Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

# ANALISIS SANKSI PIDANA TERHADAP KEBOCORAN DATA YANG TERJADI PADA DATA NASABAH APLIKASI PERBANKAN DIGITAL DI INDONESIA

**Najwa Putri Gunawan [1], Sidi Ahyar Wiraguna [2]**
[1, 2] Fakultas Ilmu Hukum, Hukum, Universitas Esa Unggul Jakarta

**Abstract (English)**

*Data theft crimes are a crucial issue faced in today's digital era. When personal data falls into the hands of irresponsible people, it can have a detrimental impact on various parties. One case of data theft occurred in a state financial institution, namely Bank Indonesia. This study uses a normative legal method with a library research approach, the data sources of which come from secondary data, including primary, secondary, and tertiary legal materials. Data are analyzed qualitatively and presented descriptively-analystically, while conclusions are drawn through a deductive approach. Based on the results of the study, there are a number of regulations governing data protection in Indonesia. Perpetrators of data theft crimes can be subject to sanctions in the form of imprisonment and fines. However, existing regulations are not yet fully able to provide adequate protection and legal certainty. Therefore, handling cybercrime must be accompanied by the application of strict and severe penalties. The ratification of the Personal Data Protection Bill is very important to ensure public protection, especially in the face of rapidly developing technological and internet advances. The state, through the government, has full responsibility to protect the privacy rights of citizens, including the security of their personal data.*

**Article History**
Submitted: 21 Mei 2025
Accepted: 24 Mei 2025
Published: 25 Mei 2025

**Key Words**
*Personal data, Law, Cybercrime, Protection, Regulation*

**Abstrak (Indonesia)**

Kejahatan pencurian data merupakan persoalan krusial yang dihadapi dalam era digital saat ini. Ketika data pribadi jatuh ke tangan yang tidak bertanggung jawab, hal ini dapat menimbulkan dampak yang merugikan bagi berbagai pihak. Salah satu kasus pencurian data terjadi di institusi keuangan negara, yaitu Bank Indonesia. Penelitian ini menggunakan metode hukum normatif dengan pendekatan studi pustaka (library research), yang sumber datanya berasal dari data sekunder, mencakup bahan hukum primer, sekunder, dan tersier. Data dianalisis secara kualitatif dan disajikan secara deskriptif-analitis, sedangkan penarikan kesimpulan dilakukan melalui pendekatan deduktif. Berdasarkan hasil penelitian, terdapat sejumlah regulasi yang mengatur perlindungan data di Indonesia. Pelaku tindak pidana pencurian data dapat dikenai sanksi berupa pidana penjara dan denda. Namun demikian, peraturan yang ada belum sepenuhnya mampu memberikan perlindungan serta kepastian hukum yang memadai. Oleh karena itu, penanganan terhadap kejahatan siber harus diiringi dengan penerapan hukuman yang tegas dan berat. Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi menjadi sangat penting guna menjamin perlindungan masyarakat, khususnya dalam menghadapi kemajuan teknologi dan internet yang berkembang dengan pesat. Negara, melalui pemerintah, memiliki tanggung jawab penuh untuk melindungi hak privasi warga negara, termasuk keamanan atas data pribadi mereka.

**Sejarah Artikel**
Submitted: 21 Mei 2025
Accepted: 24 Mei 2025
Published: 25 Mei 2025

**Kata Kunci**
Data pribadi, Hukum, Kejahatan siber, Perlindungan, Regulasi

## PENDAHULUAN

Perkembangan teknologi telah memberikan dampak besar dalam mempermudah berbagai aktivitas manusia. Manfaatnya dapat dirasakan dalam kehidupan sehari-hari, salah satunya melalui penggunaan telepon genggam yang memungkinkan komunikasi jarak jauh secara praktis (Sri

