Legal: Jurnal Reformasi Hukum Pidana dan Perdata
Volume: 1, Nomor: 2, (2026), Juni: 94 - 110
Website: https://ejournal.ojs-lppm.com/index.php/Legal/article/view/62
E-ISSN: 3124-8624

TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI SARANA *SHORT MESSAGE SERVICE*

Lambok Tri Junianto Simanjuntak [1], Wenly R. J. Lolong [2], Merry L. Kumajas [3]
Program Studi Ilmu Hukum, Universitas Negeri Manado, Indonesia [1,2,3]
Corresponding Author: *lamboktjas6@gmail.com[1*]*, *wenly.lolong@unima.ac.id[2]*, *Merry.kumajas@unima.ac.id[3]*

Info Artikel
Received: *10 April 2026*
Revised : *07 Mei 2026*
Accepted: *13 Mei 2026*
Published: *25 Mei 2026*

Keywords: *Crime, Theft, Personal Data, Short Message Service*

Abstract
The development of information technology has given rise to the phenomenon of cybercrime in the form of personal data theft via SMS. This study aims to analyze the legal provisions governing the protection of personal data against theft via Short Message Service (SMS) and to identify forms of personal data theft via SMS that can be classified as criminal acts. This study is a normative legal study by examining the Personal Data Protection Law, the Electronic Information and Transactions Law and its amendments, the Consumer Protection Law, and relevant provisions in the Criminal Code. The results show that personal data theft via SMS, such as phishing, misuse of institutional identity, use of data for illegal transactions, and sale of data to third parties, fulfills the elements of a criminal act in the form of intent, unauthorized access, unlawful acts, unauthorized dissemination of data, and intent to control or gain profit. All of these methods have a clear basis for criminal punishment in Indonesian positive law and emphasize the importance of strengthening legal protection of personal data in the digital era.

Kata Kunci*:* Tindak Pidana, Pencurian, Data Pribadi, *Short Message Service*

Abstrak
Perkembangan teknologi informasi memunculkan fenomena kejahatan siber berupa pencurian data pribadi melalui sarana SMS. Penelitian ini bertujuan untuk menganalisis ketentuan hukum yang mengatur perlindungan data pribadi terhadap pencurian melalui Short Message Service (SMS) serta mengidentifikasi bentuk-bentuk pencurian data pribadi melalui SMS yang dapat dikualifikasikan sebagai tindak pidana. Penelitian ini adalah penelitian hukum normatif dengan menelaah Undang-Undang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Perlindungan Konsumen, dan ketentuan relevan dalam Kitab Undang-Undang Hukum Pidana. Hasil penelitian menunjukkan bahwa pencurian data pribadi melalui SMS, seperti phishing, penyalahgunaan identitas lembaga, penggunaan data untuk transaksi ilegal, serta penjualan data kepada pihak ketiga, memenuhi unsur-unsur tindak pidana berupa kesengajaan, akses tanpa hak, perbuatan melawan hukum, penyebarluasan data tanpa izin, dan niat untuk menguasai atau memperoleh keuntungan. Seluruh modus ini memiliki dasar pemidanaan yang jelas dalam hukum positif Indonesia dan menegaskan pentingnya penguatan perlindungan hukum atas data pribadi di era digital.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Publisher: Lembaga Penerbit Penelitian Multidisipliner

PENDAHULUAN

Perkembangan teknologi informasi telah melahirkan berbagai bentuk kejahatan siber, salah satunya adalah pencurian data pribadi.[1] Data pribadi pada hakikatnya merupakan identitas yang melekat pada seseorang dan bersifat unik, seperti nomor induk kependudukan, nomor rekening, maupun informasi pribadi lain yang jika disalahgunakan dapat menimbulkan kerugian bagi pemiliknya.[2] Salah satu sarana yang sering digunakan untuk pencurian data adalah *Short Message Service* (SMS). Melalui SMS, pelaku dapat menyebarkan pesan berisi tautan palsu, undian berhadiah, atau permintaan data pribadi yang seolah-olah berasal dari lembaga resmi.[3] Modus sederhana ini terbukti efektif karena SMS masih digunakan secara luas oleh masyarakat, khususnya dalam layanan perbankan, komunikasi, dan notifikasi digital.

Fenomena pencurian data pribadi bukan lagi isu yang bersifat potensial, melainkan telah menjadi masalah nyata dengan dampak luas. Laporan Kominfo tahun 2022 menunjukkan bahwa mayoritas kasus penyalahgunaan data pribadi di Indonesia dilakukan melalui kanal komunikasi sederhana seperti SMS dan *WhatsApp*[4]. Beberapa kasus menimbulkan kerugian finansial, seperti hilangnya dana nasabah bank setelah mengklik tautan dalam SMS *phishing*. Fenomena ini menegaskan bahwa pencurian data pribadi melalui SMS tidak hanya menyasar masyarakat awam, tetapi juga dapat merugikan korporasi maupun lembaga keuangan yang kredibilitasnya dicatut oleh pelaku.

