RECHTSVINDING
Vol. 4, 2 (July-December, 2026), pp. 35-44
EISSN: 2987-4424, DOI: https://doi.org/10.59525/rechtsvinding.1859

Legal Responsibility of Telecommunication Providers for Personal Data Protection in the Reuse of Phone Numbers

Nazzarina Saharani[1], Adfiyanti[1], Rahmia Rachman[1]

[1] Universitas Tadulako, Indonesia

ARTICLE INFO

Keywords:

Personal Data;
Phone Number;
Legal Responsibility

Article history:

Received 2025-05-02
Revised 2026-06-05
Accepted 2026-07-10

ABSTRACT

The practice of reusing (recycling) expired mobile phone numbers is an administrative necessity for the sake of limited numbering efficiency. However, in the digital ecosystem, this phenomenon poses a residual data risk that threatens constitutional privacy rights because new numbers are often still linked to the old owner's bank accounts and social media. This study aims to analyze the legal construction of phone number reuse from the perspective of personal data protection and to formulate the form of legal accountability of telecom providers for the damages caused. The research used a normative juridical method with a statute approach, a conceptual approach, and a comparative approach. The study found a conflict between Minister of Communication and Informatics Regulation No. 14 of 2018, which focuses on numbering efficiency, and Law No. 27 of 2022 on Personal Data Protection (PDP Law). Telecom operators, as Data Controllers, have a legal responsibility to apply the right to erasure before giving out phone numbers again. If they don't make sure a number is 'clean,' they can be sued in civil court for breach of contract (Article 1239 of the Civil Code) or for unlawful acts (Article 1365 Civil Code in conjunction with Article 12 of the PDP Law). This study recommends reconstructing sectoral regulations by adopting the Privacy by Design principle through providing interconnection clearing Application Programming Interface (API) infrastructure across platforms to ensure legal certainty and consumer protection.

Corresponding Author:
Nazzarina Saharani
Universitas Tadulako, Indonesia; saharanyyyy@gmail.com

1. INTRODUCTION

The most basic need in modern communication is a cell phone. Among the benefits you can feel are the ability to make long-distance communication easier and to increase knowledge related to technological advancements. Technology not only polishes our lifestyle but also shapes patterns of human interaction. Various activities and interactions that used to take place in real time and space are now done digitally. Real space and time are replaced by electronic places (phones) or virtual spaces (the internet).

Communicating between individuals through telecommunication tools like cell phones (handphones) (Arrasuli & Fahmi, 2023).

A cell phone is a telecommunications device that uses wireless radio wave technology and transmitter networks for voice and data communication. Cell phones can be used through a small electronic chip embedded in a SIM card (Subscriber Identity Module) that stores various important personal data such as National Identification Number (NIK), Family Card (KK), financial information, and other sensitive information related to an individual, and can connect to various strategic services like digital banking, social media, and e-commerce platforms. Personal data represents an individual's identity that is attached to every citizen. Personal data is not just an administrative record but has become a representation of an individual's existence in both public and private spaces. Therefore, the sentence 'personal data is directly related to the constitutional right to feel safe' is not just a normative statement, but rather a reflection of the real needs of society (Widianti, 2026).

In connection with this matter, Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia states that 'everyone has the right to personal, family, honor, dignity, and property protection under their control, as well as the right to feel safe and be protected from threats or fear in doing or not doing something that is a basic right.' The meaning of personal rights is not only limited to ownership rights but also includes the right to privacy and personal data protection.

Privacy rights are rights that every person has. By being protected in the constitution, these privacy rights become one of the fundamental rights that every individual has without exception (Greenleaf, 2014). The right to personal data protection is recognized as part of human rights in Article 3 of Law Number 27 of 2022 on Personal Data Protection. Personal data protection is all efforts to ensure the security, confidentiality, and control of personal data by the data subject. In this context, banks act as personal data controllers who have a legal obligation to ensure that any processing of personal data is carried out legally, transparently, limited to specific purposes, and equipped with adequate security systems. This obligation is also confirmed in Articles 16 and 47 of the Personal Data Protection Law.

