

Table Of Contents

| | |
|---|----------|
| Journal Cover | 1 |
| Author[s] Statement..... | 3 |
| Editorial Team | 4 |
| Article information | 5 |
| Check this article update (crossmark) | 5 |
| Check this article impact | 5 |
| Cite this article..... | 5 |
| Title page..... | 6 |
| Article Title | 6 |
| Author information | 6 |
| Abstract | 6 |
| Article content | 7 |

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Copyright © Author(s). This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/legalcode>

EDITORIAL TEAM

Editor in Chief

Dr. Wisnu Panggah Setiyono, Universitas Muhammadiyah Sidoarjo, Indonesia ([Scopus](#)) ([Sinta](#))

Managing Editor

Rifqi Ridlo Phahlevy , Universitas Muhammadiyah Sidoarjo, Indonesia ([Scopus](#)) ([ORCID](#))

Editors

Noor Fatimah Mediawati, Universitas Muhammadiyah Sidoarjo, Indonesia ([Sinta](#))

Faizal Kurniawan, Universitas Airlangga, Indonesia ([Scopus](#))

M. Zulfa Aulia, Universitas Jambi, Indonesia ([Sinta](#))

Sri Budi Purwaningsih, Universitas Muhammadiyah Sidoarjo, Indonesia ([Sinta](#))

Emy Rosnawati, Universitas Muhammadiyah Sidoarjo, Indonesia ([Sinta](#))

Totok Wahyu Abadi, Universitas Muhammadiyah Sidoarjo, Indonesia ([Scopus](#))

Complete list of editorial team ([link](#))

Complete list of indexing services for this journal ([link](#))

How to submit to this journal ([link](#))

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

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

Yessa Milianty, yessa.205220060@stu.untar.ac.id, (1)

Program Studi Ilmu Hukum, Universitas Tarumanagara, Indonesia

Tundjung Herning Sitabuana, tundjung@fh.untar.ac.id, (0)

Program Studi Ilmu Hukum, Universitas Tarumanagara, Indonesia

⁽¹⁾ Corresponding author

Abstract

General Background: The rapid expansion of digital services in Indonesia has transformed mobile phone numbers into core digital identifiers across banking, e-commerce, transportation, and governmental platforms. **Specific Background:** Under current regulations, particularly Ministerial Regulation No. 14/2018, inactive numbers may be recycled and reassigned without uniform data-sanitization procedures, exposing users to substantial privacy and security risks. **Knowledge Gap:** Despite the enactment of the Personal Data Protection Law, there remains regulatory disharmony between Ministerial Regulation No. 14/2018 and No. 5/2021, especially regarding conflicting timelines for data retention and number reassignment, with no standardized technical safeguards in place. **Aims:** This study examines the inconsistencies between these regulations and evaluates their implications for data protection, consumer security, and legal certainty. **Results:** Findings indicate that number-recycling practices allow residual digital identities to persist, enabling unauthorized access, data breaches, and identity theft, thereby conflicting with data-protection principles and consumer-rights provisions. **Novelty:** This research highlights the structural legal gap that permits overlapping identity cycles and proposes adopting a Reassigned Numbers Database model to mitigate misdirected authentication risks. **Implications:** Harmonizing regulatory frameworks and establishing national technical standards are urgently required to safeguard user privacy, strengthen digital-ecosystem integrity, and ensure compliance with emerging data-protection norms.

Highlights:

- Regulatory disharmony creates legal uncertainty and heightens privacy risks.
- Recycled numbers enable unauthorized access to prior users' digital accounts.
- A national Reassigned Numbers Database is crucial for safer digital authentication.