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

Mulyati, 202). Kehadiran internet menjadi tonggak penting dalam kemajuan teknologi, karena tidak hanya memudahkan masyarakat Indonesia, tetapi juga memberikan dampak global yang signifikan. Peran teknologi informasi, media, komunikasi dan sistem elektronik sangat bermanfaat bagi perubahan perilaku masyarakat secara global. Sistem elektronik yang dimaksud yaitu perangkat keras, perangkat lunak komputer, jaringan telekomunikasi dan sistem komunikasi elektronik[1]. Seiring waktu, teknologi internet terus mengalami kemajuan pesat yang ditandai dengan munculnya berbagai aplikasi digital yang dirancang untuk menunjang dan mempermudah berbagai kegiatan manusia. Kegagalan dan kesalahan dalam teknologi informasi dan sistem elektronik terkadang berasal dari langkah-langkah keamanan yang tidak memadai yang dirancang untuk melindungi data pribadi pelanggan yang telah mendaftar di platform daring (Shafa Salsabila, 2025). Perangkat lunak komputer, jaringan telekomunikasi, dan sistem komunikasi elektronik[2]. Namun demikian, kemajuan teknologi di sektor perbankan turut membawa dampak negatif berupa munculnya sejumlah permasalahan hukum yang berkaitan dengan tindak pidana di bidang informasi dan transaksi elektronik. Apabila isu-isu tersebut tidak direspons secara tepat dan menyeluruh, maka dapat menimbulkan konsekuensi yang merugikan tidak hanya bagi institusi perbankan, tetapi juga bagi masyarakat luas dan para nasabah sebagai pengguna layanan perbankan. Dalam beberapa tahun terakhir, Indonesia menghadapi berbagai insiden kebocoran data pada layanan digital, termasuk di sektor perbankan (Elda Septi Darmayanti, 2025).

Meskipun demikian, dalam praktiknya insiden kebocoran data nasabah masih kerap terjadi. Hal ini disebabkan oleh dua faktor utama, yaitu meningkatnya kompleksitas serangan siber serta kelalaian internal dari pihak perbankan. Ancaman digital seperti peretasan data (data *breach), phishing*, dan penyebaran *malware* semakin intensif menyerang sistem perbankan dengan memanfaatkan kelemahan dalam sistem keamanan guna memperoleh informasi sensitive, Kasus-kasus seperti dugaan kebocoran data nasabah oleh oknum di internal perusahaan, hingga serangan siber yang menyebabkan data nasabah bocor ke pasar gelap digital (*dark web*), menunjukkan lemahnya perlindungan hukum terhadap data pribadi. Dalam sistem implementasinya, teknologi informasi dan komunikasi berfungsi sebagai pedang bermata dua. Teknologi informasi menawarkan berbagai keuntungan untuk meningkatkan kebahagiaan dan peradaban manusia, serta memajukan layanan publik dan internal dalam industri jasa (Mugiono Mugiono, 2025). Sebaliknya, teknologi informasi dimanfaatkan oleh oknum yang tidak bertanggung jawab untuk melakukan tindakan ilegal yang melanggar kepentingan hukum individu, masyarakat, dan negara[3]. Di samping itu, faktor kelalaian internal seperti kesalahan operasional akibat human error dalam pengelolaan data, ketidakpatuhan terhadap prosedur keamanan, serta potensi penyalahgunaan akses oleh pegawai bank juga menjadi kontributor utama terjadinya kebocoran data. Konsekuensi dari insiden tersebut tidak hanya menimbulkan kerugian secara finansial bagi nasabah, tetapi juga dapat mencoreng citra institusi perbankan, menurunkan tingkat kepercayaan publik, serta menghadirkan ancaman hukum yang serius (Anesya Fritiana, Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online: Analisis Perlindungan dan Sanksi Hukum, 2025).

Kitab Undang-Undang Hukum Pidana (KUHP) secara umum mencantumkan ketentuan terkait tindak pidana yang juga dapat dikaitkan dengan kejahatan siber. Namun, dalam sistem

[1] Bala Tim PY, Undang-Undang Informasi Dan Transaksi Elektronik: Seri Perundangundangan (Yogyakarta: Pustaka Yustisia, 2019), hal 33–34.
[2] Kusuma, A. C., & Rahmani, A. D. (2022). *Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia* (Studi Kasus Kebocoran Data Pada Bank Indonesia). SUPREMASI: Jurnal Hukum, 5(1), 46-63.
[3] Adam Chazawi. *Tindak Pidana Informasi Dan Transaksi Elektronik*. Malang: Media Nusa Crative, 2015.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

hukum Indonesia berlaku asas *lex specialis derogat legi generalis*, yang berarti bahwa ketentuan hukum yang bersifat khusus akan mengesampingkan ketentuan yang bersifat umum apabila keduanya mengatur hal yang sama. Oleh karena itu, Indonesia telah menetapkan sejumlah regulasi khusus yang secara lebih rinci mengatur aspek hukum siber di sektor perbankan, antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 10 Tahun 1998 sebagai perubahan dari Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP) (Faisal Santiago, 2023). Adanya perlindungan hukum bagi nasabah memberikan rasa aman kepada nasabah terkait dengan eksploitasi data pribadinya[4]

## METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif, yang berfokus pada studi kepustakaan *(library research*) (Ahyar Sidi, 2025). Penelitian ini dilakukan dengan mengkaji buku-buku dan literatur terkait yang diperoleh dari perpustakaan dan relevan dengan topik yang dibahas. Dalam pendekatan normatif ini, pendekatan yang diterapkan adalah pendekatan perundang-undangan, atau yang dikenal dengan *statute approach*. Data yang digunakan dalam penelitian ini merupakan data sekunder, yang terdiri dari bahan hukum primer, seperti peraturan perundang-undangan yang berkaitan dengan kebocoran data, serta bahan hukum sekunder berupa buku dan jurnal yang mendalami tema penelitian ini.