The existence of privacy rights serves as a protective tool. But if not managed properly, it can become a loophole for neglecting someone's personal data protection, like the risk of personal data misuse when reusing phone numbers. In recent years, the practice of reusing phone numbers has become common, leading to serious legal implications (Setiawan, 2023)

Based on the 2024 National Socio-Economic Survey (SUSENAS), the Indonesian Central Statistics Agency (BPS Indonesia) found that 93.21% of households in Indonesia have more than one mobile phone number, which is an increase compared to 2023 when the figure was 89.02% (Sutarsih dkk., 2025). With the increasing demand for phone numbers, telecom service providers are expected to provide more phone numbers to meet users' needs.

The high number of mobile phone ownership is directly proportional to the turnover of phone numbers in the telecommunications market. Every month, millions of numbers are deactivated by users for various reasons, such as switching services or forgetting to top up credit, which causes telecom providers to face limitations in numbering resources. As a result, the practice of recycling numbers becomes an unavoidable economic and technical choice for spectrum allocation efficiency. However, this phenomenon creates a worrying legal paradox; on one hand, the government is pushing for the acceleration of the digital economy ecosystem that integrates phone numbers as a single identity for financial verification, but on the other hand, the technical regulations on managing the recycling of these numbers are still stuck in place and haven't adopted risk-based data protection principles.

Based on Appendix 1 Chapter 1 Number 5 of the Minister of Communication and Informatics Regulation Number 14 of 2018 on the National Telecommunications Fundamental Technical Plan regarding Number Allocation Rules (hereinafter referred to as Permenkominfo No. 14 of 2018), it states that "Customer numbers that for one reason or another are no longer used by their owners must be made available for other potential customers who need them". Even so, the waiting period between when a customer number is returned by the previous customer/owner and when that number is given to a new

customer is no less than 2 (two) months. A 2-month waiting period is technically enough to cut off communication lines, but it doesn't fully guarantee that the old owner's digital identity is erased.

Referring to customer data security as regulated in Article 13 Paragraph (2) of the Ministry of Communication and Digital Regulation of the Republic of Indonesia Number 7 of 2026 (hereinafter referred to as Permenkomdigi No. 7 of 2026) it states that "In the event that a Telecommunications Service customer is no longer active, the Telecommunications Service provider is required to keep the customer's data for at least 3 (three) months starting from the date the telecommunications service customer becomes inactive" (Hutama dkk., 2026). There is a 1 (one) month period where numbers can be given to new customers while the new customers still have the old customer data. Without a clear data cleaning (data scrubbing) mechanism, this grace period just becomes a 'pause' that doesn't really provide protection for personal data subjects.

The mismatch in regulations between the reuse of phone numbers and the obligation to store customer history data is made worse by the lack of a centralized data scrubbing requirement between mobile operators and third-party platforms. Data controllers in banking, social media, and e-commerce generally don't have automatic systems to know whether a phone number has changed owners or been recycled. As a result, when the number goes to a new user, the right to erasure and withdrawal of consent guaranteed by Law No. 27 of 2022 effectively becomes powerless in practice. Former data subjects often lose full control over their personal data without realizing it, creating multiple layers of vulnerability to individual privacy.

The Personal Data Protection Law Number 27 of 2022 (hereinafter referred to as PDP Law No. 27 of 2022) in Article 8 states that, 'Personal Data Subjects have the right to terminate the processing, delete, and/or destroy Personal Data about themselves in accordance with the provisions of the laws and regulations.' This is further reinforced in Article 9 which states, 'Personal Data Subjects have the right to withdraw their consent for the processing of Personal Data about themselves that has been given to the Personal Data Controller' (Setiawan, 2023). Furthermore, in Article 12 Paragraph (1), it states, 'Personal Data Subjects have the right to sue and receive compensation for violations of the processing of Personal Data about themselves in accordance with the provisions of the laws and regulations". Thus, the Personal Data Protection Law clearly places the Personal Data Subject as the party who has full control over their Personal Data. Personal Data Subjects are not only given the right to withdraw consent and stop the processing of their Personal Data, but they are also protected through the right to delete or destroy their Personal Data and can claim compensation if any violations occur.

For comparison, Personal Data Protection Regulations are comprehensively governed by the General Data Protection Regulation (hereinafter referred to as GDPR) in the member states of the European Union (Ziqra et al., 2021). According to Article 5, the principle of data minimization requires that personal data must be processed lawfully, fairly, and transparently, collected for specific and legitimate purposes and not used outside of those purposes, limited only to data that is relevant and necessary, kept confidential and updated when needed, stored no longer than required according to the processing purpose, and processed with adequate security measures to protect against unauthorized access, loss, or damage. Therefore, telecommunications providers must have already deleted old users' personal data after the number has been reassigned to new customers.