Keywords: Number Recycling, Data Protection, Privacy, Telecommunications Regulation, Consumer Security

Published date: 2025-11-18

Pendahuluan

Manusia merupakan makhluk sosial yang terus berinteraksi antara satu sama lain. Perkembangan teknologi informasi dan komunikasi telah mengubah nomor telepon seluler dari sekadar sarana komunikasi menjadi identitas digital utama dalam berbagai transaksi, mulai dari perbankan, layanan keuangan berbasis digital, e-commerce, transportasi daring, hingga sistem otentikasi dua langkah (Two-Factor Authentication/2FA). Dengan demikian, ketika suatu nomor didaur ulang oleh penyelenggara jasa telekomunikasi, risiko terhadap keamanan data pribadi, privasi, dan perlindungan konsumen meningkat secara signifikan. Praktik daur ulang nomor pelanggan (number recycling) dilakukan oleh operator seluler untuk mengelola keterbatasan sumber daya numerik yang dialokasikan negara mengingat sumber daya numerik merupakan sumber daya yang terbatas [1].

Ketika pelanggan berhenti menggunakan kartu atau tidak melakukan isi ulang dalam jangka waktu tertentu, nomor tersebut dinonaktifkan, kemudian dimasukkan ke dalam masa tenggang, dan setelahnya dipasarkan kembali kepada pelanggan baru tanpa persetujuan dari pelanggan sebelumnya. Secara administratif, kebijakan ini legal dan memang diperlukan untuk efisiensi manajemen numerasi. Namun, dari perspektif perlindungan data pribadi dan Hak Asasi Manusia (Selanjutnya disebut "HAM"), praktik ini menimbulkan persoalan serius mengingat tidak adanya kebijakan mengenai mekanisme perlindungan data yang bersangkutan dengan daur ulang nomor ini. Daur ulang nomor dapat membuka peluang pengambilalihan akun (account hijacking), akses tidak sah terhadap pesan pribadi, dan potensi penyalahgunaan layanan digital pemilik nomor sebelumnya, penelitian tersebut menunjukkan bahwa sebagian besar nomor lama yang didaur ulang masih tertaut pada berbagai akun digital yang menggunakan SMS sebagai metode pemulihan akun [2]. Temuan ini menunjukkan bahwa masalah daur ulang nomor bukan isu sederhana, tetapi berkaitan dengan struktur keamanan digital secara keseluruhan.

Dalam konteks Indonesia, risiko tersebut semakin relevan karena banyak layanan publik dan swasta yang menggunakan nomor telepon sebagai syarat otentikasi. Marketplace, mobile banking, layanan e-government, dan aplikasi ride-hailing seluruhnya mengandalkan nomor telepon sebagai basis verifikasi identitas. Ketika nomor tersebut dialihkan kepada pemilik baru tanpa prosedur keamanan yang ketat, peluang penyalahgunaan data pribadi pemilik sebelumnya sangat tinggi. Dugaan kasus-kasus semacam ini telah muncul dalam pemberitaan media nasional, termasuk laporan mengenai akses akun keuangan digital seseorang yang tidak sengaja berpindah ke pemilik nomor baru [3]. Namun demikian, regulasi Indonesia belum sepenuhnya siap menghadapi kompleksitas persoalan tersebut. Peraturan Menteri Komunikasi dan Informatika yang mengatur registrasi pelanggan prabayar, penyimpanan data pelanggan, kewajiban operator, serta manajemen numerasi masih memiliki sejumlah celah implementasi. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi (selanjutnya disebut "Permenkominfo No. 5 Tahun 2021") misalnya, mengatur registrasi pelanggan dan kewajiban penyelenggara telekomunikasi, tetapi tidak mengatur secara spesifik standar teknis sanitasi data sebelum nomor didaur ulang. Hal ini menyebabkan prosedur antaroperator berbeda-beda dan tidak adanya standar minimal nasional yang mengatur keamanan data pribadi ketika nomor berpindah tangan. Di sisi lain, lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (selanjutnya disebut "UU PDP") memperkuat kewajiban penyelenggara telekomunikasi sebagai pengendali data untuk melindungi data pribadi pelanggan [4], termasuk data yang mungkin masih terkait dengan nomor ponsel yang didaur ulang. Pasal 5 UU PDP mengharuskan pengendali data melakukan perlindungan melalui langkah organisasi, prosedur, serta teknis yang memadai [5].