## HASIL DAN PEMBAHASAN

### Tindakan Hukum Terhadap Kejahatan Peretasan Data di Indonesia

Seiring dengan perubahan zaman dan pola perilaku masyarakat, kejahatan siber mengalami peningkatan signifikan, didorong oleh berbagai motif di balik aksi kriminal di ruang digital. Setiap informasi digital seperti teks, gambar, video, maupun rekaman suara yang telah beredar di internet umumnya sulit untuk dihapus secara permanen. Oleh karena itu, apabila data pribadi seseorang tidak memperoleh perlindungan yang memadai, risiko terjadinya kebocoran data menjadi sangat tinggi dan berpotensi mengancam keselamatan individu. Kondisi ini menegaskan pentingnya penerapan sistem perlindungan yang ketat terhadap data digital yang telah diunggah, guna mencegah penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab (Anesya Fritiana, Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online: Analisis Perlindungan dan Sanksi Hukum, 2025). Banyaknya kasus peretasan data di Indonesia mengakibatkan peningkatan rasa kekhawatiran masyarakat untuk melakukan transaksi melalui media online ataupun lebih mempertimbangkan dalam pengunggahan data pribadi yang dibutuhkan oleh pihak yang bersangkutan seperti, pembukaan rekening di bank ataupun melakukan verifikasi terhadap aplikasi yang membutuhkan pengunggahan data pribadi[5]. Dalam ranah hukum perdata, tanggung jawab hukum dapat timbul apabila terbukti bahwa kelalaian menjadi faktor utama terjadinya kerugian yang dialami oleh nasabah. Konsep ini berkaitan erat dengan tanggung jawab kontraktual, di mana hubungan hukum antara pihak bank dan nasabah didasarkan pada suatu perjanjian. Melalui

[4] Triputri, D. H., Mofea, S., Yulviani, D., & Pratama, R. (2023). Analisis Yuridis Terhadap Penerapan Sanksi Pidana Bagi Pelaku Penipuan Dalam Transaksi Elektronik Berdasarkan Asas Lex Specialis Derogat Legi Generali Ditinjau Dari Kuhp Dan UU ITE.Lex Veritatis,2(01), 42-51.

[5] D F T Popal, "*Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime*)," Lex Administratum, no. 5 (2023),https://ejournal.unsrat.ac.id/index.php/administratum/article/view/51005%0Ahttps://ejournal.unsrat.ac.id/i ndex.php/administratum/article/download/51005/43956.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

perjanjian tersebut, bank memiliki kewajiban untuk menyediakan layanan keuangan yang aman, termasuk menjamin perlindungan terhadap data pribadi nasabah. Jika bank gagal menjalankan kewajiban tersebut sehingga menyebabkan kerugian, maka bank dapat dimintai pertanggungjawaban dalam bentuk kompensasi atau ganti rugi. Dalam prinsip hukum perdata, tanggung jawab hukum dapat timbul apabila terbukti bahwa kelalaian menjadi faktor utama terjadinya kerugian yang dialami oleh nasabah. Konsep ini berkaitan erat dengan tanggung jawab kontraktual, di mana hubungan hukum antara pihak bank dan nasabah didasarkan pada suatu perjanjian. Melalui perjanjian tersebut, bank memiliki kewajiban untuk menyediakan layanan keuangan yang aman, termasuk menjamin perlindungan terhadap data pribadi nasabah. Jika bank gagal menjalankan kewajiban tersebut sehingga menyebabkan kerugian, maka bank dapat dimintai pertanggungjawaban dalam bentuk kompensasi atau ganti rugi.