However, the existing regulations often don't align with social reality. The reuse of phone numbers doesn't always guarantee the protection of the owner's personal data. One real example experienced by Felicia Regina Tjhang started on March 15, 2024. Felicia was using a prepaid card that, even though it was rarely used for regular communication, was still recharged regularly because it was connected to various credit cards, financial apps, and businesses. However, due to negligence, the prepaid balance top-up accidentally stopped, causing the number to enter a grace period. The phone number was then assigned to a new user, who turned out to be a hacker. In their use, the hacker managed to withdraw $1,200 from PayPal, change the email and password, make shopping transactions worth IDR 500,000 through a Key Look account, and attempt breaches on other social media apps still linked to the phone number. As a

result, Felicia suffered financial losses and experienced a lack of legal protection for previous users whose numbers had been reassigned to new users.

The case that Felicia went through is a loud wake-up call proving that the losses caused by this systemic weakness are no longer just potential—they're a real threat that can be destructive both financially and psychologically. From a doctrinal perspective, the operator's failure to mitigate the risk of digital identity leaks when reselling used phone numbers can be seen as a form of neglecting the duty of care. When the existing positive legal instruments are not yet able to provide a solution for victims, then reconstructing the concept of legal responsibility, whether through the approach of breach of contract in subscription clauses or through Unlawful Acts (PMH), becomes very crucial to formulate in order to provide legal certainty and fair protection for telecommunications consumers in Indonesia.

Someone's personal data is becoming increasingly vulnerable to potential breaches amid the rapid growth of the digital world. As a developing country, Indonesia needs to uphold privacy rights by protecting personal data. Everyone has human rights, known as the right to privacy, to ensure the safety and confidentiality of their personal information. The country must have strong laws and regulations to safeguard citizens' privacy rights, especially considering the rising incidents of privacy data violations through the reuse of phone numbers.

Based on the description above, the author feels it is necessary to further research how far legal protection can guarantee privacy rights for each individual, leading to a study entitled: "Legal Accountability of Telecommunication Providers for the Protection of Personal Data in the Reuse of Phone Numbers".

2. METHODS

This research is a normative legal study that focuses on analyzing regulatory gaps, the synchronization of rules, and the doctrine of legal responsibility related to the practice of phone number recycling. The research approaches used include the statute approach to examine PDP Law No. 27/2022, Ministry of Communication and Information Regulation No. 14/2018, and Ministry of Digital Regulation No. 7/2026; the conceptual approach to explore the concepts of civil liability and the principle of privacy by design; as well as the comparative approach to compare regulations in Indonesia with the European Union's General Data Protection Regulation (GDPR). The subjects of this study are legal norms, principles, and doctrines regarding personal data protection and the responsibilities of telecommunications providers as data controllers. The materials used in this study rely on secondary data, which include primary legal materials such as relevant laws and regulations; secondary legal materials like law books, scientific journals, and case reports; as well as tertiary legal materials such as legal dictionaries. The main instrument used is the researcher themselves as a human instrument, supported by a digital-based legal document search system. The research procedure begins with identifying legal issues related to the risk of data misuse on redistributed numbers, which is then followed by data collection through library research using techniques like inventorying, classifying, and systematically recording documents. Finally, the data analysis is carried out qualitatively using deductive reasoning, where the collected legal materials are interpreted grammatically and systematically to produce precise legal interpretations and arguments regarding the forms of civil liability that can be imposed on telecommunications providers.

3. FINDINGS AND DISCUSSION

The purpose of forming the Unitary State of the Republic of Indonesia is to provide protection and ensure the welfare of all its people. Therefore, the state, especially the government, has the responsibility to guarantee that the constitutional rights of every citizen are fulfilled, including the right to protection and fair legal certainty as mandated in Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Legal protection is a tangible form of the rule of law concept embraced by Indonesia. Its development cannot be separated from the history of national law, which includes various important events and the dynamics of legal systems that have been in place in the past and

continue to influence the development of Indonesian law today. The history of Indonesian law actually goes way back even before the Proclamation of Independence. Every legal system has its own characteristics and unique features that set it apart from other legal systems. This diversity has a positive impact, offering various options that can be used to strengthen, develop, and improve the legal system applied in each country (Lasatu et al., 2023).