Dalam perspektif hukum, pencurian data pribadi melalui SMS dapat dikualifikasikan sebagai tindak pidana karena menyangkut perolehan dan penggunaan data pribadi tanpa hak. Indonesia sebenarnya telah memiliki perangkat hukum untuk melindungi data pribadi, yakni Undang-Undang Nomor 11 Tahun 2008. UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE)[5],

---

[1] Syarfani dan Mahendra Putri Kurnia, "Tinjauan Yuridis terhadap Perlindungan Data Pribadi di Media Elektronik (Berdasarkan Pasal 25 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik)," *Jurnal Beraja Niti* 3 (2014).
[2] Richardus Eko Indrajit, "Fenomena Kebocoran Data: Mencari Sumber Penyebab dan Akar Permasalahannya," diakses 18 Mei 2024, http://folder.idsirtii.or.id/pdf/IDSIRTII-Artikel309 FenomenaKebicoranData.pdf

[3] I Made Wahyu Chandra Satriana dan Ni Made Liana Dewi, "Penyuluhan Hukum tentang *Spamming* SMS yang Mengandung Unsur Perjudian di Kalangan Generasi Muda," *Journal of Human Education* 3, no. 4 (2023): 62–66.
[4] Kementerian Komunikasi dan Informatika Republik Indonesia, "Waspada Kejahatan Siber dan Kebocoran Data Pribadi di Era Digital," *Kominfo.go.id*, diakses 18 Mei 2024 https://aptika.kominfo.go.id/.
[5] Republik Indonesia, *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, sebagaimana telah diubah dengan *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Lembaran Negara Republik Indonesia Tahun 2024 Nomor 12.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)[6]**,** serta Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen[7]. Namun, dalam implementasinya, regulasi tersebut seringkali belum berjalan optimal. Masih banyak kasus pencurian data melalui SMS yang hanya berakhir dengan pemblokiran nomor pelaku tanpa proses pidana yang tuntas. Kondisi ini menunjukkan adanya kesenjangan antara norma hukum dan praktik penegakan hukum di lapangan.

Meskipun UU ITE, UU Perlindungan Konsumen, dan UU Perlindungan Data Pribadi telah memberikan dasar normatif bagi perlindungan hukum atas data pribadi, namun implementasinya di lapangan masih menunjukkan berbagai keterbatasan. Norma hukum yang ada cenderung bersifat fragmentaris, belum sepenuhnya menyentuh pada modus pencurian data melalui sarana SMS, sehingga sering kali penanganan kasus hanya berhenti pada tataran administratif. Kondisi ini menimbulkan pertanyaan akademik tentang sejauh mana instrumen hukum yang ada mampu melindungi data pribadi masyarakat secara efektif.

Menurut Nugroho, Samsudi, dan Nurhayati, persoalan penyebaran spam melalui SMS dalam UU ITE belum diatur secara tegas sebagai tindak pidana, karena pasal yang ada lebih menekankan pada gangguan sistem elektronik. Hal ini relevan dengan penelitian ini karena sama-sama menggunakan SMS sebagai sarana, meskipun fokus kajian berbeda: Nugroho menekankan aspek spam dan sistem elektronik, sementara penelitian ini menitikberatkan pada pencurian data pribadi dan perlindungan korban[8]. Selanjutnya, menurut Nabila, perlindungan hukum korban penipuan melalui SMS dapat ditemukan dalam KUHP, UU Perlindungan Saksi dan Korban, serta hukum pidana Islam. Relevansinya dengan penelitian ini terletak pada posisi korban sebagai subjek yang perlu dilindungi, hanya saja penelitian ini memberikan pendekatan lebih luas dengan mengintegrasikan UU ITE, UU Perlindungan Konsumen, dan UU Perlindungan Data Pribadi[9]. Dengan demikian, riset ini memperluas ruang lingkup kajian dengan menghubungkan perlindungan hukum pidana, perlindungan konsumen, dan perlindungan data pribadi secara komprehensif dalam konteks pencurian data melalui SMS.

---

[6] Republik Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 237, Pasal 65 ayat (1).
[7] Republik Indonesia, *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*, Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42, Pasal 9 ayat (1).
[8] Christian Adhi Nugroho S., Samsudi, dan Dwi Endah Nurhayati, *Kebijakan Hukum Pidana terhadap Pembuatan Penyebaran Spam melalui Short Message Service (SMS)*, Artikel Ilmiah Hasil Penelitian Mahasiswa (Jember: Fakultas Hukum, Universitas Jember, 2023).
[9] Farid Nabila, *Perlindungan Hukum terhadap Korban Penipuan melalui SMS (Short Message Service)*, Skripsi (Jember: Fakultas Syariah, Universitas Islam Negeri Kiai Haji Achmad Siddiq, 2023).

Urgensi penelitian ini terletak pada pentingnya memberikan perlindungan hukum yang efektif terhadap korban pencurian data pribadi melalui SMS. Penelitian ini bertujuan untuk menjawab dua permasalahan utama, yaitu: (1) Bagaimana ketentuan hukum yang mengatur pencurian data pribadi melalui sarana Short Message Service (SMS) dalam Undang-Undang ITE, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi?; dan (2) Bagaimana bentuk pertanggungjawaban pelaku pencurian data pribadi melalui sarana Short Message Service (SMS) menurut hukum pidana? Dengan menjawab kedua pertanyaan tersebut, penelitian ini diharapkan dapat memberikan kontribusi akademik sekaligus rekomendasi praktis bagi pembuat kebijakan dan aparat penegak hukum.

Teori yang digunakan dalam penelitian ini adalah teori perlindungan hukum yang menempatkan hukum sebagai sarana untuk mengintegrasikan berbagai kepentingan masyarakat agar tercipta keadilan, ketertiban, dan kepastian. Menurut Salmond dalam Fitzgerald (1966), hukum berfungsi melindungi kepentingan tertentu dengan cara membatasi kepentingan lainnya, sehingga hukum memiliki otoritas untuk menentukan kepentingan mana yang perlu diatur dan dijaga.[10] Setiono (2004), memandang perlindungan hukum sebagai upaya mencegah tindakan sewenang-wenang penguasa demi terciptanya ketenteraman[11], sedangkan Muchsin (2003), menekankan perlindungan hukum sebagai usaha melindungi individu melalui penyerasian nilai-nilai dan kaidah dalam kehidupan bermasyarakat[12]. Dengan demikian, sebagai negara hukum berdasarkan Pancasila, Indonesia berkewajiban memberikan perlindungan hukum kepada seluruh warga negara tanpa diskriminasi, termasuk dalam konteks perlindungan data pribadi.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif, yaitu penelitian hukum yang bertumpu pada studi kepustakaan dengan menelaah norma hukum positif yang berlaku, asas-asas hukum, serta doktrin-doktrin yang relevan.[13] Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*) dengan menelaah ketentuan dalam UU ITE, UU Perlindungan Data Pribadi, dan UU Perlindungan Konsumen**,** serta pendekatan konseptual (*conceptual approach*)[14] untuk memahami ketentuan hukum yang mengatur tndak pidana pencurian data melalui sarana SMS dan bentuk-bentuk

