targets. Yet the legal framework that should govern how those tools are authorized, operated, secured and audited is still missing. Law No. 20 of 2025 on the Code of Criminal Procedure (KUHAP), in force since 2

January 2026, lists interception as a coercive measure, but its Article 136(2) leaves the procedure to a separate statute on interception [7]. The interception bill entered the 2026 national legislation programme [8], and commentators have set out the matters it should cover [9]. Until it passes, interception rests on scattered sectoral provisions.

Interception has always been among the most intrusive powers a state can hold. A single intercept captures the target and everyone the target speaks to. The claim that individuals deserve protection from such intrusion is older than digital networks [10], and modern privacy theory treats surveillance as a harm of information collection in its own right, separate from later disclosure or misuse [11]. Königs adds that the main danger of government surveillance in democracies lies in access to collected data and its possible use for purposes that lack legitimacy, a risk that grows if institutions decay over time [12]. A regime that leaves collection, access and use unregulated exposes citizens to all three harms at once.

The Constitutional Court recognized this two decades ago. In Decision No. 006/PUU-I/2003, and again in Decision No. 5/PUU-VIII/2010, it held that interception restricts a constitutional right and must be governed by a dedicated statute [13], [14]. Indonesian scholarship published in Scopus-indexed journals has documented the consequences of that statute's absence: approval kept inside the investigating institution [15], procedures that differ across sectoral laws [16], and oversight that lacks accountability and transparency [17]. These studies come mainly from criminal procedure and constitutional law. Three questions receive much less attention. The first is technical: what an interception system must do in software and network design for legal limits to be enforceable at all. The second belongs to private law: what a person whose communications were intercepted unlawfully can claim, from whom, and with what evidence. The third concerns the interaction between interception and the Personal Data Protection Law (PDP Law), which since 2022 has given data subjects a statutory right to sue and receive compensation [18].

This article addresses those gaps through three research questions. (RQ1) How does Indonesian law currently allocate the authority to intercept, and which safeguards are missing when the instruments are compared against recognized standards? (RQ2) Which IT governance controls are required to make lawful interception auditable and secure? (RQ3) How can civil liability under the Civil Code, the PDP Law and the Telecommunications Law serve as a remedy for unlawful interception? The contribution is twofold. First, the article codes nine safeguards across five Indonesian statutes and shows where the gaps lie (Fig-3). Second, it proposes a Regulatory Governance Model for Lawful Digital Interception (RG-LDI) that ties each legal requirement to a technical control and to a civil remedy, linked by a single warrant identifier (Fig-5). To the author's knowledge, no earlier study has connected the technical design of interception systems with the civil liability regime under Indonesian law in this way.

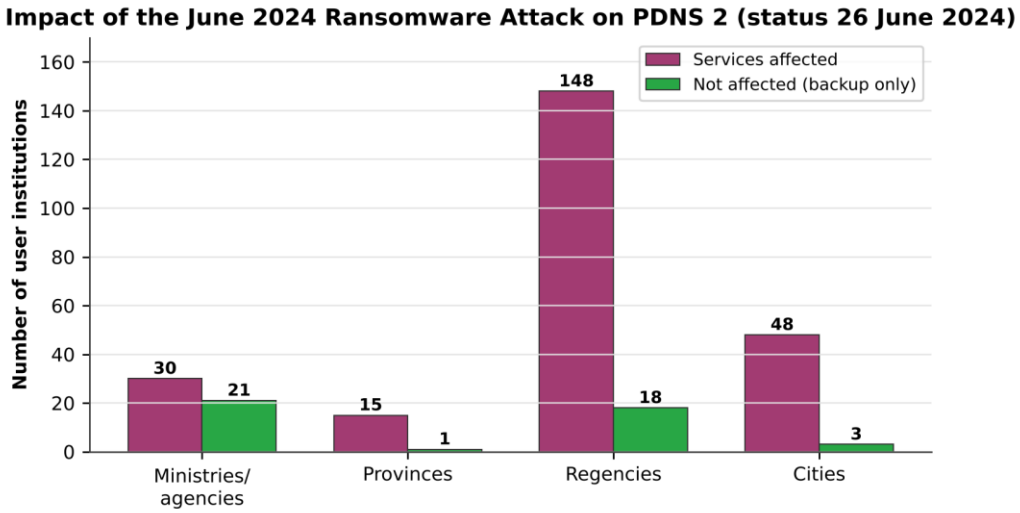


Fig-1: Impact of the June 2024 PDNS 2 ransomware attack by type of user institution, as reported by the Ministry of Communication and Informatics. The ministry gave 239 affected users in total; the category figures as reported sum to 241.

II. LITERATURE REVIEW

a) Interception and Due Process in Indonesian Scholarship

Christianto compared three procedural regimes in corruption cases and found that interception by the Corruption Eradication Commission (KPK) followed a crime control model more closely than a due process model. Approval passed through internal channels, and the 2019 amendment to the KPK Law turned interception into a procedural tool meant to strengthen coordination among agencies rather than to protect privacy [15]. Fadhil inventoried the sectoral rules and showed that different institutions exercising the same kind of authority follow different mechanisms. He argued that interception, as a coercive measure that limits privacy, must specify the permit request, the authorized subjects, court supervision and cooperation with telecommunications operators, and he noted that an interception bill had entered the 2019 legislation programme [16]. Mahdy, Hartiwiningsih and Isharyanto compared Indonesian law with other jurisdictions and found legal ambiguity, inconsistent enforcement and oversight that lacks accountability and

transparency. They recommended strict judicial oversight, open reporting and clearly defined limits [17]. The Constitutional Court's Decision No. 70/PUU-XVII/2019, which removed the requirement that the KPK obtain permission from its supervisory board, shows how unsettled the approval question remains [19].