The right to privacy is a constitutional right guaranteed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which in the digital era has transformed into personal data protection, including mobile phone numbers that now serve as digital identities and access keys to various important accounts. On the other hand, the practice of reusing (recycling) phone numbers that have been administratively deactivated is a legal action for efficiency in managing limited numbering resources based on the Minister of Communication and Informatics Regulation Number 14 of 2018, with a minimum waiting period of 60 calendar days. However, these sectoral regulations are still purely focused on the technical aspects of the telecommunications business and haven't anticipated the shift in the function of phone numbers, which triggers residual data risks like data leaks, unauthorized access, or even the previous owner's financial account being compromised by a new user if the number is transferred without properly clearing the digital links.

Personal identity is data related to someone that can be used to identify their ownership. Privacy is a high-value human right because it involves the secrecy of ownership. For example, nowadays the phone number someone has on their mobile phone is considered personal identity. This is because activating a phone number requires using the National Identification Number (NIK). The right to personal identity protection has developed from the right to respect private life (Sari & S, 2022).

The main legal issue in this phenomenon isn't the legality of number recycling practices, but rather the vagueness of the norms (vage normen) and the lack of harmony in regulations in Indonesia. Even though there are legal instruments like Permenkominfo No. 14 of 2018, Permenkomdigi No. 7 of 2026, and Law No. 27 of 2022 on Personal Data Protection (PDP Law), there's still no regulation that explicitly requires operators to ensure the certainty of clean numbers. The absence of mandatory mechanisms like network integration cleansing, digital account termination verification, cross-platform coordination, or a system for notifying number ownership changes makes the 60-day quarantine period just a formal administrative step and fails to provide real protection for the data subject's rights.

Under the PDP Law regime, telecom operators legally qualify as Personal Data Controllers because they collect, store, and decide the purposes of processing customer data. This status means operators have to strictly follow data protection principles, especially granting the rights of old number owners to delete (right to erasure) or destroy inactive data so it's not processed beyond the original registration purpose. Therefore, the operator's legal responsibility shouldn't be reduced just for business efficiency; they must ensure that every number transfer doesn't create loopholes for misuse of the previous owner's data, and be prepared to face administrative sanctions or civil lawsuits for damages based on Unlawful Acts (PMH) if they fail to maintain cybersecurity during the recycling process.

Legally, the status of mobile phone numbers under Indonesia's telecommunications law is classified as part of telecommunication numbering, which is a limited resource owned by the state. According to Law Number 36 of 1999 on Telecommunications, the management of this limited resource is controlled by the state and allocated to telecom operators based on permits issued by the government (Suari & Sarjana, 2023). From the perspective of administrative law, consumers or end-users never actually own the phone number outright or permanently; they are only granted the right to use the telecom service as long as their subscription lasts or their prepaid card remains active. When the card expires because it isn't renewed, the consumer's legal right to use it ends, and the operator has an administrative duty to reclaim the number so it can be redistributed to maintain efficiency and optimize the allocation of frequency spectrum and national numbering ((Bukit & Ayunda, 2022). In fact, the consumer protection referred to here, according to Article 1 number 1 of Law Number 8 of 1999 on Consumer Protection (UU PK), is any effort that ensures legal certainty to provide protection to consumers (Rachman, 2022).

However, the dynamics of technology have created a blurring of norms (vage normen) due to the delay of positive law in anticipating the functional shift of phone numbers in society. Conventional telecommunications law doctrines outlined in the Telecommunications Law place phone numbers purely as technical transmission tools for conveying voice and text messages (SMS). In reality, our positive law struggles to deal with the cyber transformation where phone numbers have shifted functions to become a single digital identity and the main authentication key to access personal data on various electronic platforms, such as banking, digital wallets, and social media (Kusnadi & Putri, 2025). The misalignment between the technical-legal functions in old regulations and the cyber-sociological functions in the era of the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law) creates a vacuum (rechtsvacuum) regarding whether a phone number is considered just a communication tool or personal data itself.

This shift in function is what triggers the emergence of residual data risk when operators engage in the practice of withdrawing and reselling expired numbers on the market. In theory, when a number that is still linked to the old owner's digital accounts is allocated to a new user, the mechanism for sending One-Time Password (OTP) codes or SMS verification will automatically switch to the new number holder (Rullyandi & Fahmi Ginanjar, 2025). This technical loophole creates opportunities for illegal account breaches, receiving sensitive information by the wrong person, and even identity theft that can harm the previous owner both financially and morally. From the perspective of cyber law doctrine, residual data risk appears because the personal data of former owners still remains digitally on third-party servers (like banks or social media platforms) due to the lack of data cleaning interconnection between telecom operators and external digital platform providers (Wahyudin & Sumanto, 2024).