[10] Satjipto Rahardjo, *Ilmu Hukum* (Bandung: PT Citra Aditya Bakti, 2000), 53.
[11] Setiono, *"Rule of Law"* (Disertasi S2, Fakultas Hukum, Universitas Sebelas Maret, Surakarta, 2004), 3.
[12] Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia* (Disertasi S2, Fakultas Hukum, Universitas Sebelas Maret, Surakarta, 2003), 14.
[13] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2017), hlm. 35.
[14] Ibid., hlm. 93.

modus pencurian data pribadi**.**

Sumber data yang digunakan adalah data sekunder diperoleh dari studi kepustakaan (*library research*)[15]. Terdiri atas bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian, serta bahan hukum tersier berupa kamus hukum dan ensiklopedia. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan, sedangkan analisis bahan hukum dilakukan dengan metode deskriptif-kualitatif, yaitu menguraikan, menafsirkan, dan menghubungkan norma hukum yang ada dengan fakta hukum dalam kasus pencurian data pribadi melalui SMS, sehingga diperoleh jawaban atas rumusan masalah yang telah ditetapkan.

HASIL DAN PEMBAHASAN

A. Ketentuan Hukum yang Mengatur Perlindungan Data Pribadi terhadap Pencurian melalui SMS

1. Pengaturan umum perlindungan data pribadi di Indonesia

Perkembangan teknologi komunikasi telah memungkinkan terjadinya interaksi yang cepat dan luas antarindividu, namun di sisi lain juga memunculkan berbagai bentuk kejahatan berbasis digital, salah satunya adalah pencurian data pribadi melalui sarana Short Message Service (SMS). Dalam konteks hukum Indonesia, perbuatan ini diatur melalui beberapa perangkat peraturan perundang-undangan, yang saling melengkapi dalam memberikan perlindungan terhadap hak individu atas data pribadi.

Perlindungan terhadap data pribadi di Indonesia telah diatur melalui berbagai instrumen hukum. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan landasan utama dalam mengatur hak subjek data dan kewajiban pengendali maupun prosesor data. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diperbarui dengan Undang-Undang Nomor 1 Tahun 2024 menegaskan pentingnya persetujuan subjek data dalam penggunaan informasi pribadi. Selain itu, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen turut memberikan perlindungan bagi masyarakat dari informasi menyesatkan yang sering menjadi bagian dari modus kejahatan melalui SMS. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap pencurian data pribadi melalui SMS tercakup dalam beberapa regulasi, yaitu:

2. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

[15] Ibid., hlm. 95.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan regulasi yang memberikan dasar hukum komprehensif dalam mengatur hak subjek data, kewajiban pengendali serta prosesor data, dan larangan pengumpulan maupun penyebarluasan data pribadi tanpa dasar yang sah.[16] Ketentuan dalam undang-undang ini menegaskan bahwa setiap proses pengolahan data pribadi harus dilakukan secara transparan, aman, dan sesuai tujuan yang telah diinformasikan kepada pemilik data. Relevansi UU PDP menjadi sangat penting dalam konteks pencurian data pribadi melalui SMS, karena praktik tersebut pada umumnya dilakukan tanpa persetujuan, tanpa dasar hukum, dan seringkali disertai manipulasi yang merugikan subjek data pribadi. Oleh karena itu, pasal-pasal yang terdapat dalam UU PDP perlu dianalisis secara rinci untuk melihat sejauh mana ketentuan tersebut dapat memberikan perlindungan yang efektif terhadap korban pencurian data melalui sarana SMS.

a. Pasal 4 UU PDP – Hak Subjek Data Pribadi

Pasal 4 ayat (1) menyatakan bahwa subjek data pribadi memiliki hak:

1. hak memperoleh informasi mengenai kejelasan identitas pengendali data, dasar kepentingan, serta tujuan permintaan data pribadi;
2. hak untuk melengkapi, memperbarui, dan/atau memperbaiki kesalahan data pribadi.
3. hak memperoleh akses dan salinan data pribadi;
4. hak untuk menghentikan pengolahan data;
5. hak untuk menarik persetujuan pengolahan data pribadi;
6. hak untuk mengajukan keberatan atas tindakan pengolahan data pribadi;
7. hak untuk menolak keputusan yang semata-mata berdasarkan pemrosesan otomatis;
8. hak untuk menghapus data pribadi;
9. hak untuk mengajukan gugatan dan memperoleh ganti rugi.

Ketentuan ini memberikan landasan bahwa setiap orang berhak mengendalikan data pribadinya. Dalam kasus pencurian data melalui SMS, pelaku memperoleh data dengan cara manipulatif (*phishing*), sehingga subjek data tidak dapat menggunakan hak-haknya sebagaimana diatur dalam Pasal 4. Pengambilan data tanpa pemberitahuan yang benar dan tanpa persetujuan jelas merupakan pelanggaran langsung terhadap hak subjek data pribadi.

b. Pasal 35 UU PDP – Kewajiban Pengendali Data Pribadi.