Sementara itu, regulasi Indonesia belum sepenuhnya mengantisipasi kompleksitas persoalan tersebut. Permenkominfo No. 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi mengatur bahwa data pelanggan yang sudah tidak aktif harus disimpan sekurang-kurangnya 3 bulan sejak tanggal ketidakaktifan [6]. Namun, ketentuan ini berbenturan dengan Peraturan Menteri Komunikasi dan Informatika Nomor 14 Tahun 2018 tentang Rencana Dasar Teknis Telekomunikasi Nasional (selanjutnya disebut "Permenkominfo No. 14 Tahun 2018"), yang menyatakan bahwa nomor pelanggan dapat diberikan kepada pelanggan baru setelah masa jeda 60 hari (2 bulan) [7]. Perbedaan pengaturan ini menimbulkan ketidakpastian hukum mengenai kapan data pelanggan harus dihapus dan kapan nomor boleh dipasarkan kembali. Kontradiksi ini berpotensi menimbulkan benturan antara perlindungan data dan efisiensi manajemen numerasi. Jika nomor dapat didaur ulang setelah 60 hari, tetapi data pelanggan masih wajib disimpan selama 90 hari, maka terdapat masa 30 hari di mana nomor dapat diberikan kepada pengguna baru sementara data pelanggan lama masih tersimpan oleh operator. Hal ini menimbulkan risiko kebocoran data, pelanggaran privasi, dan ketidakjelasan tanggung jawab operator telekomunikasi. Kekosongan hukum mengenai mekanisme penghapusan data dan juga mekanisme daur ulang nomor pelanggan juga merupakan penyebab semakin maraknya kasus kebocoran data pribadi di Indonesia.

Kasus-kasus nyata terus bermunculan, misalnya pada tahun 2024, seorang warga melalui akun X @shakazam1524 melaporkan kehilangan dana sejumlah US\$1.200 dari akun PayPal akibat nomor ponselnya didaur ulang tanpa pemberitahuan memadai [8]. Kasus tersebut menunjukkan lemahnya perlindungan terhadap pelanggan dan ketidaksiapan operator dalam memastikan keamanan data pribadi. Dari perspektif HAM, Undang-Undang Dasar Negara Republik Indonesia tahun 1945 (selanjutnya disebut "UUD NRI 1945") Pasal 28G ayat (1) menjamin hak atas rasa aman dan perlindungan dari ancaman terhadap diri pribadi [9]. Pelanggaran data pribadi melalui daur ulang nomor dapat dikategorikan sebagai pelanggaran terhadap hak atas privasi sebagai bagian dari HAM modern. Warren dan Brandeis telah menekankan sejak 1890 bahwa hak atas privasi merupakan hak dasar manusia untuk "be let alone" [10]. Hingga kini, belum ada standar nasional seperti reassigned numbers database sebagaimana di Amerika Serikat, yang memungkinkan layanan digital memeriksa status nomor sebelum mengirimkan kode verifikasi kepada pengguna [11].

Ketidakharmonisan dan kekosongan hukum ini menyebabkan pelanggan tidak mendapatkan perlindungan yang memadai dan tidak adanya standar nasional yang mengatur bagaimana data harus dihapus, diverifikasi, atau diamankan sebelum nomor kembali dipasarkan. Oleh karena itu, pengharmonisan Permenkominfo menjadi kebutuhan mendesak. Dengan

demikian, urgensi pengharmonisasian regulasi bukan sekadar untuk memperbaiki ketentuan administratif, tetapi untuk melindungi integritas ekosistem digital nasional, keamanan data pribadi warga negara, dan kepercayaan publik terhadap penyelenggara telekomunikasi. Kegiatan ekonomi digital bergantung pada stabilitas sistem identitas elektronis, dan tanpa regulasi yang selaras, dampak terhadap ekonomi nasional dapat signifikan. Berdasarkan uraian tersebut, jelas bahwa pengharmonisasian Peraturan Menteri Komunikasi dan Informatika dengan UU PDP dan UU Perlindungan merupakan kebutuhan strategis dalam memastikan bahwa kebijakan daur ulang nomor tidak menimbulkan risiko terhadap privasi, keamanan, dan hak-hak pelanggan di era digital.

