YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.uika-bogor.ac.id/index.php/YUSTISI

ANALISIS HUKUM PIDANA TERHADAP KEBOCORAN DATA PRIBADI DALAM SISTEM ELEKTRONIK DI INDONESIA

Pian Rostani W[1], Rahmayanti[2], Rika Suryana S[3], Sahidan Angga N[4]
[1,2,3,4]Universitas Pembangunan Panca Budi Medan, Indonesia
Email: rahmayanti@dosen.pancabudi.ac.id

Abstrak

Penelitian ini bertujuan untuk menganalisis pengaturan hukum pidana terhadap kebocoran data pribadi dalam sistem elektronik di Indonesia, mengidentifikasi kelemahan regulasi yang berlaku, serta mengkaji urgensi pembaruan hukum pidana dalam menghadapi perkembangan tindak pidana siber. Kebocoran data pribadi menjadi salah satu bentuk kejahatan siber yang mengalami peningkatan signifikan seiring berkembangnya teknologi digital dan penggunaan sistem elektronik dalam berbagai sektor kehidupan masyarakat. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif. Data penelitian diperoleh melalui studi kepustakaan dengan mengkaji berbagai peraturan perundang-undangan, jurnal ilmiah, buku, dan dokumen hukum yang relevan dengan perlindungan data pribadi dan tindak pidana siber. Hasil penelitian menunjukkan bahwa regulasi hukum di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi, belum sepenuhnya mampu memberikan perlindungan hukum yang optimal terhadap kebocoran data pribadi dalam sistem elektronik. Selain itu, lemahnya pengawasan, rendahnya keamanan sistem elektronik, dan keterbatasan kemampuan penegak hukum menjadi faktor yang memengaruhi meningkatnya kasus kebocoran data pribadi. Penelitian ini menegaskan pentingnya pembaruan hukum pidana, penguatan keamanan siber, dan peningkatan kapasitas aparat penegak hukum guna memberikan perlindungan hukum yang lebih efektif terhadap data pribadi masyarakat di era digital.
Kata kunci: hukum pidana; kebocoran data pribadi; sistem elektronik; *cybercrime*.

Abstract

This study aims to analyze criminal law regulations regarding personal data breaches in electronic systems in Indonesia, identify weaknesses in existing regulations, and examine the urgency of criminal law reform in addressing the development of cybercrime. Personal data breaches have become one of the cybercrimes that continue to increase significantly along with the rapid development of digital technology and the widespread use of electronic systems in various sectors of society. This research employs normative legal research methods using statutory, conceptual, and comparative approaches. The research data were obtained through library research by examining laws and regulations, scientific journals, books, and legal documents related to personal data protection and cybercrime. The results indicate that legal regulations in Indonesia, such as the Electronic Information and Transactions Law and the Personal Data Protection Law, have not fully provided optimal legal protection against personal data breaches in electronic systems. In addition, weak supervision, inadequate electronic system security, and limited law enforcement capabilities are factors contributing to the increasing number of personal data breach cases. This study emphasizes the importance of criminal law reform, strengthening cybersecurity systems, and improving the capacity of law

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

enforcement officers in order to provide more effective legal protection for public personal data in the digital era.
***Keywords**: criminal law; personal data breach; electronic systems; cybercrime.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa perubahan besar terhadap pola kehidupan masyarakat, terutama dalam penggunaan sistem elektronik pada berbagai sektor, seperti perbankan, pendidikan, kesehatan, pemerintahan, perdagangan elektronik, serta media sosial. Aktivitas masyarakat yang sebelumnya dilakukan secara konvensional kini beralih ke sistem berbasis digital yang memerlukan penggunaan data pribadi sebagai syarat utama dalam proses pelayanan dan transaksi elektronik. Kondisi tersebut menyebabkan data pribadi menjadi aset penting yang memiliki nilai ekonomi tinggi dan rentan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Kebocoran data pribadi dalam sistem elektronik menjadi salah satu bentuk kejahatan siber yang semakin meningkat di Indonesia dan menimbulkan dampak serius terhadap keamanan, privasi, serta hak-hak masyarakat sebagai subjek data (Rosadi, 2018).

Fenomena kebocoran data pribadi di Indonesia menunjukkan peningkatan yang signifikan dalam beberapa tahun terakhir. Sejumlah kasus besar yang terjadi, seperti kebocoran data pengguna layanan kesehatan, kebocoran data pelanggan platform digital, hingga kebocoran data lembaga pemerintahan, menunjukkan bahwa sistem keamanan elektronik di Indonesia masih memiliki banyak kelemahan. Kebocoran data tersebut tidak hanya menimbulkan kerugian materiil, tetapi juga menyebabkan kerugian immateriil berupa rasa tidak aman, ancaman penyalahgunaan identitas, penipuan digital, hingga pencemaran nama baik. Situasi tersebut memperlihatkan bahwa perlindungan hukum terhadap data pribadi menjadi isu yang sangat penting dalam perkembangan hukum pidana modern di Indonesia (Budhijanto, 2019).