Pasal 35 menetapkan bahwa pengendali data wajib:

1. mengamankan data pribadi dari kehilangan, penyalahgunaan, gangguan, dan akses tanpa izin;

[16] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

2. menerapkan langkah teknis dan administratif untuk melindungi data pribadi;
3. memastikan pengolahan data dilakukan sesuai tujuan awal pengumpulan data.

Pasal ini relevan ketika pencurian data terjadi melalui gangguan keamanan sistem SMS atau penyerangan terhadap SMS *Gateway*. Jika operator, penyedia layanan, atau entitas pengendali data tidak menerapkan keamanan yang memadai, maka dapat terjadi kebocoran data. Dalam konteks ini, kegagalan melindungi data pribadi konsumen yang berinteraksi melalui SMS dapat dinilai sebagai pelanggaran kewajiban perlindungan data sesuai Pasal 35.

c. Pasal 65 UU PDP – Larangan Mengumpulkan Data Pribadi Tanpa Hak

- Pasal 65 ayat (1): *"Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain."*
- Pasal 65 ayat (2) menetapkan hukuman pidana penjara dan/atau denda bagi pelanggar.

Modus pencurian data melalui SMS seperti pengiriman tautan palsu, permintaan OTP, dan penipuan identitas termasuk tindakan memperoleh data pribadi tanpa dasar hak. Pelaku jelas bertujuan memperoleh keuntungan, sehingga seluruh unsur Pasal 65 terpenuhi. Pasal ini merupakan ketentuan paling langsung dan eksplisit dalam menjerat pelaku pencurian data pribadi melalui SMS.

d. Pasal 67 UU PDP – Larangan Penyebarluasan Data Pribadi Tanpa Hak

"*Setiap orang yang menyebarluaskan data pribadi tanpa hak atau melawan hukum dipidana dengan pidana penjara atau denda*."

Data pribadi hasil pencurian umumnya diperjualbelikan kepada pihak ketiga atau digunakan untuk penipuan berulang. Penyebarluasan informasi seperti nomor telepon, NIK, alamat, atau OTP merupakan pelanggaran Pasal 67. Ketentuan ini sangat relevan bagi pelaku yang tidak hanya mengumpulkan, tetapi juga memperdagangkan data pribadi hasil curian.

3. Undang-Undang Nomor 11 Tahun 2008 tentang ITE beserta perubahan terakhir melalui UU No. 1 Tahun 2024

Undang-Undang ITE beserta perubahan terakhirnya merupakan instrumen hukum yang mengatur pemanfaatan teknologi informasi, termasuk pengelolaan data pribadi dalam sistem elektronik[17]. Regulasi ini memberikan norma jelas mengenai kewajiban memperoleh persetujuan subjek data, larangan mengakses sistem elektronik tanpa hak, serta penjatuhan sanksi pidana bagi

[17] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

pihak yang menyalahgunakan data pribadi. Relevansinya terhadap pencurian data pribadi melalui SMS sangat kuat sebab modus tersebut umumnya melibatkan akses tidak sah, pengumpulan data tanpa izin, serta penggunaan informasi pribadi untuk tujuan yang merugikan. Analisis terhadap pasal-pasal penting dalam UU ITE diperlukan untuk menegaskan bagaimana ketentuan tersebut dapat digunakan dalam mengkualifikasikan pencurian data melalui SMS sebagai tindak pidana.

a. Pasal 26 UU ITE – Kewajiban Persetujuan Pemilik Data Pribadi

Pasal 26 ayat (1): *"Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan."*

Data pribadi korban yang diberikan karena tertipu oleh SMS phishing bukanlah bentuk persetujuan yang sah. Persetujuan harus diberikan secara bebas, eksplisit, dan atas dasar informasi yang benar. Karena pelaku menggunakan tipuan dan manipulasi, maka setiap pemanfaatan data pribadi korban secara otomatis melanggar Pasal 26.

b. Pasal 30 UU ITE – Larangan Akses Tanpa Hak

- Pasal 30 ayat (1): *"Setiap orang dilarang mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun."*
- Pasal 30 ayat (2): melarang kegiatan memintas, menerobos, atau melampaui sistem keamanan.
- Pasal 30 ayat (3): melarang memperoleh data elektronik dengan cara melawan hukum.

Pelaku yang meminta kode OTP, mengarahkan korban login ke situs palsu, atau meretas SMS Gateway termasuk dalam kategori "akses tanpa hak". Ketika pelaku menggunakan data pribadi korban untuk mengakses akun keuangan atau akun digital lainnya, unsur Pasal 30 terpenuhi. Ketentuan ini menjadi landasan pidana yang kuat untuk menjerat pelaku pencurian data pribadi berbasis SMS.

c. Pasal 45 UU ITE – Ancaman Pidana atas Penyalahgunaan Data Pribadi.

Pasal 45 mengatur sanksi penjara dan/atau denda atas perbuatan:

- mengakses sistem elektronik tanpa hak,
- memanipulasi, mengubah, menghapus, atau mendistribusikan data elektronik secara melawan hukum.

Setelah data dicuri melalui SMS, pelaku umumnya menggunakannya untuk transaksi ilegal, pembobolan rekening, atau menjual data. Seluruh bentuk pemanfaatan data pribadi hasil curian termasuk perbuatan yang secara tegas dilarang oleh Pasal 45. Pasal ini mengatur sanksi atas tahapan "setelah pencurian", yakni penggunaan data untuk merugikan korban.

4. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Perlindungan Konsumen memberikan dasar normatif bagi masyarakat untuk memperoleh informasi yang benar, jelas, dan tidak menyesatkan dari pelaku usaha.[18] Ketentuan dalam undang-undang ini menjadi relevan ketika pencurian data pribadi dilakukan melalui SMS yang menggunakan tipu daya, penyamaran identitas, atau klaim palsu atas nama perusahaan tertentu. Modus tersebut tidak hanya merugikan konsumen secara materiil, tetapi juga melanggar prinsip transparansi dan kejujuran yang diwajibkan oleh undang-undang. Oleh sebab itu, analisis terhadap pasal-pasal kunci dalam UU Perlindungan Konsumen diperlukan untuk menunjukkan bagaimana regulasi ini dapat memberikan perlindungan tambahan bagi korban pencurian data pribadi melalui SMS.

a. Pasal 9 ayat (1) – Larangan Informasi Menyesatkan

"*Pelaku usaha dilarang menawarkan, mempromosikan suatu barang atau jasa secara tidak benar, dan/atau menyesatkan konsumen."*

Dalam banyak kasus penipuan melalui SMS, pelaku menggunakan identitas palsu, seperti mengatasnamakan bank, marketplace, atau lembaga pemerintah. Meskipun pelaku bukan pelaku usaha yang sah, norma Pasal 9 tetap digunakan sebagai dasar untuk menunjukkan bahwa tindakan pelaku telah memenuhi unsur "informasi menyesatkan". Ketentuan ini memperjelas bahwa pelaku merugikan konsumen melalui penyalahgunaan identitas lembaga resmi.

B. Bentuk Tindak Pencurian Data Pribadi melalui SMS yang Dapat Dikualifikasikan sebagai Tindak Pidana

Modus pencurian data pribadi melalui SMS dibagi menjadi beberapa pola utama, yakni (1) pengiriman tautan phishing, (2) penyalahgunaan identitas lembaga, (3) permintaan data pribadi secara langsung oleh pelaku, (4) penipuan hadiah atau promo palsu, serta (5) akses ilegal ke sistem penyedia layanan. Modus-modus tersebut bertujuan untuk memperoleh informasi penting seperti nama lengkap, NIK, nomor rekening, PIN, OTP, atau data personal lain yang dapat digunakan untuk tindak pidana lanjutan. Dalam sebagian kasus, pelaku juga menjual data pribadi yang berhasil dicuri kepada pihak lain. Hasil penelitian menunjukkan bahwa terdapat berbagai bentuk pencurian data pribadi melalui SMS yang memenuhi unsur-unsur tindak pidana, yaitu;

1. Phishing melalui tautan palsu

Pelaku mengirim tautan situs palsu untuk mencuri PIN, OTP, password, atau identitas penting lainnya. Perbuatan ini memenuhi unsur kesengajaan dan akses ilegal sesuai Pasal 30 UU ITE serta Pasal 65 UU PDP.

[18] Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

- Pasal 30 ayat (1) – (3) UU ITE[19]

Ayat (1) *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun."*

Ayat (2) *"Setiap orang dengan sengaja dan tanpa hak memperoleh Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain."*

Ayat (3) *"Setiap orang dengan sengaja dan tanpa hak menerobos, melampaui, atau menjebol sistem keamanan."*

Phishing melalui tautan palsu memenuhi seluruh unsur Pasal 30 karena pelaku secara sengaja mengarahkan korban pada situs palsu untuk memperoleh data elektronik seperti OTP, PIN, atau password. Perbuatan ini dilakukan tanpa hak dan bertujuan mengambil informasi elektronik milik korban. Rekayasa teknis dan sosial yang dilakukan pelaku menunjukkan adanya tindakan menerobos sistem keamanan melalui manipulasi akses, sehingga Pasal 30 cocok diterapkan pada modus phishing ini.

- Pasal 65 ayat (1) UU PDP

"Setiap orang yang dengan sengaja dan melawan hukum mengumpulkan Data Pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain dipidana dengan pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5.000.000.000,00."

Phishing jelas merupakan tindakan mengumpulkan data pribadi tanpa hak, dan unsur kesengajaan terpenuhi karena pelaku membuat tautan palsu dengan tujuan spesifik memperoleh keuntungan. Data yang dikumpulkan berupa OTP, PIN, atau identitas korban, yang termasuk kategori data pribadi menurut UU PDP. Oleh karena itu, Pasal 65 dapat diterapkan secara langsung sebagai dasar pemidanaan.

2. Penyalahgunaan identitas lembaga atau perusahaan

Pelaku mengaku sebagai bank atau perusahaan tertentu untuk mengelabui korban. Modus ini merupakan pelanggaran terhadap Pasal 9 UU Perlindungan Konsumen dan Pasal 26 UU ITE.

- Pasal 9 ayat (1) UU Perlindungan Konsumen

"Pelaku usaha dilarang menawarkan, mempromosikan, mengiklankan suatu barang dan/atau jasa secara tidak benar, dan/atau menyesatkan."

Dalam modus ini, pelaku mengaku sebagai bank, perusahaan layanan digital, atau instansi pemerintah untuk menipu korban. Tindakan tersebut memenuhi unsur "informasi tidak benar dan

[19] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, Pasal 30 ayat (1)–(3)

menyesatkan" sebagaimana dimaksud dalam Pasal 9, karena menggunakan nama pihak lain untuk memperoleh data pribadi. Ketentuan ini memberi dasar bahwa penyamaran identitas lembaga merupakan bentuk penyesatan konsumen yang dapat dikualifikasikan sebagai perbuatan melawan hukum.

- Pasal 26 ayat (1) UU ITE

"Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan."

Pada modus ini, pelaku menggunakan identitas lembaga atau perusahaan untuk meminta data pribadi korban tanpa persetujuan sah. Walaupun korban menyerahkan data karena tertipu, persetujuan tersebut tidak dianggap sah menurut Pasal 26 karena diperoleh melalui pemalsuan identitas. Oleh sebab itu, tindakan pelaku merupakan pelanggaran langsung terhadap prinsip persetujuan yang menjadi dasar perlindungan data pribadi.