Metode

Metode penelitian yang digunakan dalam penelitian ini adalah metode yuridis normatif, yang merupakan pendekatan penelitian hukum yang fokus pada kajian terhadap aturan dan prinsip hukum yang terdapat dalam peraturan perundang-undangan, doktrin hukum, dan literatur hukum tertulis lainnya [12]. Penelitian ini dilakukan dengan menelaah dan menganalisis secara mendalam sumber-sumber hukum resmi seperti Peraturan Menteri Komunikasi dan Informatika, peraturan perundang-undangan terkait, serta dokumen hukum lain yang relevan untuk mendapatkan gambaran komprehensif mengenai urgensi pengharmonisasian kebijakan daur ulang nomor pelanggan. Data yang diperoleh bersifat kualitatif dan dianalisis secara normatif dengan pendekatan perundang-undangan (statute approach) dan konseptual (conceptual approach) untuk memahami hubungan antar norma dan merumuskan argumen yang mendasari kebutuhan harmonisasi regulasi tersebut. Penelitian ini tidak melibatkan pengumpulan data lapangan sehingga seluruh kajian berbasis kepustakaan dan dokumen hukum resmi.

Hasil dan Pembahasan

Penggunaan teknologi pada saat ini sudah berkembang pesat dan tidak dapat dipisahkan dalam kehidupan sehari-hari masyarakat global. Ponsel merupakan salah satu inovasi teknologi mempermudah manusia sebagai makhluk sosial untuk berinteraksi antara satu sama lain. Di tahun 2024 menunjukkan kurang lebih 353-354 juta koneksi ponsel yang aktif dengan penetrasi hingga 126,8% yang menjadikan Indonesia sebagai pasar ponsel terbesar ke-4 (empat) di dunia [13]. Paralel dengan lonjakan pengguna ponsel, jumlah SIM (Subscriber Identity Module) yang aktif di Indonesia terdapat sekitar 315-348 juta dari April sampai Mei 2025, data ini menunjukkan satu orang memiliki lebih dari satu nomor mengingat jumlah penduduk di Indonesia hanya sekitar 280 juta jiwa [14]. Meningkatnya permintaan akan nomor telepon khususnya di Indonesia, menyebabkan pemerintah mengeluarkan kebijakan daur ulang nomor ponsel (recycle) yang dituangkan dalam Permenkominfo No. 14 Tahun 2018 untuk menjawab permintaan tersebut. Nomor telepon perlu dikelola secara efisien dan diatur secara bijak agar dapat memenuhi kebutuhan masyarakat secara berkelanjutan, mengingat nomor telepon merupakan sumber daya numerik yang terbatas.

Nomor telepon yang sudah tidak aktif akan didaur ulang oleh Penyedia Jasa Telekomunikasi (operator) dengan ataupun tanpa persetujuan dari pelanggan sebelumnya, hal ini meningkatkan risiko kebocoran data pribadi pelanggan sebelumnya. Nomor telepon menjadi identitas tunggal masyarakat yang terkoneksi dengan akun - akun digital yang penting seperti e-banking, e-commerce, e-wallet, dan akun media sosial yang merupakan ranah privasi. Ancaman ini menjadi nyata ketika banyaknya kasus yang bermunculan mengenai kebocoran data akibat dari praktik daur ulang nomor ponsel yang dikeluarkan pemerintah tanpa adanya pengaturan yang jelas mengenai mekanisme sanitasi data dan juga mekanisme daur ulang nomor yang jelas. Kebocoran data dialami oleh akun x @shakazam1524 di tahun 2024 yang mengalami pembobolan kartu kredit dan penarikan uang sebesar US\$1.200, ia tidak memperhatikan masa aktif nomornya hingga diblokir oleh operator tanpa sepengetahuannya [8]. Operator dapat dengan memblokir dan memperjuangkan kembali nomor pelanggan tanpa pengetahuan dan persetujuan pelanggan meningkatkan risiko ancaman keamanan mengenai privasi pelanggannya terlebih jika nomor tersebut berujung pada pihak ke-3 (tiga) yang tidak bertanggung jawab dan berniat untuk mengambil keuntungan melalui data pribadi dan juga akun yang masih terkoneksi dalam nomor telepon.