These studies agree on the diagnosis: fragmented rules, internal approval and weak oversight. They seldom examine the systems through which interception is carried out, and they rarely discuss civil remedies. Table-1 summarizes the state of the art and the gap this article addresses.

Table-1: State of the art and research gap

Study	Main focus and finding	What remains open
Christianto (2020) [15]	KPK interception follows a crime control model; approval is internal	Technical enforcement of limits; civil remedies
Fadhil (2020) [16]	Disparity among sectoral interception rules; need for one harmonized bill	System-level controls; position of the PDP Law
Mahdy et al. (2025) [17]	Ambiguity, inconsistent enforcement, weak oversight; call for judicial control and reporting	How oversight can verify what systems actually did
Bates et al. (2015); Panwar et al. (2019) [20], [21]	Audit layers and ledgers can verify wiretap activity against court orders	Translation into statutory duties in a civil law system
Knetsch (2022); Li (2023) [22], [23]	Compensation for non-material loss after data protection violations in the EU	Application to interception under Indonesian law
This article	Codes nine safeguards across five statutes; links IT controls with civil liability in the RG-LDI model	Empirical testing of the model (future work)

b) Comparative accountability and oversight

Comparative research shows that the gap between interception powers and privacy protection is not unique to Indonesia. Koops traced Dutch interception law from 1838 to 2002 and concluded that privacy had become a secondary factor in legislative practice, raised after the need for new powers had already been accepted [24]. Gill argues that oversight must cover authorization, control and review, and that the growing reliance on private infrastructure calls for regulation that reaches corporate as well as state actors [25]. Molnar and Warren show how statutory reporting on the use of surveillance powers works as a primary accountability mechanism, while also noting its limits [26]. Scott, studying IMSI catchers in the United Kingdom, finds that even where the law is published, secrecy about the facts of deployment can make accountability close to impossible [27].

European human rights law offers the most developed set of standards. In *Big Brother Watch and Others v. United Kingdom*, the lack of oversight over the selection of intercepted material and weak safeguards for related communications data were found to violate Article 8 of the Convention [28]. The Grand Chamber in 2021 confirmed that bulk interception is not unlawful as such but requires safeguards at every stage, from authorization through examination to deletion [29]. Malgieri and De Hert describe the emphasis both European courts place on independent control before and after the measure, and argue that the controlling body need not be a judge as long as it is independent and effective [30]. Eijkman examines Dutch reforms that introduced prior judicial consent and a binding complaint procedure, and shows that access to justice for people affected by interception is still contested [31]. Dimitrova and De Hert add that when individuals cannot access their own data directly, the supervisory authority acting on their behalf must have real powers to check the legality of processing [32].

c) Accountable interception in computer security research

Computer security research approaches the same problem from the system side. Bates et al. observed that CALEA wiretap implementations in the United States were built on the assumption that operators can be trusted, and proposed a lightweight audit layer that lets independent parties verify wiretap activity at modest overhead [20]. Panwar et al. designed SAMPL, which uses public ledgers to audit surveillance involving courts, agencies and companies and can identify any party that goes beyond the scope of a court order [21]. Goldwasser and Park proposed record keeping with publicly verifiable audits that preserve the privacy of the records themselves [33]. Buccafurri et al. identified a missing standard for the interaction between law enforcement agencies and the monitoring facility that stores intercepted content, and built a proof of concept using self-sovereign identity to make authorizations machine-readable [34]. Green, Kaptchuk and Van Laer formalized abuse-resistant law enforcement access, addressing operator abuse and theft of key material [35]. At the network level, Gogoulos et al. enforced privacy-aware access control on monitoring data before it reaches an analyst [36], and Haryadi and Malik, writing for countries without interception retention rules, recommended separate administrative, collection and management functions, each with its own log [37].

On the risk side, Abelson et al. warned that mandated exceptional access adds complexity and new points of failure [6], and Li et al. reviewed government hacking practices across five countries and the challenges they pose to lawful interception rules [38]. For lawyers the lesson is direct. A legal limit on duration, scope or target only works if the system enforces it and records what it did.

d) Civil liability for privacy harms

Indonesian civil law has long recognized tort liability under Article 1365 of the Civil Code: a person whose unlawful act causes loss to another must compensate that loss [39]. The PDP Law added a specific statutory right in Article 12(1), under which a data subject may sue and receive compensation for violations in the processing of personal data about them [18]. Comparative work shows the questions such a right raises. Knetsch identified unresolved issues in compensating non-pecuniary loss under Article 82 of the GDPR [22]. Li reviewed Case C-300/21, in which the Court of Justice held that infringement alone does not give rise to compensation, that there is no threshold of seriousness for non-material damage, and that Member States must set the criteria for assessment [23]. Empirical work from the United States found that firms were 3.5 times more likely to be sued when individuals suffered financial harm, and that cases settled more often when plaintiffs alleged financial loss [40]. Proof of loss, in other words, drives private enforcement. Interception adds a further obstacle, because the person affected usually does not know it happened.