This phenomenon ultimately triggers a real conflict of norms within positive law in Indonesia, namely between the operator's duty to implement numbering efficiency and the duty to protect personal data confidentiality. On one hand, according to the Minister of Communication and Informatics Regulation No. 14 of 2018, operators are legally required to recycle inactive numbers after a minimum quarantine period of 60 days for operational efficiency. On the other hand, the PDP Law imperatively commands that every data controller must maintain security, accuracy, and destroy personal data once its purpose has ended (Pangestu et al., 2024). This clash of legal obligations puts operators in a legal dilemma: letting expired numbers go unused would violate the principle of telecom efficiency, but reselling them without a thorough data cleansing mechanism could potentially infringe on the constitutional right to privacy of data subjects protected by Article 28G paragraph (1) of the 1945 Indonesian Constitution.

In the landscape of personal data protection law in Indonesia, telecom providers legally qualify as Personal Data Controllers. This status is based on the fact that operators have full authority to determine the purposes, legal basis, and control over processing customer data from the stage of registering prepaid or postpaid cards. As a consequence of this legal position, operators have an imperative duty to comply with the principles of personal data protection mandated in Article 16 of Law Number 27 of 2022 on Personal Data Protection (PDP Law). Maintaining accuracy, limiting the purpose, and setting data retention periods become really important in this context. Once a phone number has expired and is no longer actively used, the original purpose of processing that customer's data is legally over. So, operators should actually have a normative duty to apply the right to erasure and completely destroy leftover data in their internal systems before the number is reassigned to a new user to prevent overlapping data ownership.

If data protection fails due to a messy recycling process, the legal liability doctrine can be applied by analyzing the limits of negligence between the operator and the previous user through a Liability Based on Fault approach (Fajar & Achmad, 2010). In practice, disputes often bring up the argument that losses happen because the previous user was careless and didn't unlink their personal digital accounts from the old number. However, from a legal standpoint, the user's negligence doesn't automatically absolve the operator of fault (Barkatulah, 2008). As a corporation operating in the field

of technology services with specialized expertise, operators have a higher legal duty of care to mitigate cyber risks arising from their business activities. Operators can't just pass the entire mitigation burden onto consumers, considering consumers' weak bargaining position and their limited technical ability to ensure that released numbers are truly clean from external interconnection networks.

The gap in the operator's negligence in performing leftover data (residual data) cleaning triggers the validity of filing a lawsuit for Unlawful Acts (PMH) in a normative way. The application of Article 1365 of the Civil Code (KUHPerdata) can be combined (juncto) with the provisions on the right to claim compensation specifically regulated in Article 12 of the PDP Law. To hold the operator accountable, the claimant must prove the fulfillment of four main elements of PMH, which are the existence of an unlawful act, the presence of fault or negligence, the occurrence of loss, and the existence of a causal relationship (causal verband) between the operator's negligence and the loss suffered by the previous number owner (Ramli & Prabandari, 2025). When an operator releases a number that's still linked to a bank account to the market, allowing it to be accessed by a new user illegally, it's considered a violation of the operator's civil legal duty to keep data secure. The previous data owner who suffers material losses like stolen funds, or immaterial losses like a breach of privacy, has the right to claim full compensation for the faulty telecom service (Hanim et al., 2019).

Besides civil liability, the PDP Law also provides doctrinal law enforcement tools that are coercive through administrative sanctions for data controllers who break the law. According to the normative provisions of the PDP Law, failing to keep users' personal data secure during the allocation and recycling of numbers can result in operators facing graduated penalties, ranging from written warnings, temporary suspension of data processing activities, deletion or destruction of personal data, to administrative fines that are very significant (Febiyani et al., 2025). A doctrinal review shows that these administrative sanctions serve as a guarantee function (ultimum remedium) of the state to enforce corporate compliance. Imposing these sanctions makes it clear that any technical failure in managing the phone number lifecycle that leads to personal data leaks is no longer just an internal administrative matter for the company, but a serious legal violation against public order in Indonesia's cyberspace.