Permasalahan semakin kompleks ketika ditinjau dari aspek normatif karena terdapat ketidaksinkronan (legal gap) antara Permenkominfo No. 14 Tahun 2018 dengan Permenkominfo No. 5 Tahun 2021. Permenkominfo No. 5 Tahun 2021 mewajibkan penyelenggara telekomunikasi untuk menyimpan data pelanggan yang tidak aktif selama paling sedikit 3 bulan sejak dinyatakan tidak aktif [6]. Bertentangan dengan Permenkominfo No. 14 Tahun 2018 yang menyatakan bahwa nomor bisa dimanfaatkan oleh calon pelanggan lain minimal 60 hari (2 bulan) sejak dinyatakan tidak aktif atau tidak lagi dipergunakan [7]. Dengan demikian, ketika suatu nomor telah didaur ulang setelah 60 hari, data pemilik sebelumnya masih tersimpan dan menjadi tanggung jawab operator selama kurang lebih 30 hari berikutnya. Ketidaksinkronan antara jangka waktu penyimpanan data (90 hari) dan jangka waktu daur ulang (60 hari) menciptakan kondisi di mana nomor yang sudah dipindahtangankan kepada pengguna baru masih memiliki keterhubungan data dengan pemilik lama. Kontradiksi antara kedua regulasi ini menimbulkan permasalahan yang berdampak langsung terhadap perlindungan konsumen serta perlindungan atas privasi. Dalam kasus tertentu, pengguna baru kerap kali menemukan bahwa nomor yang mereka peroleh masih terhubung dengan berbagai akun digital milik pemilik sebelumnya. Misalnya, pengguna baru masih dapat menemukan akun WhatsApp pemilik lama, terhubung dengan akun marketplace seperti Shopee atau Tokopedia, bahkan menerima pesan penagihan dari aplikasi kredit digital seperti Kredivo, OVO Paylater, atau Gopaylater. Situasi ini tidak hanya mengganggu kenyamanan pengguna baru, tetapi juga menyebabkan pemilik lama berpotensi mengalami kebocoran data pribadi, akses tidak sah terhadap akun, dan risiko pencurian identitas.

Dalam Pasal 153 ayat (2) Permenkominfo No. 5 Tahun 2021 menjelaskan bahwa Penyelenggara Jasa Telekomunikasi wajib untuk menerapkan prinsip mengenal pelanggan, definisi prinsip pengenalan pelanggan terdapat dalam Pasal 1 angka 37 Permenkominfo tersebut yang berbunyi: "Prinsip Mengetahui Pelanggan (Know Your Customer/KYC), adalah prinsip yang diterapkan untuk mengetahui identitas pelanggan adalah benar dan digunakan oleh orang yang berhak." [6] Secara hukum,

prinsip KYC tidak hanya berkaitan dengan verifikasi identitas saat tahap awal pendaftaran, melainkan juga mencakup kewajiban penyelenggara untuk memastikan bahwa setiap akses terhadap layanan telekomunikasi benar-benar dilakukan oleh subjek data yang sah sepanjang siklus penggunaan nomor tersebut. Dalam Permenkominfo No. 5 Tahun 2021 Pasal 153 ayat (5) mewajibkan Penyelenggara Jasa Telekomunikasi untuk mengedarkan Kartu Perdana dalam kondisi tidak aktif untuk seluruh layanan Jasa Telekomunikasi [6]. Secara normatif, ketentuan ini menggambarkan bahwa penyelenggara telekomunikasi memiliki tanggung jawab kuat untuk menjaga keamanan identitas pelanggan sejak tahap pra-aktivasi hingga pasca-pengakhiran layanan. Hal ini menjadi tidak terpenuhi jika banyak kasus kebocoran data yang terjadi karena akun digital pelanggan sebelumnya masih dapat diakses oleh pelanggan berikutnya bahkan tidak jarang disalahgunakan oleh pihak yang tidak bertanggung jawab.