III. METHODOLOGY

This study uses normative (doctrinal) legal research, combined with a design-oriented step that constructs a governance model. Three approaches were applied. The statutory approach examined the main instruments on interception and personal data: Law No. 36 of 1999 on Telecommunications, Law No. 11 of 2008 on Electronic Information and Transactions as last amended by Law No. 1 of 2024, Law No. 27 of 2022 on Personal Data Protection, Law No. 1 of 2023 on the Criminal Code, Law No. 20 of 2025 on the Code of Criminal Procedure, and the Civil Code [7], [18], [39], [41], [42], [43]. Constitutional Court decisions were treated as authoritative interpretations [13], [14], [19], [44]. The conceptual approach drew on privacy theory [10], [11], [12] and on accountable surveillance research [20], [21], [33], [34]. The comparative approach used European human rights standards [28], [29], [30] and comparative studies of oversight [24], [25], [31].

Secondary literature was located through the Consensus and SciSpace scholarly databases. Priority went to sources in journals indexed in Scopus; each journal's indexation and quartile were checked against SCImago Journal Rank (SJR 2025), and bibliographic metadata were checked against Crossref. Primary legal texts were read from official repositories where available. News and NGO reports were used only to document recent events, not as authority for legal claims.

The analysis ran in three steps. First, nine safeguards were derived from the comparative standards and the literature: an explicit interception power, named authorized bodies, prior independent approval, a maximum duration, security and logging duties, deletion of irrelevant product, notice to the subject, a sanction for unlawful interception, and a civil compensation route. Second, each of the five statutes was coded against each safeguard as full, partial, absent, deferred to a special law, or not applicable, based on the text of the instrument (Fig-3). Third, every gap was assigned to a legal or technical control, and the controls were grouped into the layers of the RG-LDI model (Table-3, Fig-5). The coding reflects the author's reading of statutory text, not observed practice, and the model has not been tested on an operating platform. Both limitations are discussed in Section V.

IV. RESULTS AND DISCUSSION

a) A Fragmented Authorization Regime

Fig-2 traces the development of the relevant law, and Table-2 summarizes what each instrument says about interception and remedies.

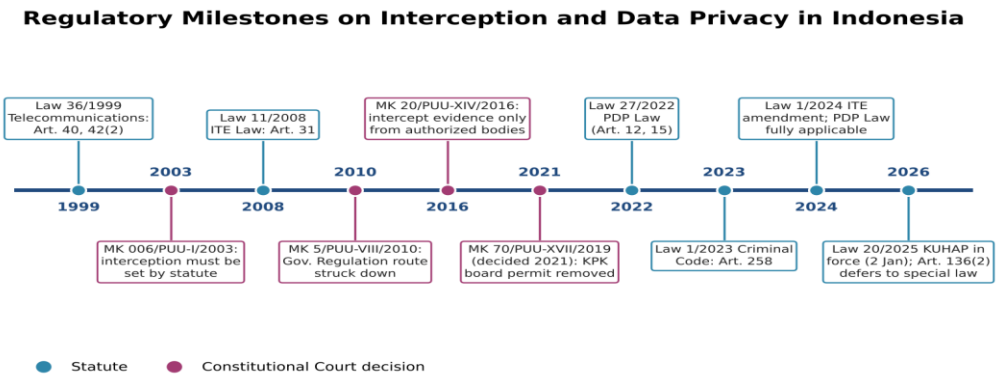


Fig-2: Regulatory milestones on interception and data privacy in Indonesia, 1999-2026

Table-2: Main Indonesian instruments relevant to interception, privacy and civil liability

Instrument	Relevance to interception
Law No. 36/1999 (Telecommunications)	Art. 40 prohibits interception of information sent through telecommunications networks, with a criminal sanction in Art. 56. Art. 42(2) allows operators to record information for criminal proceedings at the written request of the Attorney General or the National Police Chief, or of investigators for certain offences. Art. 15 obliges operators to compensate loss caused by their fault or negligence unless they prove otherwise [41].
Law No. 11/2008 as amended by Law No. 1/2024 (ITE Law)	Art. 31 prohibits unlawful interception and exempts interception for law enforcement requested by authorized institutions. Art. 26(2) lets a person whose rights are violated sue for the resulting loss. Under Art. 5 and Decision No. 20/PUU-XIV/2016, intercept product is admissible only when obtained for law enforcement by an institution authorized by statute [42], [44].
Law No. 27/2022 (PDP Law)	Art. 12 gives data subjects a right to sue and receive compensation. Art. 15(1) allows the rights in Arts. 8, 9, 10(1), 11 and 13(1)-(2) to be set aside for law enforcement and other listed interests; Art. 15(2) limits the exemption to the implementation of a statute [18].
Law No. 1/2023 (Criminal Code)	Art. 258 criminalizes unlawful interception [43], [45].
Law No. 20/2025 (KUHAP)	Art. 89 lists interception among coercive measures. Art. 136(1) lets investigators intercept for the purpose of investigation; Art. 136(2) leaves the details to a separate law on interception [7].
Civil Code	Art. 1365: liability to compensate loss caused by an unlawful act [39].

The pattern is consistent. Interception is recognized in many places and regulated in detail in none. Sectoral laws give interception powers to different agencies, with approval routes that vary from internal sign-off to permission from a district court chair, and some laws say nothing at all on the point [15], [16]. The 2025 KUHAP was the obvious place to set one baseline for every agency, but Article 136(2) defers that task. Until the interception law passes, investigators work under sectoral rules that the Constitutional Court has twice found insufficient [13], [14].