Insiden kebocoran data pada sektor perbankan menjadi salah satu sasaran utama serangan oleh peretas, di mana informasi yang telah berhasil diakses secara ilegal sering kali disalahgunakan, baik untuk diperjualbelikan kepada pihak lain maupun dimanfaatkan demi keuntungan pribadi pelaku. Aksi pencurian data ini telah berkembang menjadi isu krusial di era digital, karena dapat menimbulkan dampak negatif yang signifikan dan menambah kekhawatiran terhadap potensi penyalahgunaan informasi pribadi. Dalam menjalankan aksinya, para pelaku kejahatan siber biasanya memanfaatkan teknologi telematika yang canggih, menjadikan aktivitas mereka sulit terdeteksi dan dapat dilakukan secara lintas lokasi dan waktu. Teknik serta modus operandi yang digunakan semakin beragam dan kompleks, menciptakan tantangan besar dalam mewujudkan keamanan yang sepenuhnya terjamin di dunia maya. Penerapan hukuman pidana yang efektif tidak hanya dimaksudkan sebagai bentuk penghukuman terhadap pelaku kejahatan, tetapi juga berperan sebagai instrumen preventif untuk menekan angka kejahatan siber serta melindungi masyarakat di ruang digital. Dalam konteks keamanan dunia maya, pemberlakuan sanksi pidana tidak semata-mata bersifat reaktif terhadap tindakan kriminal yang telah terjadi, melainkan juga merupakan bagian dari strategi preventif yang bertujuan untuk mengurangi risiko terjadinya tindak kejahatan serupa di masa yang akan datang. Dalam menciptakan lingkungan hukum yang memadai untuk melindungi informasi yang *sensitive*, menjaga stabilitas infrastruktur digital, dan mencegah dampak yang dirugikan akibat kejahatan siber, maka dalam melakukan penerapan sanksi pidana harus dilakukan secara efektif dan melakukan pembaharuan peraturan perundang-undang khusunya tindak pidana *cyber*, sehingga dengan munculnya modus baru dalam melakukannya dapat teratasi dan tidak menjadi pasal karet, agar memiliki kekuatan hukum yang tetap[6]. Dalam melakukan bentuk penindakan kejahatan peretas data di Indonesia sendiri sering mengalami hambatan dalam melakukan penegakan hukum pidana, faktor yang menjadi penghambat dalam penanggulangan tindak pidana siber sendiri tidak terlepas dari faktor internal dan faktor eksternal, selebihnya akan dijelaskan sedikit mengenai faktor yang menjadi penghambat yaitu:

1. **Faktor Internal**
   Penegakan hukum terhadap kejahatan siber sangat erat kaitannya dengan mutu sumber daya aparat penegak hukum serta keberadaan regulasi yang berlaku. Aparat yang dimaksud mencakup institusi seperti hakim, jaksa, dan kepolisian, yang bekerja berdasarkan ketentuan perundang-undangan yang berlaku. Meskipun secara formal Indonesia telah

[6] Duarif Duarif and Moh Saleh, "*Pencegahan Dan Penindakan Tindak Pidana Siber Oleh Kepolisian Resort Teluk Bintuni*," UNES Law Review 6, no. 4 (2024): 12110–19.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

memiliki kerangka hukum yang relatif memadai, keberhasilan implementasinya tetap sangat ditentukan oleh profesionalisme dan integritas aparat penegak hukum itu sendiri. Jika aparat hukum tidak profesional, korup, atau kurang memiliki pemahaman mengenai teknologi digital, maka penanganan kasus kejahatan siber menjadi tidak optimal. Sebaliknya, apabila aturan hukum tidak diperbarui mengikuti perkembangan teknologi informasi, maka akan timbul celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan siber[7].