Kewajiban normatif tersebut tidak terpenuhi ketika dalam praktiknya masih banyak terjadi kebocoran data dan akses ilegal melalui nomor seluler yang telah didaur ulang. Fakta bahwa akun-akun digital milik pelanggan sebelumnya masih dapat diakses oleh pengguna baru menunjukkan adanya kegagalan operator dalam menegakkan prinsip KYC secara menyeluruh, khususnya pada fase post-termination. Ketika suatu nomor diberikan kepada pengguna baru tanpa memastikan bahwa semua data, riwayat akun, dan tautan digital milik pemilik sebelumnya telah sepenuhnya diputus, maka identitas yang seharusnya terlindungi justru berpindah kepada pihak lain yang tidak berhak. Situasi ini bertentangan langsung dengan definisi KYC, karena identitas digital yang melekat pada nomor tersebut tidak lagi “digunakan oleh orang yang berhak”. Lebih jauh lagi, kondisi tersebut juga mencerminkan bahwa kewajiban mengedarkan kartu perdana dalam keadaan tidak aktif menjadi tidak bermakna apabila nomor hasil daur ulang secara implisit masih membawa jejak identitas digital pemilik sebelumnya. Hal ini menyebabkan dua konsekuensi hukum: (1) pelanggan baru dapat mengakses data pribadi yang bukan miliknya, sehingga berpotensi melakukan tindakan penyalahgunaan identitas; dan (2) pelanggan lama kehilangan kontrol atas akunnya karena identitas digital yang terautentikasi melalui nomor tersebut berpindah ke orang lain. Dengan demikian, kebocoran data yang terjadi dalam proses daur ulang nomor bukan sekadar masalah teknis, tetapi merupakan bentuk ketidakpatuhan terhadap kewajiban perlindungan data pribadi, asas keamanan, dan prinsip KYC yang diwajibkan oleh regulasi. Kondisi ini memperlihatkan adanya celah dalam mekanisme pengelolaan data oleh operator, khususnya dalam memastikan bahwa proses pengakhiran layanan benar-benar disertai pemutusan dan penghapusan data pelanggan (data wiping) sebelum nomor dialokasikan kembali. Tanpa perbaikan mekanisme ini, kewajiban KYC tidak hanya gagal diterapkan, tetapi juga berpotensi menimbulkan kerugian hukum, kerugian ekonomi, dan pelanggaran privasi yang serius bagi konsumen.

Pada tingkat yang lebih fundamental, data pribadi merupakan HAM atas privasi yang harus dipenuhi dan tidak dapat dikurangi (*derogable rights*). definisi data pribadi termaktub dalam Pasal 1 angka 1 UU PDP yang menjelaskan bahwa: "Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik." [5]. HAM diatur secara internasional dalam Pasal 12 Universal Declaration of Human Rights tahun 1948 yang mengatur bahwa: "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" [15]. Pasal 1 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (selanjutnya disebut "UU HAM"), mengatur definisi HAM bahwa: "Hak Asasi Manusia (HAM) adalah seperangkat hak yang melekat pada hakikat dan keberadaan manusia sebagai makhluk Tuhan Yang Maha Esa dan merupakan anugerah-Nya yang wajib dihormati, dijunjung tinggi, dan dilindungi oleh negara, hukum, pemerintah dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia." [16] Seiring pesatnya perkembangan teknologi dan informasi, pemahaman tentang hak pribadi mengalami perluasan, tidak lagi terbatas pada hak kepemilikan, tetapi juga mencakup hak atas privasi [17].