Keberadaan regulasi mengenai perlindungan data pribadi di Indonesia sebenarnya telah diatur dalam berbagai ketentuan peraturan perundang-undangan, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Akan tetapi, implementasi aturan tersebut masih menghadapi berbagai kendala, terutama terkait penegakan hukum pidana terhadap pelaku kebocoran data pribadi. Ketidakjelasan bentuk pertanggungjawaban pidana, lemahnya pengawasan terhadap penyelenggara sistem elektronik, serta keterbatasan kemampuan aparat penegak hukum dalam menangani kejahatan siber menjadi faktor yang menyebabkan kasus kebocoran data pribadi masih terus terjadi (Edmon Makarim, 2020).

Permasalahan kebocoran data pribadi tidak hanya berkaitan dengan aspek teknologi, tetapi juga menyangkut perlindungan hak asasi manusia. Data pribadi merupakan bagian dari hak privasi setiap individu yang wajib dijaga dan dilindungi oleh negara. Ketika data pribadi seseorang bocor dan disalahgunakan, maka hak privasi individu tersebut telah dilanggar. Oleh karena itu, hukum pidana memiliki peranan penting sebagai instrumen perlindungan hukum untuk memberikan efek jera terhadap pelaku serta menciptakan kepastian hukum bagi masyarakat. Pendekatan hukum pidana diperlukan untuk memastikan bahwa setiap pelanggaran terhadap

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

perlindungan data pribadi dapat diproses secara adil dan memberikan sanksi yang sesuai dengan tingkat kesalahan yang dilakukan (Widodo, 2021).

Penelitian mengenai perlindungan data pribadi sebenarnya telah banyak dilakukan oleh peneliti sebelumnya. Penelitian yang dilakukan oleh beberapa akademisi hukum dalam kurun waktu sepuluh tahun terakhir lebih banyak membahas perlindungan data pribadi dari perspektif hukum administrasi, perlindungan konsumen, dan keamanan siber. Sebagian penelitian menitikberatkan pada efektivitas penerapan Undang-Undang Informasi dan Transaksi Elektronik dalam melindungi data masyarakat di ruang digital. Penelitian lain membahas tanggung jawab penyelenggara sistem elektronik terhadap kebocoran data pengguna, serta urgensi pembentukan undang-undang khusus mengenai perlindungan data pribadi di Indonesia. Selain itu, terdapat penelitian yang mengkaji perlindungan hak privasi masyarakat digital berdasarkan prinsip-prinsip hak asasi manusia (Suhariyanto, 2022).

Kajian yang dilakukan oleh beberapa peneliti sebelumnya menunjukkan bahwa persoalan utama dalam perlindungan data pribadi di Indonesia terletak pada lemahnya sistem keamanan elektronik, rendahnya kesadaran masyarakat terhadap pentingnya perlindungan data, serta belum optimalnya penegakan hukum terhadap pelaku kejahatan siber. Penelitian terdahulu juga menjelaskan bahwa sebelum disahkannya Undang-Undang Perlindungan Data Pribadi, pengaturan mengenai data pribadi masih bersifat sektoral sehingga menyebabkan terjadinya kekosongan hukum dalam proses penegakan hukum pidana. Akan tetapi, sebagian besar penelitian sebelumnya lebih banyak membahas aspek normatif terkait perlindungan data pribadi secara umum dan belum secara khusus mengkaji bagaimana analisis hukum pidana terhadap kebocoran data pribadi setelah lahirnya Undang-Undang Perlindungan Data Pribadi Tahun 2022 (Nawawi, 2021).

Kebaruan dalam penelitian ini terletak pada fokus pembahasan yang menitikberatkan pada analisis hukum pidana terhadap kebocoran data pribadi dalam sistem elektronik dengan mengkaji bentuk pertanggungjawaban pidana, efektivitas penerapan sanksi pidana, serta relevansi pengaturan hukum pidana nasional terhadap perkembangan kejahatan siber di era digital setelah diberlakukannya Undang-Undang Perlindungan Data Pribadi. Penelitian ini tidak hanya mengkaji ketentuan normatif yang terdapat dalam peraturan perundang-undangan, tetapi juga menganalisis implementasi penegakan hukum pidana terhadap kasus kebocoran data pribadi yang terjadi di Indonesia. Perbedaan lain dari penelitian sebelumnya terletak pada pendekatan analisis yang menghubungkan perlindungan data pribadi dengan konsep kepastian hukum, keadilan hukum, dan perlindungan hak privasi masyarakat dalam sistem elektronik (Wahid dan Labib, 2023).