2. **Faktor Eksternal**
   a. **Faktor dari masyarakat :** Masyarakat memiliki posisi strategis sebagai elemen utama dalam upaya pencegahan dan identifikasi dini terhadap tindak kejahatan digital. Namun demikian, masih rendahnya tingkat literasi digital di kalangan masyarakat Indonesia menciptakan celah yang cukup besar antara eksistensi potensi ancaman siber dan kemampuan masyarakat dalam mengenali serta meresponsnya. Minimnya pengetahuan terkait bentuk-bentuk *cybercrime* menyebabkan banyak kasus yang tidak diketahui atau tidak dilaporkan oleh korban. Dalam konteks ini, masyarakat tidak hanya berperan sebagai penerima perlindungan hukum, melainkan juga sebagai pelaku aktif dalam proses pengawasan serta pelaporan terhadap aktivitas siber yang mencurigakan.
   b. **Faktor Budaya:** Dalam konteks budaya hukum yang berdampak pada penegakan hukum, khususnya terkait efektivitas penindakan hukum terhadap pengguna media sosial, ada beberapa hal penting yang perlu diperhatikan:
      1) Kesadaran akan Peraturan Perundang-undangan: Ketika undang-undang diundangkan, diasumsikan bahwa masyarakat mengetahui aturan hukum yang berlaku. Namun, banyak orang yang masih belum mengetahui tentang undang undang tertentu, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Kesenjangan ini menunjukkan adanya kesenjangan yang signifikan antara keberadaan hukum dan pengetahuan masyarakat tentang hukum tersebut.
      2) Memahami isi dari peraturan, Mengetahui undang-undang saja tidak cukup; masyarakat juga harus memahami isi peraturan, termasuk tujuan dan manfaatnya. Pemahaman yang lebih dalam ini sangat penting untuk kepatuhan dan keterlibatan yang efektif terhadap hukum.
      3) Kepatuhan dan Perilaku, Setelah mendapatkan kesadaran dan pemahaman tentang undang-undang ini, diharapkan individu akan menerjemahkan pemahaman ini ke dalam perilaku yang patuh ketika menggunakan media elektronik. Kepatuhan ini sangat penting untuk mendorong lingkungan digital yang bertanggung jawab dan memastikan bahwa transaksi elektronik mematuhi standar hukum.
   c. **Faktor Sarana dan Fasilitas:** Jika undang-undang sudah baik dan mentalitas penegak hukum juga positif, tetapi fasilitas yang tersedia tidak memadai, maka penegakan hukum tidak akan berjalan dengan efektif.
      Perkembangan teknologi di Indonesia yang semakin cepat dan kemajuan ilmu pengetahuan yang semakin pesat mengakibatkan timbulnya jenis kejahatan *cyber crime* yang semakin bervariasi, tentu masyarakat harus mengikuti perkembangan teknologi

[7] Achmad, Fadillah. (2021). *Hukum dan Teknologi Informasi: Dinamika dan Tantangan di Era Digital*, Jakarta: Kencana, hlm. 112.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

yang kemudian masyarakat juga memperhatikan secara khusus[8]. Bentuk-bentuk dari tindak pidana *cyber crime* sendiri meliputi:

1. Kejahatan *Phising*
2. Serangan *Ransomware*
3. Penipuan Online
4. Peretasan Situs dan Email
5. Kejahatan *Skimming*
6. Kejahatan Konten Ilegal
7. *Cyber Espionage*
8. Pemalsuan Data
9. *Cyber Terorism*
10. *Identity Thef*

**Bagaimana ketentuan hukum pidana di Indonesia dalam mengatur perlindungan data nasabah pada aplikasi perbankan digital?**

Perkembangan teknologi digital telah melahirkan berbagai kemudahan dalam aktivitas manusia, termasuk dalam sektor perbankan. Munculnya aplikasi perbankan digital menjadi solusi efisien bagi masyarakat dalam melakukan transaksi keuangan secara daring. Namun demikian, kemajuan ini turut menghadirkan tantangan serius terhadap perlindungan data pribadi nasabah. Tidak sedikit peristiwa kebocoran data terjadi akibat lemahnya sistem keamanan, serta belum maksimalnya pelaksanaan ketentuan hukum yang mengatur perlindungan tersebut. Data pribadi nasabah yang digunakan dalam aplikasi perbankan digital terdiri atas informasi sensitif seperti nama lengkap, nomor induk kependudukan, nomor rekening, data transaksi, hingga informasi perangkat elektronik yang digunakan. Data-data tersebut merupakan informasi yang sangat berharga dan jika jatuh ke tangan pihak yang tidak bertanggung jawab, dapat dimanfaatkan untuk melakukan kejahatan siber, seperti pencurian identitas dan penyalahgunaan akun perbankan. Oleh karena itu, urgensi keberadaan perlindungan hukum menjadi sangat penting untuk menjamin keamanan dan privasi nasabah sebagai pengguna aplikasi perbankan digital (Khetrina Maria Angnesia, 2025).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan tonggak baru dalam sistem hukum Indonesia yang secara khusus mengatur tentang tata kelola data pribadi. Undang-undang ini mendefinisikan data pribadi sebagai setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik. Dalam konteks perbankan digital, lembaga perbankan bertindak sebagai pengendali data pribadi, yang memiliki tanggung jawab untuk memastikan keamanan dan penggunaan data secara sah dan proporsional[9]

Kewajiban pengendali data pribadi, sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, mencakup antara lain kewajiban memperoleh persetujuan eksplisit dari subjek data, menjamin keakuratan dan integritas data, serta melindungi data dari akses ilegal. Apabila terjadi pelanggaran terhadap ketentuan ini, undang-undang tersebut mengatur sanksi administratif dan pidana sebagai bentuk konsekuensi hukum (Berto Purnomo

[8] Ervina Chintia et al., "*Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya*," *Journal of Information Engineering and Educational Technology* 2, no. 2 (2019): 65, https://doi.org/10.26740/jieet.v2n2.p65-69.