Fig-3 shows the result of coding the five statutes against the nine safeguards. Three findings stand out. First, no instrument provides prior independent approval, a maximum duration, or notice to the subject for interception in general. Second, security and logging duties and the deletion of irrelevant product appear only indirectly, through the general obligations of the PDP Law, and the deletion right is among those that may be set aside for law enforcement. Third, the KUHAP column is dominated by deferral: the code that should anchor the regime leaves five of the nine safeguards to a statute that does not yet exist. Sanctions for unlawful interception, by contrast, are well covered. Indonesian law is better at punishing unlawful interception after the fact than at preventing or detecting it.

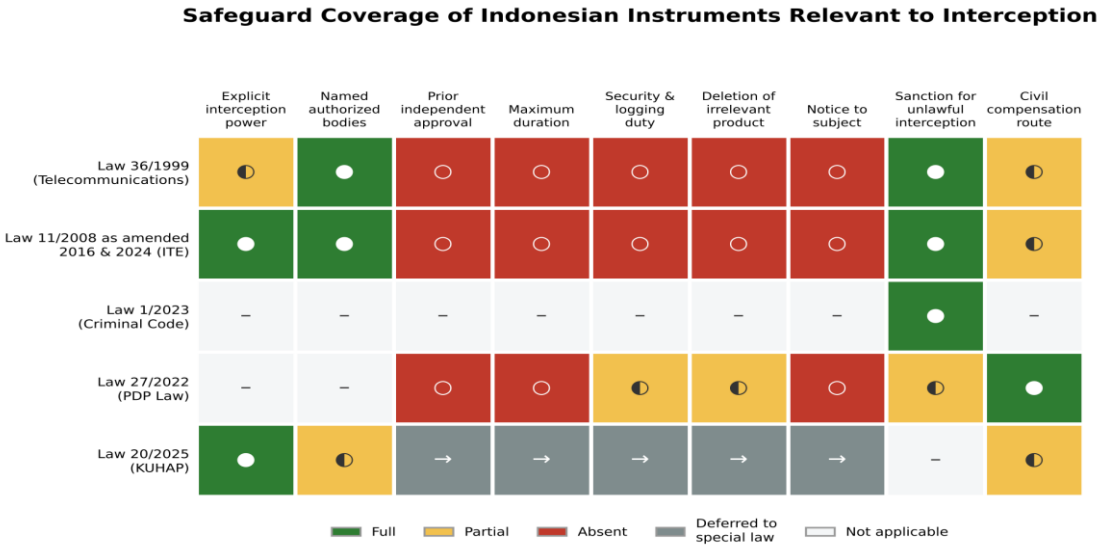


Fig-3: Safeguard coverage of five Indonesian statutes relevant to interception (author's coding of statutory text)

From a rule of law standpoint, the central problem is foreseeability. A person cannot know in advance on what grounds, for how long and under what checks their communications may be intercepted. The European courts treat this

kind of foreseeability as part of the "quality of law" requirement [29], [30]. Indonesian scholars reach the same conclusion through the due process model [15], [17]. Koops's observation that privacy tends to enter the legislative process only after new powers have been accepted [24] describes the Indonesian sequence closely: the power was confirmed in the KUHAP first, and the safeguards were postponed.

b) Missing technical governance

None of the instruments in Table-2 imposes technical duties on interception systems. They do not say who may operate the interception management system, how a warrant is entered into it, how the system enforces the warrant's scope and expiry, what must be logged, who may read the logs, or when intercepted content must be destroyed. Haryadi and Malik made a similar observation about interception data retention more than a decade ago and proposed function-level logging as a minimum [37]. Buccafurri et al. point to a related gap at the international level: there is still no standard for how law enforcement agencies access content stored by the monitoring facility [34].

The gap matters because many legal safeguards depend on the system. A duration limit holds only if the system stops provisioning when the warrant expires. A target limit holds only if provisioning is tied to a validated warrant identifier. A duty to delete holds only if the system records and proves the deletion. The CALEA experience shows that systems built on trust in operators are hard to audit after the event [20]. Designs such as SAMPL show that courts and independent auditors can receive cryptographic evidence of what was collected without seeing the content [21], and privacy-aware access control can keep analysts away from data outside their authorization [36]. These are not exotic proposals; they apply ordinary security engineering to a sensitive function.

Security is the second concern. Abelson et al. argued that mandated access raises the risk that third parties will exploit it [6], and the Salt Typhoon intrusion showed exactly that [4]. The PDNS 2 incident suggests that Indonesian public infrastructure is not immune to such failures [2]. The Amnesty findings add a third problem: tools procured through opaque channels may never pass through any official system at all [1], and interception that leaves no record cannot be audited. Scott's warning about secrecy of fact [27] applies here with particular force. A statute that regulates interception only on paper, without technical duties, leaves precisely this kind of activity outside its reach.

c) Interception and the PDP Law

Intercepted communications contain personal data, often of the specific categories that the PDP Law protects more strictly, such as health or financial information. The PDP Law therefore applies to the processing of intercept product, subject to its exemptions. Article 15(1) allows certain data subject rights to be set aside for law enforcement, national defence and security, and a few other listed interests [18]. The rights that can be set aside are those in Articles 8, 9, 10(1), 11 and 13(1)-(2), covering the ending of processing and erasure, withdrawal of consent, objection to automated decisions, restriction of processing, and data portability. Article 15(2) adds that the exemption applies only in the implementation of a statute.