3. Penggunaan data pribadi untuk kejahatan lanjutan

Data yang dicuri digunakan untuk transaksi ilegal, penipuan, atau mengakses layanan finansial korban. Tindakan ini dapat dikualifikasikan sebagai pencurian dalam Pasal 362 KUHP dan pelanggaran UU PDP.

- Pasal 362 KUHP dan Pasal 65 UU PDP

"Barang siapa mengambil sesuatu benda yang seluruhnya atau sebagian adalah milik orang lain, dengan maksud untuk menguasai benda itu secara melawan hukum, dipidana karena pencurian."

Penggunaan data pribadi yang dicuri untuk melakukan transaksi, mengambil uang, atau mengakses layanan finansial korban memenuhi unsur "mengambil barang milik orang lain untuk menguasai secara melawan hukum". Dalam konteks digital, data pribadi dipandang sebagai benda tidak berwujud yang memiliki nilai ekonomis. Ketika data tersebut digunakan untuk merugikan korban, unsur tindak pidana pencurian terpenuhi sehingga Pasal 362 dapat diterapkan. Setiap penggunaan data korban untuk kejahatan lanjutan adalah lanjutan dari pengumpulan data tanpa hak. Data tersebut digunakan untuk motif keuntungan, sehingga unsur Pasal 65 terpenuhi sepenuhnya. Tindakan ini menunjukkan perluasan tindak pidana dari tahap pengumpulan hingga eksploitasi data.

4. Penjualan atau distribusi data pribadi

Data yang berhasil dicuri dijual kepada pihak lain melalui kanal ilegal. Tindakan ini termasuk pelanggaran berat menurut Pasal 67 UU PDP.

- Pasal 67 UU PDP

"Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp4.000.000.000,00."

Penjualan data pribadi hasil pencurian merupakan bentuk nyata dari "mengungkapkan data pribadi" kepada pihak lain. Pelaku tidak hanya mengambil data dari korban tetapi juga menyebarkannya dengan tujuan keuntungan ekonomi. Oleh karena itu, unsur perbuatan melawan hukum dan kesengajaan dalam Pasal 67 terpenuhi, sehingga penjualan data pribadi termasuk tindak pidana berat dalam kerangka UU PDP.

5. Akses ilegal ke sistem SMS Gateway

Pelaku melakukan peretasan untuk mengambil database pengguna. Tindakan ini merupakan pelanggaran Pasal 30 UU ITE. Peretasan SMS Gateway atau sistem penyedia layanan merupakan tindakan yang secara jelas memenuhi unsur akses ilegal, memperoleh informasi, serta menerobos sistem keamanan. Modus ini merupakan bentuk *cyber intrusion* karena pelaku menembus sistem yang dilindungi. Tindakan tersebut menunjukkan pelanggaran substansial terhadap Pasal 30.

- Pasal 45 UU ITE

"Setiap orang yang melanggar ketentuan Pasal 30 dipidana dengan pidana penjara dan/atau denda sesuai ketentuan tingkat pelanggaran."

Pasal 45 menjadi dasar pemberian sanksi terhadap pelaku akses ilegal. Ketika pelaku meretas sistem untuk memperoleh data pribadi, tindakan tersebut memenuhi unsur pelanggaran Pasal 30 sehingga Pasal 45 wajib diterapkan. Kombinasi kedua pasal ini menegaskan bahwa pencurian data melalui peretasan bukan hanya pelanggaran administratif, tetapi merupakan tindak pidana dengan konsekuensi pidana yang jelas.

Seluruh bentuk pencurian data pribadi melalui SMS yang ditemukan dalam penelitian ini dapat dikualifikasikan sebagai tindak pidana karena memenuhi unsur-unsur yang diatur dalam KUHP, Undang-Undang Informasi dan Transaksi Elektronik (ITE), serta Undang-Undang Perlindungan Data Pribadi (PDP). Setiap modus operasi pelaku mengandung unsur kesengajaan, perbuatan melawan hukum, dan pemanfaatan data pribadi tanpa hak. Selain itu, pelaku secara aktif menggunakan sarana elektronik seperti tautan palsu, pesan singkat, maupun penyamaran identitas untuk memperoleh, menguasai, atau mendistribusikan data pribadi korban. Unsur-unsur ini menjadikan perbuatan tersebut bukan hanya pelanggaran etis, tetapi juga masuk kategori tindak pidana sebagaimana diatur dalam peraturan perundang-undangan.

Berdasarkan bentuk-bentuk tindak pidana dalam pencurian data melalui SMS. Dapat di

uraikan analisis unsur tindak pidana pada berbagai bentuk pencurian data pribadi melalui SMS. Analisis ini diuraikan untuk memperjelas pemenuhan unsur tindak pidana terhadap berbagai bentuk pencurian data pribadi melalui SMS.

a) Unsur Kesengajaan

Menurut M. Utoyo dan K. Afriani, kesengajaan dalam hukum pidana Indonesia dipahami sebagai "menghendaki" dan "mengetahui". Artinya, seseorang yang melakukan perbuatan dengan sengaja harus menghendaki perbuatannya dan memahami akibat dari perbuatan tersebut. Unsur ini menunjukkan adanya sikap batin atau mens rea pada diri pelaku ketika melakukan tindakan yang masuk dalam rumusan delik.[20] Pelaku yang mengirim SMS *phising* secara aktif memilih untuk:

1. Membuat tautan palsu,
2. Mengirimkan kepada korban, dan
3. Mengharapkan korban mengisi data pribadi.

Dengan demikian, unsur kesengajaan terpenuhi karena pelaku menghendaki akibat berupa diperolehnya data korban. Hal tersebut sesuai dengan ketentuan pada pasal 30 ayat 1, 2 dan 3 UU ITE. Pelaku dengan sengaja memgarahkan korban pada situs palsu agar dapat mengakses data elektronik korban. Prilaku ini merupakan tindak pidana akses ilegal dimana pelaku melakukan tindakan menerobos sistem keamanan data dengan memanipulasi akses data melalui modus *phising*.