Efforts to overcome legal disharmony between telecommunications regulations and privacy protection require a progressive regulation overhaul from the Ministry of Communication and Digital (Kemenkomdigi). The current sectoral numbering regulations, especially the Minister of Communication and Informatics Regulation Number 14 of 2018, urgently need to be revised to adopt the principles of Privacy by Design and Privacy by Default as mandated by modern cyber law doctrine. Through this reconstruction, phone number allocation governance should no longer be seen merely as a commercial technical management issue, but must be integrated from the start with a privacy-friendly cyber security architecture system (Indrayati, 2026). The integration of this principle requires regulators to set up standard operating procedures where every numbering comparison system managed by operators automatically has built-in data protection features, so that potential harm to data subjects can be mitigated systemically before the phone number is released back to the market.

The sectoral harmonization steps need to be followed by a normative rearrangement regarding the duration of the quarantine period and the institutionalization of the obligation to cleanse interconnection networks. The previous rule setting a minimum quarantine period of 60 calendar days has proven insufficient amid the massive use of phone numbers as the basis for digital account identities (Milianty & Sitabuana, 2025). Ideally, this quarantine period should be significantly extended, for example, to at least 180 days, to give systems and users enough time to cut off links to residual data. More than just extending wait times, the new regulations should require operators to actively clean up interconnections by providing a Number Clearing Application Programming Interface (API) infrastructure, which allows operators to coordinate directly with third parties like banks and digital platform providers to automatically remove data still linked to expired numbers.

Through this integrative regulatory reconstruction, the principles of legal certainty and consumer protection can be upheld in a balanced way without compromising the efficiency of telecommunications businesses. Legal certainty won't be achieved as long as operators hide behind the

excuse of numbering efficiency to avoid responsibility for systemic failures in personal data protection. By making the obligation to clean up leftover data part of the operational standards for telecommunications providers, the state steps in to provide substantive protection guarantees for citizens' constitutional rights to privacy. This normative solution will eventually create legal certainty that's fair, where the growth of the telecommunications industry goes hand in hand with cyber law compliance, and people's right to privacy as data subjects remains fully protected in the digital transformation era (Utomo, 2025).

Law enforcement regarding the fulfillment of data subject rights as regulated in Article 5 of Law Number 27 of 2022 on Personal Data Protection (PDP Law) is a key pillar in creating legal certainty for mobile phone users in Indonesia. From a consumer protection law perspective, telecom consumers are in an unequal bargaining position against operators who have full technical control over digital infrastructure. So far, the right to privacy, which is essentially a constitutional right guaranteed by the constitution, is often diminished and outweighed by business efficiency arguments and corporate revenue optimization under the pretext of recycling phone numbers. Without binding legal certainty, the rights of consumers with old numbers to receive substantive protection of their personal data will become an empty abstract norm. Therefore, re-evaluating the strict implementation of Article 5 of the PDP Law in telecommunications operational regulations is a normative necessity, so that data subjects' rights to refuse further processing, request deletion (the right to be forgotten), and claim compensation for leftover data leaks can be enforced fairly without giving operators any room to evade their legal responsibilities.

This legal certainty ultimately has to put consumer protection and privacy rights as absolute boundaries that shouldn't be bargained away just for economic gain. Re-commercializing phone numbers that have expired without any guarantee of clean data is a legal flaw in service provision that violates consumers' right to security and safety as outlined in the Consumer Protection Law. Indonesia's positive legal regime should firmly state that the efficiency of managing limited numbering resources must not come at the expense of citizens' cybersecurity. By coherently integrating the principles of legal certainty and consumer protection, the state provides assurance to the public that when they give up the right to use a phone number, their personal data will not be swept away and become a threat later on. This human-faced legal certainty will not only protect individual legal interests as consumers, but also build a national digital ecosystem that is trustworthy, healthy, and adheres to human rights protection standards in cyberspace.

Based on the provisions of Articles 42 and 43 of the PDP Law, telecom operators have normative obligations that go beyond just waiting for a phone number quarantine period to end. They also need to make sure to properly stop processing and delete the personal data of old customers. If an operator reallocates an expired phone number without properly unlinking the digital connections, this could be considered a failure to fulfill their data protection duties. From a civil law perspective, this negligence opens the door to breach of contract lawsuits since the operator hasn’t fulfilled its duty to safeguard data as part of telecom services, meaning they could be liable for both material and immaterial damages to the customer under Article 1239 of the Civil Code.