Two consequences follow. First, the exemption is conditional. Processing that has no statutory basis, such as interception outside any authorized procedure or by tools acquired outside the formal framework, cannot rely on Article 15. Second, the right to sue and receive compensation in Article 12 is not on the list of rights that may be set aside. On a plain reading of the text, a person whose data was processed in breach of the law keeps that right even when the processing was carried out in the name of law enforcement. The author found no Indonesian court decision that has tested this reading, and the implementing regulations and the data protection agency will shape how it is applied in practice. Dimitrova and De Hert's analysis of indirect access [32] suggests one further requirement: if individuals cannot see their own intercept data, the supervisory body that acts for them must have real powers to check the legality of processing.

d) Civil liability for unlawful interception

Fig-4 maps the three settings in which a civil claim can arise, the legal basis available in each, and what the claimant must prove.

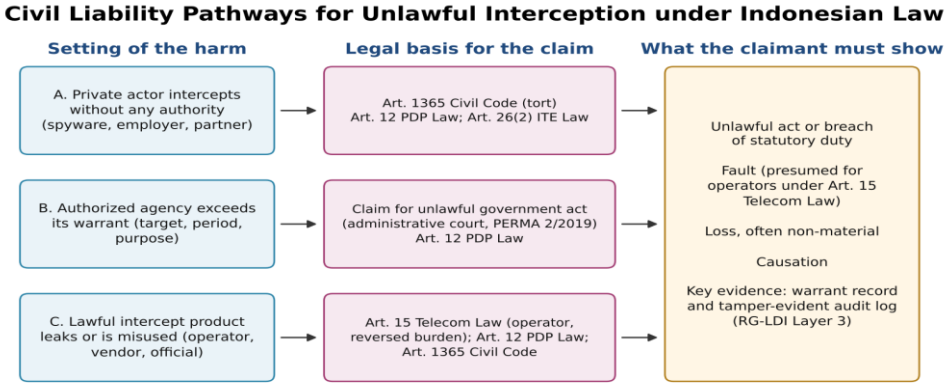


Fig-4: Civil liability pathways for unlawful interception under Indonesian law

The first setting is interception by a private person or company without any legal authority, for example spyware installed on a partner's phone or an employer reading private messages without a lawful basis. The second is interception by an authorized agency that goes beyond its authorization: the wrong target, a longer period than permitted, or use of the product for an unrelated purpose. The third is leakage or misuse of lawfully obtained intercept product by a network operator, a vendor or an official.

Under Article 1365 of the Civil Code the claimant must prove an unlawful act, fault, loss and a causal link [39]. Indonesian doctrine reads "unlawful" broadly, covering breach of a statutory duty, infringement of another person's subjective right, and conduct contrary to propriety. Interception without authority breaches Article 31 of the ITE Law, Article 40 of the Telecommunications Law and Article 258 of the 2023 Criminal Code [41], [42], [43], and it infringes the right to privacy protected by Article 28G(1) of the 1945 Constitution. In the first setting, then, the unlawful act is usually easy to establish. Article 12 of the PDP Law and Article 26(2) of the ITE Law supply more specific bases [18], [42].

The third setting has a feature that is easy to overlook. Article 15 of the Telecommunications Law requires an operator to compensate loss caused by its fault or negligence, unless it proves that the loss was not caused by its fault [41]. The burden of proof is reversed. Where intercept product held by an operator leaks, or where an operator's interception interface is compromised in the way Salt Typhoon compromised American carriers, the affected subscriber does not have to prove the operator's fault. This provision gives operators a strong private-law incentive to secure their interception systems, independent of any criminal or administrative sanction.

The second setting is the hardest. When the defendant is a state agency, claims for unlawful government acts now fall within the jurisdiction of the administrative courts under Supreme Court Regulation No. 2 of 2019 [46], and the interception law should confirm that route. Two further obstacles remain. Interception is secret by design, so the person affected often never learns of it. Notifying the subject after the measure ends is a safeguard the European courts examine [29], [30], but Indonesian law does not require it. In addition, the evidence about the scope of the interception is held by the defendant. This is where the technical controls discussed above matter for private law. A tamper-evident log that a court can inspect turns a suspicion that cannot be proved into a claim that can be decided.

Loss in privacy cases is often non-material: distress, damage to reputation, and loss of trust in private communication. Indonesian courts can award immaterial damages, but the amounts are hard to predict. The European experience shows the difficulty. After Case C-300/21, a claimant must show actual damage, but no seriousness threshold applies, and assessment is left to national law [22], [23]. The United States data suggest that without provable financial harm, few claims are brought [40]. An interception statute could address both problems by setting a minimum statutory sum per violation, so that a claimant need not prove monetary loss before receiving any compensation.

e) Intercept product as electronic evidence

Under Article 5 of the ITE Law, read with Constitutional Court Decision No. 20/PUU-XIV/2016 and the 2024 amendment, intercept product is valid evidence only if it was obtained for law enforcement at the request of an institution authorized by statute [42], [44]. This exclusionary rule protects the accused in criminal proceedings. It does nothing for third parties caught in the intercept, and it does not deal with integrity. A recording that cannot be traced to a valid warrant and an unbroken chain of custody should not be admitted. The same audit trail that supports civil claims would help a criminal court assess authenticity, so one technical investment serves both the defence and the victim.

f) The RG-LDI model

Building on the gaps identified above, this article proposes the Regulatory Governance Model for Lawful Digital Interception (RG-LDI), shown in Fig-5 and set out in Table-3. Its five layers apply in sequence to every interception and are linked by a single warrant identifier, so that each legal limit has a matching technical control and a record that an oversight body can check.