b) Unsur Perbuatan Melawan Hukum

Menurut Indah Sari, konsep *perbuatan melawan hukum* dalam hukum pidana adalah perbuatan melawan hukum merujuk pada tindakan yang bertentangan dengan ketentuan yang secara tegas dilarang dalam KUHP. Perbuatan tersebut mencakup tindakan yang melanggar undang-undang, tindakan yang dilakukan di luar batas kewenangan yang dimiliki pelaku, serta tindakan yang bertentangan dengan asas-asas umum dalam hukum pidana.[21] Pada modus phishing melalui SMS, pelaku secara jelas memenuhi unsur perbuatan melawan hukum karena tindakannya bertentangan dengan peraturan perundang-undangan. Pelaku secara aktif membangun mekanisme untuk memperoleh data pribadi korban melalui cara yang dilarang. Pelaku merekayasa situs palsu untuk mengumpulkan data pribadi korban.

1. Pelaku mengumpulkan data pribadi yang bukan miliknya,
2. Pengumpulan dilakukan melalui manipulasi atau tipu daya, dan

[20] M. Utoyo, K. Afriani, R. Rusmini, dan H. Husnaini, "Sengaja dan Tidak Sengaja dalam Hukum Pidana Indonesia," *Lex Librum* 7, no. 1 (2020): 75–85.
[21] Indah Sari, "Perbuatan Melawan Hukum (PMH) dalam Hukum Pidana dan Hukum Perdata," *Jurnal Ilmiah Hukum Dirgantara* 11, no. 1 (2020).

3. Tindakan tersebut menimbulkan kerugian serta risiko penyalahgunaan data bagi korban

Ketiga tindakan tersebut memenuhi unsur perbuatan melawan hukum sebagaimana dimaksud dalam Pasal 65 ayat (1) UU Perlindungan Data Pribadi (UU PDP), yang menyatakan bahwa setiap orang yang dengan sengaja dan melawan hukum mengumpulkan data pribadi tanpa hak dapat dipidana.[22] Unsur melawan hukum semakin jelas karena pengumpulan data dilakukan bukan hanya tanpa izin, tetapi juga melalui teknik penipuan yang bertentangan dengan kewajiban perlindungan data pribadi. Dengan demikian, unsur perbuatan melawan hukum terpenuhi secara nyata pada kasus *phishing* melalui SMS, sebab pelaku bertindak tanpa dasar kewenangan dan merampas hak eksklusif korban atas data pribadinya.

c) Unsur Penyesatan Konsumen dan Pelanggaran Hak Privasi

Menurut Widiarty dan Saragih, tindakan yang menyesatkan konsumen terjadi ketika pelaku memberikan informasi yang tidak benar, memalsukan identitas, atau menyembunyikan hal-hal penting sehingga konsumen mengambil keputusan yang merugikan dirinya. Unsur ini muncul ketika pelaku secara sadar menggunakan nama, logo, atau ciri lembaga tertentu untuk menciptakan kesan bahwa pesan tersebut berasal dari pihak resmi. Dengan demikian, korban percaya dan menyerahkan data pribadinya.[23]

Pada kasus penyalahgunaan identitas lembaga melalui SMS, pelaku biasanya menyamar sebagai bank, marketplace, atau perusahaan layanan digital. Modus ini memenuhi unsur penyesatan karena pelaku mengarahkan korban pada informasi palsu, seolah-olah berasal dari institusi yang sah. Unsur pelanggaran hak privasi juga terpenuhi karena pelaku meminta atau mengambil data pribadi tanpa persetujuan sebagaimana dipersyaratkan Pasal 26 UU ITE. Tindakan ini melanggar Pasal 9 ayat (1) UU Perlindungan Konsumen, yang melarang pelaku usaha memberikan informasi menyesatkan. Pasal 26 UU ITE juga dilanggar karena pelaku mengambil dan memanfaatkan data pribadi tanpa persetujuan yang sah. Dengan demikian, unsur penyesatan dan pelanggaran privasi lengkap terpenuhi.

d) Unsur Kepemilikan dan Niat Menguasai

Penggunaan data pribadi korban untuk transaksi ilegal menunjukkan terpenuhinya unsur kepemilikan data milik orang lain serta adanya niat pelaku untuk menguasai dan memperoleh keuntungan. Menurut Moeljatno, unsur niat atau *opzet* dalam tindak pidana mencakup kehendak

[22] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 65 ayat (1).
[23] W. S. Widiarty dan R. V. Saragih, *Hukum Perlindungan Konsumen di Era Globalisasi* (2024).

pelaku untuk mewujudkan akibat tertentu melalui perbuatannya.[24] Pada bentuk pelanggaran ini, pelaku menggunakan data pribadi seperti nomor rekening, OTP, atau informasi finansial korban sebagai sarana melakukan transaksi. Tindakan tersebut pada dasarnya merupakan bentuk penguasaan atas "harta" milik orang lain.