Besides fulfilling contract clauses (breach of contract), an operator's failure to mitigate residual data risks, which can lead to account takeover or privacy violations, can also be sued under Unlawful Acts (PMH) according to Article 1365 of the Civil Code. This PMH approach does not rely on whether there is a contractual relationship but rather focuses on proving that someone else's subjective rights were violated due to the operator's negligence in properly carrying out legal cyber obligations. Therefore, whether through breach of contract or PMH, telecom operators can absolutely be held fully legally responsible to pay compensation for any losses suffered by the previous number owner or the new user.

4. CONCLUSION

Based on the normative legal study that has been conducted, a clear norm antinomy was found, where sectoral regulations (Ministry of Communication and Information Regulation No. 14 of 2018) are still purely focused on the technical-efficiency aspect of number allocation, so they struggle to mitigate the risk of residual data that threatens the constitutional privacy rights of data subjects under the PDP Law. Doctrinally, the operator's failure to ensure a clean number status before releasing the number to the market constitutes an element of legal negligence. As a result, the operator as the Data Controller can be held fully civilly liable, either through a breach of contract lawsuit based on Article 1239 of the Civil Code for defective service, or through an Unlawful Act lawsuit under Article 1365 of the Civil Code in conjunction with Article 12 of the PDP Law for the material and immaterial losses suffered by the previous number owner.

This study emphasizes that quarantine periods should no longer be seen as passive administrative procedures, but rather should be realized as an active data clearing space. An urgent ius constituendum solution is the reconstruction of regulations by the Ministry of Communication and Digital to adopt the principle of Privacy by Design through the obligation to provide Application Programming Interface (API) architectures for cross-platform interconnection clearing. This agenda is currently being tested on a limited scale in the banking sector to automate account unlinking. However, the limitation of this research, which only focuses on the normative legal level, opens up a big opportunity for future studies to move towards a more juridical-empirical approach. Further research is suggested to analyze the effectiveness of enforcing administrative sanctions by the Personal Data Protection (PDP) Supervisory Agency, as well as to test the readiness of digital infrastructure and corporate compliance of telecom operators in the field in implementing a national leftover data cleanup system.

REFERENCES

Arrasuli, B. K., & Fahmi, K. (2023). PERLINDUNGAN HUKUM POSITIF INDONESIA TERHADAP KEJAHATAN PENYALAHGUNAAN DATA PRIBADI. *UNES Journal of Swara Justisia*, *7*(2), 369. https://doi.org/10.31933/ujsj.v7i2.351

Barkatulah, A. H. (2008). *Hukum perlindungan konsumen kajian teoretis dan perkembangan pemikiran* (1 ed.). FH Unlam Press.

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20. https://doi.org/10.46257/jrh.v26i1.376

Fajar, M., & Achmad, Y. (2010). *Dualisme Penelitian Hukum: Normatif & Empiris*. Pustaka Pelajar.

Febiyani, N. S., Risqi, D. S., Purwaningsih, T., Awana, D. J., & Rokhman, M. (2025). Analisis Perlindungan Hukum Terhadap Data Pribadi di Era Digital Ditinjau Dari Perspektif Hukum Telematika. *Suara Edukasi Hukum*, *1*(1). https://doi.org/10.67084/ca60ev53

Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade & Human Rights Perspectives*. Oxford University Press.

Hanim, N. F., Jafar, S., & Rahman, A. (2019). PERLINDUNGAN HUKUM TERHADAP PENCIPTA LAGU DALAM WEBSITE PENYEDIA JASA DOWNLOAD LAGU GRATIS BERDASARKAN UNDANG-UNDANG NOMOR 28 TAHUN 2014 TENTANG HAK CIPTA. *JURNAL ILMIAH MAHASISWA FAKULTAS HUKUM UNIVERSITAS MALIKUSSALEH*, *2*(3). https://doi.org/10.29103/jimfh.v2i3.4035

Hutama, S. T. A. P., Muslim, B., Perwitasari, E., Setyowati, Rr. N., & Habibah, S. M. (2026). PERAN PERATURAN MENTRI KOMUNIKASI DAN DIGITAL NOMOR 9 TAHUN 2026 DALAM MITIGASI ANCAMAN NIRMILITER DAN PENGUATAN KETAHANAN NASIONAL GENERASI MUDA. *SOCIAL : Jurnal Inovasi Pendidikan IPS*, *6*(2). https://doi.org/10.51878/social.v6i2.10167