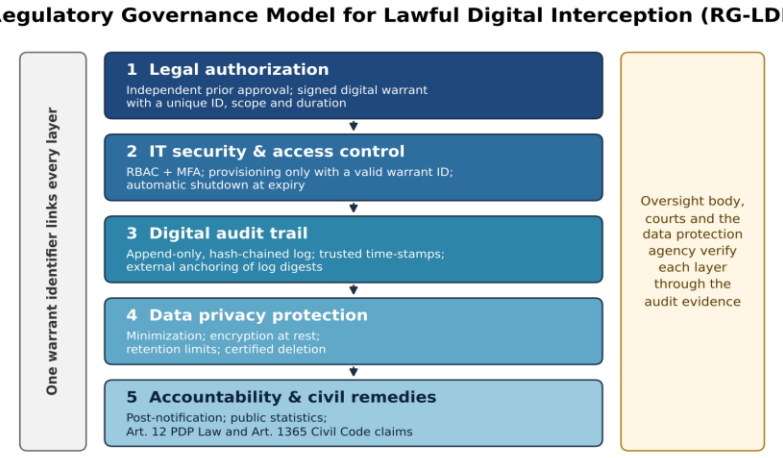


Fig-5: Regulatory Governance Model for Lawful Digital Interception (RG-LDI)

Table-3: Legal requirements, technical controls and oversight evidence in the RG-LDI model

Layer	Legal requirement	Technical control	Evidence for oversight
1. Legal authorization	Prior written approval by an independent authority; statutory list of offences; necessity and proportionality statement; maximum duration with reasoned renewal	Digital warrant with a unique ID and digital signature; machine-readable scope covering targets, period and data types [34]	Signed warrant record; register of applications, approvals and refusals
2. IT security and access control	Only designated officers operate the system; separation of duties between requesting agency, operator and approving authority	Role-based access control with multi-factor authentication; no provisioning without a valid warrant ID; automatic shutdown at expiry [35], [36]	Access control policy; list of authorized users and roles
3. Digital audit trail	Every action on target data is recorded and available to the oversight body and to courts	Append-only, hash-chained log; trusted time-stamps; periodic anchoring of log digests to an external ledger [20], [21], [33]	Log extracts; integrity proofs; periodic audit reports
4. Data privacy protection	Minimization; separate handling of irrelevant and privileged communications; retention limits; deletion	Filtering of out-of-scope content; encryption at rest; automated deletion with a deletion certificate [37]	Retention schedule; deletion certificates
5. Accountability and civil remedies	Notice to the subject once it no longer endangers the investigation; annual public statistics; compensation under Art. 12 PDP Law, Art. 15 Telecom Law and Art. 1365 Civil Code	Notification workflow; statistical reporting module; secure release of log records to a court in civil proceedings [26]	Statistical reports; notification records; court access to logs

Layer 1 answers the due process critique in the Indonesian literature [15], [17]: authorization comes from outside the requesting agency, is documented, and is specific. Layer 2 turns the warrant into system behaviour, so that the platform enforces the limits in the warrant instead of leaving them to the operator's discretion. Layer 3 is the link between law and technology. It produces evidence that a court, the data protection agency or an independent oversight body can verify, which responds to Gill's call for oversight that reaches the infrastructure as well as the agency [25]. Layer 4 applies the data protection principles of the PDP Law to intercept product. Layer 5 closes the loop by giving the person affected a way to learn of the interception and to claim compensation when an earlier layer has been breached, and by giving the public the kind of statistical reporting that Molnar and Warren identify as a core accountability tool [26].

The model leads to three recommendations for the interception bill. First, the statute should require every interception platform used by any authorized agency to implement Layers 2 to 4 and to pass a periodic independent audit, and it should prohibit the use of interception tools that are not registered in that platform. This would bring tools procured outside the telecommunications operators, of the kind documented by Amnesty International [1], into the framework. Second, the statute should state expressly that Article 12 of the PDP Law, Article 15 of the Telecommunications Law and Article 1365 of the Civil Code apply to unlawful interception, set a minimum statutory compensation, and give courts the power to order disclosure of audit logs. Third, it should require notification of the subject after the measure ends, with any deferral controlled by the approving authority.

Some trade-offs remain. Poorly handled notification and public reporting could alert organized crime groups, so the deferral mechanism must work in practice. Technical controls cost money and require operators to upgrade their systems. An independent audit body needs staff who understand both law and technology. Hash-chained logging and external anchoring add some processing overhead, although the results reported by Bates et al. suggest it is modest [20]. These are reasons to phase the model in gradually, starting with the largest operators and the agencies that intercept most often, not reasons to abandon it.

V. CONCLUSIONS

Indonesian law accepts interception as a legitimate investigative tool, but it still lacks the statute the Constitutional Court called for more than twenty years ago. Law No. 20 of 2025 recognizes interception and then defers its procedure. Coding five statutes against nine safeguards shows the consequence: prior independent approval, maximum duration, security and logging duties, deletion and notice are absent or only indirectly addressed, while criminal sanctions are well covered. The law is built to punish unlawful interception after the fact, not to prevent or detect it. Recent events, from documented spyware imports to the PDNS 2 ransomware attack and the Salt Typhoon intrusion into lawful interception systems abroad, show why that imbalance is risky.

The article also shows that the civil route deserves more attention. Article 12 of the PDP Law gives data subjects a right to compensation that is not among the rights Article 15 allows to be set aside for law enforcement. Article 15 of the Telecommunications Law presumes operator fault when a subscriber suffers loss, and Article 1365 of the Civil Code provides a general tort basis. These remedies only work if the interception process leaves evidence. The proposed RG-LDI model links legal authorization, access control, a tamper-evident audit trail, data privacy protection and civil

accountability through a single warrant identifier, so that every legal limit has a matching technical control and a record that can be checked.