[9] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 1 angka 1.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

Sidik, 2025). Hal ini menunjukkan bahwa negara menempatkan perlindungan data pribadi sebagai bagian integral dari hak asasi warga negara. Dalam Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, disebutkan bahwa setiap orang yang dengan sengaja dan melawan hukum mengumpulkan atau memperoleh data pribadi milik orang lain dengan maksud untuk menguntungkan diri sendiri atau pihak lain, dapat dipidana dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak lima puluh miliar rupiah[10]. Ketentuan ini merupakan dasar hukum pidana dalam menjerat pelaku peretasan atau penyalahgunaan data nasabah aplikasi perbankan digital.

Di sisi lain, kelalaian institusi perbankan dalam menjaga keamanan data nasabah juga tidak luput dari jerat pidana. Pasal 58 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur bahwa pengendali data pribadi yang karena kelalaiannya menyebabkan kebocoran data pribadi dapat dikenai sanksi pidana penjara paling lama empat tahun dan/atau denda paling banyak empat puluh miliar rupiah[11]. Ketentuan ini mempertegas tanggung jawab hukum lembaga perbankan terhadap perlindungan data nasabah. Ketentuan pidana dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi melengkapi aturan sebelumnya dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Dalam Pasal 40 dan 47, disebutkan bahwa bank wajib menjaga kerahasiaan data nasabah dan pelanggaran terhadap kewajiban ini dapat dikenai pidana penjara maksimal empat tahun dan/atau denda maksimal empat miliar rupiah[12]. Dengan demikian, sistem perlindungan data nasabah dalam perbankan digital telah memiliki dasar hukum yang kuat di bidang hukum pidana.

Namun demikian, dalam praktiknya, penegakan hukum terhadap pelanggaran perlindungan data pribadi masih menghadapi banyak tantangan. Salah satu kendala utama adalah keterbatasan kapasitas aparat penegak hukum dalam menangani kejahatan berbasis digital. Penanganan insiden kebocoran data memerlukan keahlian dalam bidang forensik digital, yang belum sepenuhnya dikuasai oleh banyak penegak hukum di Indonesia[13]. Di sisi lain, institusi perbankan juga sering kali bersikap tertutup terhadap insiden kebocoran data. Banyak bank lebih memilih untuk menyelesaikan masalah secara internal tanpa melaporkannya kepada otoritas berwenang, guna menjaga reputasi dan kepercayaan publik. Sikap ini justru memperburuk situasi, karena pelaku kejahatan tidak mendapat hukuman yang setimpal dan korban tidak memperoleh keadilan secara utuh[14].

Laporan dari Lembaga Studi dan Advokasi Masyarakat (ELSAM) menyatakan bahwa pada periode 2020 hingga 2022, terjadi peningkatan signifikan terhadap kasus kebocoran data pribadi, termasuk data nasabah. Sayangnya, sebagian besar dari kasus tersebut tidak ditindaklanjuti ke proses hukum karena lemahnya mekanisme pelaporan dan minimnya transparansi dari institusi yang mengalami kebocoran[15]. Penegakan hukum pidana terhadap kejahatan kebocoran data juga masih menemui hambatan dalam aspek pertanggungjawaban pidana korporasi. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah membuka ruang bagi pertanggungjawaban badan hukum, namun proses pembuktian dan identifikasi aktor yang

[10] Ibid., Pasal 67 ayat (1).
[11] Ibid., Pasal 58.
[12] Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Pasal 40 dan Pasal 47.
[13] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, 2021, hlm. 121–123.
[14] Damar Juniarto, "Kebocoran Data dan Ketimpangan Penegakan Hukum Siber di Indonesia", *ELSAM Brief*, 2022.
[15] ELSAM, *Laporan Situasi Perlindungan Data Pribadi Indonesia 2022*, hlm. 31–35.

Retorika
Jurnal Komunikasi, Sosial, dan Ilmu Politik
ISSN: 3032-7482
(2025), 2 (2): 68-77

bertanggung jawab sering kali menemui jalan buntu. Hal ini menunjukkan pentingnya pembaruan sistem hukum acara pidana yang lebih adaptif terhadap kejahatan korporasi berbasis teknologi[16].