Untuk menjawab permasalahan struktural ini, Indonesia dapat mengadopsi model Reassigned Numbers Database (RND) sebagaimana diterapkan di Amerika Serikat. RND merupakan basis data nasional yang dibentuk oleh Federal Communications Commission (FCC) untuk mencatat nomor telepon yang telah diputuskan (*disconnected*) dan kemudian dialihkan kepada pemilik baru, sehingga penyedia layanan digital dapat melakukan pemeriksaan guna memastikan apakah suatu nomor telah dialihkan sejak tanggal tertentu sebelum mengirimkan kode verifikasi atau OTP kepada pengguna [18]. Melalui sistem ini, layanan digital seperti bank, e-wallet, marketplace, atau penyedia OTP dapat melakukan pengecekan otomatis untuk mengetahui apakah sebuah nomor telah direassign sebelum mengirimkan kode verifikasi atau memberikan akses ke akun sensitif. Studi hukum dari Manatt, Phelps & Phillips juga menunjukkan bahwa penerapan RND secara signifikan mengurangi risiko kesalahan pengiriman OTP dan penipuan berbasis nomor telepon, serta menjadi instrumen kepatuhan penting terhadap Telephone Consumer Protection Act (TCPA) [19]. Implementasi RND di Indonesia akan menutup celah yang selama ini menyebabkan kebocoran data akibat nomor hasil daur ulang, sekaligus memastikan bahwa prinsip KYC, keamanan data, dan hak privasi terlindungi secara optimal. Dengan adanya basis data yang terintegrasi dan kewajiban operator untuk melakukan pelaporan berkala, mekanisme daur ulang nomor dapat dilakukan secara aman, transparan, dan bertanggung jawab. Oleh karena itu, pengembangan RND nasional merupakan langkah strategis yang tidak hanya memperkuat perlindungan konsumen dan data pribadi, tetapi juga memastikan bahwa pengelolaan numerasi telekomunikasi di Indonesia selaras dengan standar internasional dan kebutuhan masyarakat digital yang semakin kompleks.

Simpulan

Kebijakan daur ulang nomor seluler sebagaimana diatur dalam Permenkominfo No. 14 Tahun 2018 dan Permenkominfo No. 5 Tahun 2021 masih menyisakan ketidaksinkronan normatif, terutama terkait perbedaan jangka waktu penyimpanan data pelanggan dan waktu diperbolehkannya nomor untuk didaur ulang. Disharmoni tersebut menimbulkan celah regulasi yang menyebabkan tidak adanya kepastian hukum mengenai kapan data pelanggan harus dihapus dan kapan nomor boleh

dipindahtangankan kepada pengguna baru. Akibatnya, risiko tumpang tindih identitas digital, kebocoran data pribadi, hingga akses ilegal terhadap layanan digital semakin meningkat dan merugikan konsumen. Kondisi ini menunjukkan bahwa mekanisme daur ulang nomor belum sejalan dengan kewajiban perlindungan data pribadi sebagaimana diatur dalam UU PDP serta belum memenuhi prinsip keamanan dan kenyamanan konsumen sebagaimana ditentukan dalam UU Perlindungan Konsumen. Ketiadaan prosedur sanitasi data yang baku memperparah risiko tersebut, karena operator tidak diwajibkan untuk memastikan bahwa seluruh jejak digital pemilik lama telah terputus sebelum nomor dialihkan. Di sisi lain, meningkatnya ketergantungan masyarakat pada nomor telepon sebagai identitas digital menjadikan permasalahan ini semakin krusial dalam ekosistem digital nasional. Dengan demikian, dapat disimpulkan bahwa harmonisasi regulasi, penegakan mekanisme perlindungan data, dan penguatan standar teknis merupakan kebutuhan mendesak untuk memastikan keamanan privasi masyarakat dalam sistem numerasi nasional.