The study is doctrinal. The safeguard coding reflects statutory text, not observed practice, and the model has not been tested on an operating platform. Further research could measure the overhead of hash-chained logging on a lawful interception gateway, survey judges and investigators on the use of audit logs as evidence, and follow how courts handle the first civil claims brought under Article 12 of the PDP Law and Article 15 of the Telecommunications Law.

VI. REFERENCES

[1] Amnesty International Security Lab, "A web of surveillance: Unravelling a murky network of spyware exports to Indonesia," Amnesty International, Index ASA 21/7974/2024, May 2024. [Online]. Available: https://www.amnesty.org/en/documents/asa21/7974/2024/en/

[2] Bisnis.com, "Kemenkominfo sebut 239 instansi terdampak PDNS 2 down, hanya 43 yang selamat," 27 Jun. 2024. [Online]. Available: https://teknologi.bisnis.com/read/20240627/101/1777626/kemenkominfo-sebut-239-instansi-terdampak-pdns-2-down-hanya-43-yang-selamat

[3] detikInet, "Hacker serang Pusat Data Nasional, 210 instansi pemerintah terdampak," Jun. 2024. [Online]. Available: https://inet.detik.com/security/d-7406310/hacker-serang-pusat-data-nasional-210-instansi-pemerintah-terdampak

[4] TechCrunch, "FBI confirms China-backed hackers breached US telecom giants to steal wiretap data," 14 Nov. 2024. [Online]. Available: https://techcrunch.com/2024/11/14/us-confirms-china-backed-hackers-breached-telecom-providers-to-steal-wiretap-data/

[5] Axios, "What you need to know about the Salt Typhoon hack," 15 Oct. 2024. [Online]. Available: https://www.axios.com/2024/10/15/salt-typhoon-hack-china-verizon-att

[6] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. A. Specter, and D. J. Weitzner, "Keys under doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, Art. no. tyv009, 2015. doi: 10.1093/cybsec/tyv009

[7] Republic of Indonesia, Law No. 20 of 2025 on the Code of Criminal Procedure (Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana), promulgated 17 Dec. 2025, in force 2 Jan. 2026.

[8] Tirto.id, "RUU Penyadapan masuk Prolegnas 2026, KPK akan lakukan kajian," 2026. [Online]. Available: https://tirto.id/ruu-penyadapan-masuk-prolegnas-2026-kpk-akan-lakukan-kajian-hm1j

[9] Hukumonline, "Delapan substansi ini perlu diatur dalam RUU Penyadapan," 2026. [Online]. Available: https://www.hukumonline.com/berita/a/delapan-substansi-ini-perlu-diatur-dalam-ruu-penyadapan-lt69d31e382db24

[10] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193-220, 1890. doi: 10.2307/1321160

[11] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477-564, 2006. doi: 10.2307/40041279

[12] P. Königs, "Government surveillance, privacy, and legitimacy," *Philosophy & Technology*, vol. 35, no. 1, Art. no. 8, 2022. doi: 10.1007/s13347-022-00503-9

[13] Constitutional Court of the Republic of Indonesia, Decision No. 006/PUU-I/2003 on the review of Law No. 30 of 2002 on the Corruption Eradication Commission.

[14] Constitutional Court of the Republic of Indonesia, Decision No. 5/PUU-VIII/2010 on the review of Article 31(4) of Law No. 11 of 2008 on Electronic Information and Transactions.

[15] H. Christianto, "From crime control model to due process model: A critical study of wiretapping arrangement by the Corruption Eradication Commission of Indonesia," *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, vol. 7, no. 3, pp. 421-442, 2020. doi: 10.22304/pjih.v7n3.a7

[16] M. Fadhil, "The urgency of the harmonization of interception regulation in the context of law enforcement," *Substantive Justice International Journal of Law*, vol. 3, no. 2, p. 125, 2020. doi: 10.33096/substantivejustice.v3i2.75

[17] M. Mahdy, Hartiwiningsih, and Isharyanto, "Wiretapping law in Indonesia: Realising due process of law," *Asian Journal of Human Services*, vol. 28, pp. 242-272, 2025. doi: 10.14391/ajhs.28.242

[18] Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection (Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi), State Gazette 2022 No. 196.