Indrayati, R. (2026). QUO VADIS HAK ASASI MANUSIA DALAM KONSTITUSIONALISME DIGITAL: ANTARA PERLINDUNGAN DAN PENGAWASAN. *Konferensi Nasional Asosiasi Pengajar Hukum Tata Negara dan Hukum Administrasi Negara*, *3*(1), 327–346. https://doi.org/10.55292/1gmkmr94

Kusnadi, & Putri. (2025). Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi Deepfake di Indonesia. *urnal Rechtsvinding: Media Pembinaan Hukum Nasional*, *14*(2). https://doi.org/10.33331/rechtsvinding.v14i2.2135

Lasatu, A., Patila, M., & S, I. Friskanov. (2023). Penyuluhan Hukum tentang Urgensi Perlindungan Konsumen di Masa Covid-19 di SMAN 1 Palu. *BERNAS: Jurnal Pengabdian Kepada Masyarakat*, *4*(1). https://doi.org/10.31949/jb.v4i1.3554

Milianty, Y., & Sitabuana, T. H. (2025). The Urgency of Harmonizing the Regulation of the Minister of Communication and Informatics Regarding the Recycled Customer Number Policy: Urgensi Harmonisasi Peraturan Menteri Komunikasi dan Informatika Mengenai Kebijakan Nomor Pelanggan Daur Ulang. *Indonesian Journal of Law and Economics Review*, *20*(4). https://doi.org/10.21070/ijler.v20i4.1394

Pangestu, A. S., Budiarti, D., & Humiati, H. (2024). Perlindungan Hukum Data Pribadi Pemilik Nomor Telepon Yang Didaur Ulang Oleh Penyelenggara Jasa Telekomunikasi. *Yurijaya : Jurnal Ilmiah Hukum*, *6*(2), 197–212. https://doi.org/10.51213/yurijaya.v6i2.162

Rachman, R. (2022). PENINGKATAN KESADARAN HUKUM PERLINDUNGAN KONSUMEN DALAM TRANSAKSI E-COMMERCE BAGI SISWA DI SMA NEGERI 1 PALU. *KADARKUM: Jurnal Pengabdian Kepada Masyarakat*, *3*(1), 70. https://doi.org/10.26623/kdrkm.v3i1.4938

Rullyandi, M. & Fahmi Ginanjar. (2025). Peran Regulasi Hukum dalam Mengatasi Risiko Hukum Bisnis pada Platform Marketplace Berbasis Teknologi di Era Digital. *Mandalika Law Journal*, *3*(1), 1–11. https://doi.org/10.59613/mlj.v3i1.5430

Sari, D. K., & S, I. Friskanov. (2022). Edukasi Hukum Terhadap Perlindungan Identitas Diri dalam Transaksi Online Bagi Siswa di SMAN 1 Palu. *Jurnal Abdi Masyarakat Indonesia*, *2*(5), 1473–1478. https://doi.org/10.54082/jamsi.450

Setiawan, S. A. (2023). Perlindungan Hukum Negara Terhadap Hak Warga Bekerja Di Era Digital. *JURNAL RECHTENS*, *12*(1), 141–156. https://doi.org/10.56013/rechtens.v12i1.2030

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Sutarsih, T., Wulandari, V. C., Untari, R., Rozama, N. A., & Kusumantrisna, A. L. (2025). *Statistik Telekomunikasi Indonesia*. Badan Pusat Statistik.

Wahyudin, A., & Sumanto, L. (2024). Kebebasan Pers Dalam Kerangka Hukum Pelindungan Data Pribadi Di Indonesia. *Journal of Law, Administration, and Social Science*, *4*(5), 683–690. https://doi.org/10.54957/jolas.v4i5.823

Widianti, L. (2026). Konstitusi dan Keamanan Siber Layanan Publik: Kekosongan Regulasi AI sebagai Ancaman terhadap Hak atas Rasa Aman dan Perlindungan Data Pribadi. *Jurnal Kedaulatan Hukum*, *2*(1), 1–12. https://doi.org/10.65975/69q69p88

Ziqra, Y., Sunarmi, Siregar, M., & Leviza, J. (2021). Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online. *Iuris Studia: Jurnal Kajian Hukum*. https://doi.org/10.55357/is.v2i2.146