Saran untuk penelitian ini berupa pemerintah perlu segera melakukan harmonisasi regulasi antara Permenkominfo No. 14 Tahun 2018 dan Permenkominfo No. 5 Tahun 2021 untuk menghilangkan konflik normatif serta memberikan kepastian hukum mengenai jangka waktu penyimpanan data dan proses daur ulang nomor. Penyusunan standar teknis yang baku, termasuk mekanisme sanitasi data, pemutusan tautan akun digital, dan prosedur pemeriksaan keamanan sebelum nomor dialihkan, harus ditetapkan melalui regulasi yang bersifat mengikat. Pemerintah juga perlu mempertimbangkan pembangunan basis data nasional ala Reassigned Numbers Database (RND) untuk mencegah akses tidak sah pada layanan digital melalui nomor yang telah dialihkan. Operator telekomunikasi harus diwajibkan untuk meningkatkan transparansi, memberikan peringatan yang memadai kepada pelanggan sebelum nomor dinonaktifkan, serta menjamin bahwa data pelanggan lama benar-benar dihapus. Selain itu, pengawasan dan sanksi harus diperketat untuk memastikan kepatuhan operator terhadap prinsip perlindungan data pribadi. Masyarakat juga memerlukan edukasi yang lebih komprehensif mengenai risiko nomor daur ulang dan pentingnya menjaga masa aktif nomor untuk melindungi keamanan digital mereka. Dengan langkah-langkah ini, diharapkan sistem daur ulang nomor seluler dapat berjalan lebih aman, transparan, dan memberikan perlindungan optimal bagi seluruh pengguna.

References

1. K. A. Azzahra et al., "Pelindungan Hak Subjek Data Pribadi dalam Kebijakan Penggunaan Ulang Nomor Telepon Seluler Ditinjau Menurut Hukum Positif Indonesia," *Jurnal Hukum, Politik dan Ilmu Sosial*, no. 3, p. 414, 2024.
2. K. Lee and A. Narayanan, *Security and Privacy Risks of Number Recycling at Mobile Carriers*. Princeton, NJ, USA: Princeton University, 2021.
3. Y. Belinda, "Indonesia's Phone Number Recycling May Result in Data Leaks," 2021.
4. J. Matheus and A. Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan dengan KPPU," *JUSTISI*, vol. 10, no. 1, pp. 20–35, 2024.
5. Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022.
6. Republik Indonesia, Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi, 2021.
7. Republik Indonesia, Peraturan Menteri Komunikasi dan Informatika Nomor 14 Tahun 2018 tentang Rencana Dasar Teknis Telekomunikasi Nasional, 2018.
8. Suharno, "Kominfo Komentari Kabar Viral Pembobolan Rekening dari SIM Card Mati," 2024.
9. Republik Indonesia, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 27 ayat (1), 1945.
10. S. Warren and L. D. Brandeis, "The Right to Privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, 1890.
11. Telnix Engineering, "What Is the U.S. Reassigned Numbers Database?," Telnix, [Online]. Available: <https://telnix.com>
12. S. Soekanto and S. Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, 16th ed. Jakarta, Indonesia: Rajawali Pers, 2014.
13. C. Saskia, "Ada 354 Juta Ponsel Aktif di Indonesia Terbanyak Nomor Empat Dunia," 2023.
14. M. I. Nafian, "Menkomdigi Sebut SIM Card Aktif di RI Ada 315 Juta Lebih Populasi," 2025.
15. United Nations, *Universal Declaration of Human Rights*, 1948.
16. Republik Indonesia, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. Jakarta: Sekretariat Negara Republik Indonesia, 1999.
17. Y. Khairunnisa, "Pertanggungjawaban terhadap Perlindungan Data Pribadi dalam Praktik Daurlang Nomor Telepon Seluler," 2024.
18. Federal Communications Commission (FCC), "Reassigned Numbers Database Order," 2018.
19. C. M. Reilly and A. P. Heeringa, "Reassigned Number Database Up and Running," 2025.