[19] Constitutional Court of the Republic of Indonesia, Decision No. 70/PUU-XVII/2019 on the review of Law No. 19 of 2019 on the Second Amendment to the Law on the Corruption Eradication Commission, 2021.
[20] A. Bates, K. R. B. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach, "Accountable wiretapping - or - I know they can hear you now," *Journal of Computer Security*, vol. 23, no. 2, pp. 167-195, 2015. doi: 10.3233/JCS-140515
[21] G. Panwar, R. Vishwanathan, S. Misra, and A. Bos, "SAMPL: Scalable auditability of monitoring processes using public ledgers," in *Proc. 2019 ACM SIGSAC Conf. Computer and Communications Security (CCS)*, London, UK, 2019, pp. 2249-2266. doi: 10.1145/3319535.3354219
[22] J. Knetsch, "The compensation of non-pecuniary loss in GDPR infringement cases," *Journal of European Tort Law*, vol. 13, no. 2, pp. 132-153, 2022. doi: 10.1515/jetl-2022-0008
[23] S. Li, "Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21," *Maastricht Journal of European and Comparative Law*, vol. 30, no. 3, pp. 335-345, 2023. doi: 10.1177/1023263X231208835
[24] B.-J. Koops, "The shifting 'balance' between criminal investigation and privacy: A case study of communications interception law in the Netherlands," *Information, Communication & Society*, vol. 6, no. 3, pp. 380-403, 2003. doi: 10.1080/1369118032000155311
[25] P. Gill, "Of intelligence oversight and the challenge of surveillance corporatism," *Intelligence and National Security*, vol. 35, no. 7, pp. 970-989, 2020. doi: 10.1080/02684527.2020.1783875
[26] A. Molnar and I. Warren, "Governing liberty through accountability: Surveillance reporting as technologies of governmentality," *Critical Criminology*, vol. 28, no. 1, pp. 13-26, 2020. doi: 10.1007/s10612-020-09490-9
[27] P. F. Scott, "Secrecy and surveillance: Lessons from the law of IMSI catchers," *International Review of Law, Computers & Technology*, vol. 33, no. 3, pp. 349-371, 2019. doi: 10.1080/13600869.2019.1569872
[28] B. van der Sloot and E. Kosta, "Big Brother Watch and others v UK: Lessons from the latest Strasbourg ruling on bulk surveillance," *European Data Protection Law Review*, vol. 5, no. 2, pp. 252-261, 2019. doi: 10.21552/edpl/2019/2/16
[29] A. Lubin, "Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)," *International Legal Materials*, vol. 61, no. 4, pp. 605-653, 2022. doi: 10.1017/ilm.2022.2
[30] G. Malgieri and P. De Hert, "European human rights, criminal surveillance, and intelligence surveillance: Towards 'good enough' oversight, preferably but not necessarily by judges," in *The Cambridge Handbook of Surveillance Law*, D. Gray and S. E. Henderson, Eds. Cambridge, UK: Cambridge University Press, 2017, pp. 509-532. doi: 10.1017/9781316481127.023
[31] Q. A. M. Eijkman, "Access to justice for communications surveillance and interception: Scrutinising intelligence-gathering reform legislation," *Utrecht Law Review*, vol. 14, no. 1, p. 116, 2018. doi: 10.18352/ulr.419
[32] D. Dimitrova and P. De Hert, "Real transparency and real oversight of law enforcement data: The ECHR and the lack of accountability of indirect access procedures," *Utrecht Law Review*, vol. 21, no. 1, pp. 49-69, 2025. doi: 10.36633/ulr.905
[33] S. Goldwasser and S. Park, "Public accountability vs. secret laws: Can they coexist?," in *Proc. 2017 Workshop on Privacy in the Electronic Society (WPES)*, Dallas, TX, USA, 2017, pp. 99-110. doi: 10.1145/3139550.3139565
[34] F. Buccafurri, A. L. Canino, V. De Angelis, A. Laurenda, and G. Lax, "An SSI-based solution to support lawful interception," *Applied Sciences*, vol. 15, no. 4, Art. no. 2206, 2025. doi: 10.3390/app15042206
[35] M. Green, G. Kaptchuk, and G. Van Laer, "Abuse resistant law enforcement access systems," in *Advances in Cryptology - EUROCRYPT 2021*, Lecture Notes in Computer Science, Cham: Springer, 2021, pp. 553-583. doi: 10.1007/978-3-030-77883-5_19
[36] F. Gogoulos, A. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "Privacy-aware access control and authorization in passive network monitoring infrastructures," in *Proc. 10th IEEE Int. Conf. Computer and Information Technology (CIT)*, Bradford, UK, 2010, pp. 1114-1121. doi: 10.1109/CIT.2010.203
[37] S. Haryadi and I. Malik, "Lawful interception data retention regulation recommendation: Recommendations for countries that do not have relevant regulations of this field," in *Proc. 6th Int. Conf. Telecommunication Systems, Services, and Applications (TSSA)*, Bali, Indonesia, 2011, pp. 81-85. doi: 10.1109/TSSA.2011.6095411
[38] C.-Y. Li, C.-C. Huang, F. Lai, S.-L. Lee, and J. Wu, "A comprehensive overview of government hacking worldwide," *IEEE Access*, vol. 6, pp. 55053-55073, 2018. doi: 10.1109/ACCESS.2018.2871762

[39] Kitab Undang-Undang Hukum Perdata (Indonesian Civil Code, Burgerlijk Wetboek voor Indonesie, Staatsblad 1847 No. 23), Article 1365.
[40] S. Romanosky, D. Hoffman, and A. Acquisti, "Empirical analysis of data breach litigation," *Journal of Empirical Legal Studies*, vol. 11, no. 1, pp. 74-104, 2014. doi: 10.1111/jels.12035
[41] Republic of Indonesia, Law No. 36 of 1999 on Telecommunications (Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi), State Gazette 1999 No. 154.
[42] Republic of Indonesia, Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 and Law No. 1 of 2024, State Gazette 2024 No. 1.
[43] Republic of Indonesia, Law No. 1 of 2023 on the Criminal Code (Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana), State Gazette 2023 No. 1.
[44] Constitutional Court of the Republic of Indonesia, Decision No. 20/PUU-XIV/2016 on the review of Articles 5(1)-(2) and 44(b) of Law No. 11 of 2008.
[45] Hukumonline, "Urgensi RUU Penyadapan dan equality before the law," 2026. [Online]. Available: https://www.hukumonline.com/berita/a/urgensi-ruu-penyadapan-dan-equality-before-the-law-lt6afd1ce1f044c/
[46] Supreme Court of the Republic of Indonesia, Regulation No. 2 of 2019 on Guidelines for Settling Disputes over Government Acts and the Authority to Hear Unlawful Acts by Government Bodies and/or Officials (PERMA No. 2 Tahun 2019).