Unsur ini sejalan dengan ketentuan Pasal 362 KUHP, yang menyatakan bahwa pencurian adalah "mengambil sesuatu barang yang seluruhnya atau sebagian milik orang lain dengan maksud untuk dimiliki secara melawan hukum." Pasal 67 UU Perlindungan Data Pribadi menegaskan larangan penggunaan data pribadi tanpa hak, yang diancam pidana ketika perbuatan tersebut dilakukan untuk memperoleh manfaat atau menyebabkan kerugian.

e) Unsur penyebarluasan data pribadi

Menurut Pranindya, penyebarluasan data pribadi tanpa dasar hukum yang sah merupakan pelanggaran serius terhadap hak privasi karena data pribadi pada dasarnya hanya boleh diproses dan dibagikan atas persetujuan pemiliknya. Penyebarluasan tanpa izin dipahami sebagai tindakan memindahkan, membagikan, atau mengungkapkan data pribadi kepada pihak lain tanpa dasar hukum maupun persetujuan subjek data, sehingga bertentangan dengan prinsip dasar perlindungan data pribadi.[25] Dalam konteks penjualan data, pelaku secara sadar memindahkan data korban kepada pihak ketiga dengan tujuan memperoleh keuntungan. Tindakan ini memenuhi unsur *melawan hukum*, karena pelaku tidak memiliki hak apa pun atas data tersebut dan tetap menyebarkannya kepada pihak lain.

SIMPULAN

Pencurian data pribadi melalui Short Message Service (SMS) merupakan bentuk kejahatan digital yang memenuhi unsur-unsur tindak pidana sebagaimana diatur dalam UU ITE, UU Perlindungan Data Pribadi (UU PDP), UU Perlindungan Konsumen, serta ketentuan relevan dalam KUHP. Berbagai modus seperti phishing, penyalahgunaan identitas lembaga, penggunaan data untuk transaksi ilegal, dan penjualan data pribadi kepada pihak ketiga seluruhnya menunjukkan adanya unsur kesengajaan, akses tanpa hak, perbuatan melawan hukum, serta penyebarluasan data tanpa izin. Analisis terhadap setiap ketentuan hukum menunjukkan bahwa kerangka regulasi yang ada sebenarnya telah memadai untuk menjerat pelaku, namun implementasi dan penegakan hukum masih

[24] Moeljatno, *Asas-asas Hukum Pidana* (Jakarta: Rineka Cipta, 2008).
[25] K. R. A. Pranindya, "Penegakan Hukum terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Melalui Barcode Ditinjau dari UU ITE dan UU Nomor 27 Tahun 2022 tentang (UU PDP)," *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi* 2, no. 3 (2025): 123–135

menghadapi tantangan pada aspek pembuktian elektronik dan identifikasi pelaku. Oleh karena itu, penguatan regulasi teknis, peningkatan literasi digital masyarakat, dan optimalisasi penegakan hukum diperlukan untuk memastikan perlindungan yang efektif terhadap data pribadi di era digital

DAFTAR PUSTAKA

Indrajit, Richardus Eko. "Fenomena Kebocoran Data: Mencari Sumber Penyebab dan Akar Permasalahannya." Diakses 18 Mei 2024. http://folder.idsirtii.or.id/pdf/IDSIRTII-Artikel309 FenomenaKebicoranData.pdf.

Kominfo RI. "Waspada Kejahatan Siber dan Kebocoran Data Pribadi di Era Digital." Diakses 18 Mei 2024. https://aptika.kominfo.go.id/

Kurnia, Mahendra Putri, dan Syarfani. "Tinjauan Yuridis terhadap Perlindungan Data Pribadi di Media Elektronik (Berdasarkan Pasal 25 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik)." *Jurnal Beraja Niti* 3 (2014).

Marzuki, Peter Mahmud. *Penelitian Hukum.* Jakarta: Kencana Prenada Media Group, 2017.

Moeljatno. *Asas-asas Hukum Pidana*. Jakarta: Rineka Cipta, 2008.

Muchsin. *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia.* Disertasi S2, Fakultas Hukum, Universitas Sebelas Maret, Surakarta, 2003.

Nabila, Farid. *Perlindungan Hukum terhadap Korban Penipuan melalui SMS (Short Message Service).* Skripsi. Jember: Fakultas Syariah, Universitas Islam Negeri Kiai Haji Achmad Siddiq, 2023.

Nugroho S., Christian Adhi, Samsudi, dan Dwi Endah Nurhayati. *Kebijakan Hukum Pidana terhadap Pembuatan Penyebaran Spam melalui Short Message Service (SMS).* Artikel Ilmiah Hasil Penelitian Mahasiswa. Jember: Fakultas Hukum, Universitas Jember, 2023.

Pranindya, K. R. A. "Penegakan Hukum terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Melalui Barcode Ditinjau dari UU ITE dan UU Nomor 27 Tahun 2022 tentang (UU PDP)." *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi* 2, no. 3 (2025): 123–135.

Rahardjo, Satjipto. *Ilmu Hukum.* Bandung: PT Citra Aditya Bakti, 2000.

Republik Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.* Lembaran Negara Republik Indonesia Tahun 2024 Nomor 12.

Republik Indonesia. *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.* Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Republik Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.* Lembaran Negara Republik Indonesia Tahun 2022 Nomor 237.

Republik Indonesia. *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.* Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42.

Sari, Indah. "Perbuatan Melawan Hukum (PMH) dalam Hukum Pidana dan Hukum Perdata." *Jurnal Ilmiah Hukum Dirgantara* 11, no. 1 (2020).

Satriana, I Made Wahyu Chandra, dan Ni Made Liana Dewi. "Penyuluhan Hukum tentang Spamming SMS yang Mengandung Unsur Perjudian di Kalangan Generasi Muda." *Journal of Human Education* 3, no. 4 (2023): 62–66.

Setiono. "Rule of Law." Disertasi S2, Fakultas Hukum, Universitas Sebelas Maret, Surakarta, 2004.

Utoyo, M., K. Afriani, R. Rusmini, dan H. Husnaini. "Sengaja dan Tidak Sengaja dalam Hukum Pidana Indonesia." *Lex Librum* 7, no. 1 (2020): 75–85.

Widiarty, W. S., dan R. V. Saragih. *Hukum Perlindungan Konsumen di Era Globalisasi.* 2024.