Jika dibandingkan dengan negara lain, misalnya Uni Eropa yang telah menerapkan General Data Protection Regulation (GDPR), Indonesia masih tertinggal dalam hal penegakan sanksi terhadap pelanggaran perlindungan data pribadi. GDPR memberikan kewenangan kepada otoritas perlindungan data untuk menjatuhkan denda administratif yang besar, bahkan terhadap perusahaan teknologi raksasa sekalipun. Di Indonesia, mekanisme semacam ini masih dalam tahap perencanaan, meskipun telah diamanatkan oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi[17]. Selain pendekatan represif, perlindungan hukum pidana juga harus dilengkapi dengan strategi preventif. Pemerintah perlu mendorong lembaga perbankan untuk mengimplementasikan sistem manajemen keamanan informasi berbasis standar internasional seperti ISO/IEC 27001, serta melakukan audit keamanan data secara berkala. Langkah ini penting untuk mencegah terjadinya kebocoran data sejak awal, sebagai bentuk nyata dari tanggung jawab hukum lembaga perbankan[18].

Otoritas Jasa Keuangan (OJK) juga memiliki peran penting dalam mengawasi penyelenggaraan sistem teknologi informasi perbankan. Melalui Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022, OJK mewajibkan setiap bank memiliki manajemen risiko teknologi informasi yang terstruktur dan sistem pengamanan yang mumpuni. Ketidakpatuhan terhadap ketentuan ini dapat dijadikan dasar untuk penjatuhan sanksi administratif atau rekomendasi penindakan hukum[19].

Aspek penting lainnya adalah penguatan kesadaran masyarakat terhadap hak-hak data pribadi mereka. Masyarakat sebagai pengguna aplikasi perbankan digital harus dibekali literasi digital agar tidak menjadi korban kejahatan akibat keteledoran, seperti membagikan data pribadi secara sembarangan. Pemerintah dan lembaga perbankan wajib menyediakan informasi yang edukatif mengenai keamanan digital dan prosedur pengaduan apabila terjadi pelanggaran[20]. Perlindungan hukum pidana terhadap data nasabah tidak boleh berhenti pada tataran normatif belaka. Harus ada komitmen nyata dari semua pihak—pemerintah, lembaga keuangan, aparat penegak hukum, dan masyarakat—untuk menciptakan ekosistem digital yang aman dan adil. Pendekatan multidisipliner dan kolaboratif diperlukan untuk menjawab tantangan kompleksitas kejahatan siber yang terus berkembang secara dinamis.

## KESIMPULAN

Penelitian ini menunjukkan bahwa perkembangan teknologi digital, khususnya aplikasi perbankan digital, memberikan kemudahan namun juga menimbulkan risiko kebocoran data pribadi nasabah yang berdampak negatif secara hukum dan sosial. Indonesia telah mengatur perlindungan data pribadi melalui regulasi khusus, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menetapkan kewajiban dan sanksi bagi pengendali data

[16] Andi Hamzah, *Asas-Asas Hukum Pidana*, Rineka Cipta, 2020, hlm. 82.
[17] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017.
[18] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017.
[19] Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.
[20] Kementerian Komunikasi dan Informatika Republik Indonesia, "Indeks Literasi Digital 2023", www.kominfo.go.id.

ISSN: 3032-7482
(2025), 2 (2): 68-77

dan pelaku kejahatan siber. Namun, penegakan hukum terhadap tindak pidana kebocoran data dan peretasan masih menghadapi hambatan internal berupa keterbatasan profesionalisme aparat penegak hukum serta eksternal berupa rendahnya literasi digital masyarakat, budaya hukum yang kurang mendukung, dan fasilitas yang belum memadai. Oleh karena itu, perlindungan hukum yang efektif terhadap data nasabah di sektor perbankan digital belum optimal dan memerlukan perbaikan berkelanjutan baik dari aspek regulasi, sumber daya manusia, maupun kesadaran publik.

**SARAN**

1. Pemerintah dan lembaga terkait perlu meningkatkan kapasitas dan profesionalisme aparat penegak hukum melalui pelatihan khusus di bidang teknologi informasi dan forensik digital agar penanganan kejahatan siber dapat dilakukan secara efektif dan tepat waktu.
2. Perbankan sebagai pengendali data pribadi harus memperkuat sistem keamanan data dengan menerapkan teknologi mutakhir dan mematuhi regulasi perlindungan data secara ketat, serta transparan dalam melaporkan insiden kebocoran data kepada otoritas berwenang.
3. Masyarakat harus diberdayakan melalui peningkatan literasi digital dan pemahaman hukum mengenai perlindungan data pribadi, sehingga dapat menjadi bagian aktif dalam pengawasan dan pencegahan kejahatan siber.
4. Regulasi yang ada perlu terus diperbaharui menyesuaikan perkembangan modus kejahatan siber agar tidak menjadi pasal karet dan mampu memberikan efek jera bagi pelaku kejahatan digital.
5. Diperlukan kolaborasi antara pemerintah, institusi perbankan, aparat penegak hukum, dan masyarakat dalam membangun ekosistem digital yang aman dan terpercaya guna menjaga hak privasi serta keamanan data pribadi nasabah.

## DAFTAR PUSTAKA

### JURNAL

Ahyar Sidi, w. (2025). EKSPLORASI METODE PENELITIAN DENGAN PENDEKATAN NORMATIF DAN EMPIRIS DALAM PENELITIAN HUKUM DI INDONESIA. Lex Jurnalica, 66-72.

Anesya Fritiana, S. A. (2025). Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online: Analisis Perlindungan dan Sanksi Hukum. Al-Zayn: Jurnal Ilmu Sosial & Hukum, 523-520.

Anesya Fritiana, S. A. (2025). Penyalahgunaan Data Pribadi Pada Layanan Pinjaman Online: Analisis Perlindungan dan Sanksi Hukum. Al-Zayn: Jurnal Ilmu Sosial & Hukum, 523-529.

Berto Purnomo Sidik, S. A. (2025). Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora, 219-232.

Elda Septi Darmayanti, S. A. (2025). Tanggung jawab hukum pinjaman online terhadap penyebaran data nasabah secara ilegal. ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 233-251.

Faisal Santiago, A. R. (2023). Harmonization of Law on Transactions E-Commerce in order to support Indonesia's Economic Development. Journal of Social Research, 1929-1936.

Khetrina Maria Angnesia, S. A. (2025). Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital. Perspektif Administrasi Publik dan hukum, 176-187.

Mugiono Mugiono, S. A. (2025). Between Ease and Vulnerability: Juridical Analysis of Population Identity Data Protection in Digital Applications. COSMOS: Jurnal Ilmu Pendidikan, Ekonomi dan Teknologi, 684-691.

Shafa Salsabila, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi, 145-157.

ISSN: 3032-7482
(2025), 2 (2): 68-77

Sri Mulyati, S. A. (202). PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL. Causa: Jurnal Hukum dan Kewarganegaraan, 91-100.

Chintia, E., Hidayati, A. N., & Santoso, S. (2019). Kasus kejahatan siber yang paling banyak terjadi di Indonesia dan penanganannya. Journal of Information Engineering and Educational Technology, 2(2), 65–69.

Duarif, Duarif, & Saleh, Moh. (2024). Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni. UNES Law Review, 6(4), 12110–12119.

Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). Supremasi: Jurnal Hukum, 5(1), 46–63.

Popal, D. F. T. (2023). Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime). Lex Administratum, (5).

Triputri, D. H., Mofea, S., Yulviani, D., & Pratama, R. (2023). Analisis Yuridis Terhadap Penerapan Sanksi Pidana Bagi Pelaku Penipuan Dalam Transaksi Elektronik Berdasarkan Asas Lex Specialis Derogat Legi Generali Ditinjau Dari KUHP Dan UU ITE. Lex Veritatis, 2(01), 42–51.

**BUKU**

Achmad, F. (2021). Hukum dan Teknologi Informasi: Dinamika dan Tantangan di Era Digital. Jakarta: Kencana.

Arief, Barda Nawawi. (2021). Bunga Rampai Kebijakan Hukum Pidana. Bandung: Citra Aditya Bakti.

Chazawi, Adam. (2015). Tindak Pidana Informasi dan Transaksi Elektronik. Malang: Media Nusa Creative.

Hamzah, Andi. (2020). Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.

Tim PY, Bala. (2019). Undang-Undang Informasi dan Transaksi Elektronik: Seri Perundang-undangan. Yogyakarta: Pustaka Yustisia.

Voigt, Paul & von dem Bussche, Axel. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

**PERATURAN PERUNDANG – UNDANGAN**

Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 1 angka 1.

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Pasal 40 dan Pasal 47.

**WEBSITE**

ELSAM. (2022). Laporan Situasi Perlindungan Data Pribadi Indonesia 2022. Jakarta: ELSAM.

Juniarto, Damar. (2022). Kebocoran Data dan Ketimpangan Penegakan Hukum Siber di Indonesia. ELSAM Brief.

Kementerian Komunikasi dan Informatika Republik Indonesia. “Indeks Literasi Digital 2023”. Diakses dari: https://www.kominfo.go.id.