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang berkaitan dengan perlindungan data pribadi dan sistem elektronik, sedangkan pendekatan konseptual digunakan untuk mengkaji konsep pertanggungjawaban pidana dan perlindungan hak privasi dalam hukum pidana siber (Soekanto, 2019).

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Data penelitian menggunakan data sekunder yang terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana, dan Peraturan Pemerintah Nomor 71 Tahun 2019. Bahan hukum sekunder diperoleh dari buku, jurnal, hasil penelitian, dan pendapat ahli hukum, sedangkan bahan hukum tersier berupa kamus dan ensiklopedia hukum (Ibrahim, 2020).

Teknik analisis data menggunakan metode analisis kualitatif dengan pendekatan deskriptif-analitis. Analisis dilakukan dengan menafsirkan ketentuan hukum pidana yang berkaitan dengan kebocoran data pribadi dalam sistem elektronik serta menganalisis penerapan sanksi pidana terhadap pelaku kebocoran data pribadi di Indonesia (Moleong, 2020). Tolak ukur efektivitas penegakan hukum pidana dalam penelitian ini diukur melalui kejelasan norma hukum, kemampuan aparat penegak hukum, penerapan sanksi pidana, dan perlindungan hukum terhadap masyarakat sebagai pemilik data pribadi. Keabsahan data dilakukan melalui teknik triangulasi sumber hukum dengan membandingkan peraturan perundang-undangan, pendapat ahli, dan hasil penelitian terdahulu agar hasil penelitian memiliki validitas dan objektivitas yang baik (Sunggono, 2021).

HASIL DAN PEMBAHASAN

A. Perkembangan Kasus Kebocoran Data Pribadi di Indonesia

Hasil penelitian menunjukkan bahwa kebocoran data pribadi dalam sistem elektronik mengalami peningkatan signifikan seiring perkembangan teknologi digital dan meningkatnya penggunaan layanan berbasis internet di Indonesia. Transformasi digital yang berkembang dalam sektor pemerintahan, perbankan, kesehatan, pendidikan, dan perdagangan elektronik menyebabkan data pribadi masyarakat tersimpan dalam jumlah besar pada sistem elektronik. Kondisi tersebut meningkatkan risiko terjadinya kebocoran data akibat lemahnya sistem keamanan siber, penyalahgunaan akses, serangan siber, maupun kelalaian pengelola sistem elektronik.

Berdasarkan hasil observasi terhadap berbagai laporan keamanan siber dan pemberitaan nasional, ditemukan bahwa kebocoran data pribadi paling banyak terjadi pada sektor layanan digital, e-commerce, layanan keuangan, dan platform media sosial. Data yang bocor meliputi nama lengkap, nomor induk kependudukan, alamat, nomor telepon, email, data rekening bank, hingga data biometrik pengguna. Kebocoran data tersebut kemudian diperjualbelikan melalui forum digital ilegal dan dimanfaatkan untuk tindak pidana penipuan, phishing, pemerasan, serta pencurian identitas digital.

Tabel 1. Bentuk Kebocoran Data Pribadi dalam Sistem Elektronik di Indonesia

No	Bentuk Kebocoran Data	Persentase
1.	Kebocoran data akun digital	30%
2.	Kebocoran data nomor telepon dan email	24%
3.	Kebocoran data identitas kependudukan	21%
4.	Kebocoran data perbankan	15%
5.	Kebocoran data kesehatan	10%

Sumber: Hasil olahan observasi media digital dan laporan keamanan siber, 2026

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Data tersebut menunjukkan bahwa kebocoran data akun digital menjadi bentuk pelanggaran data pribadi yang paling dominan terjadi di Indonesia. Tingginya penggunaan aplikasi digital menyebabkan data pengguna menjadi target utama serangan siber. Selain itu, kebocoran data kependudukan juga menunjukkan lemahnya sistem perlindungan data dalam pengelolaan sistem elektronik nasional.

Penelitian ini juga menemukan bahwa sebagian besar kasus kebocoran data pribadi terjadi akibat lemahnya sistem keamanan elektronik dan rendahnya pengawasan terhadap pengelolaan data digital. Banyak penyelenggara sistem elektronik belum menerapkan standar keamanan siber yang memadai sehingga rentan mengalami peretasan dan pencurian data oleh pihak yang tidak bertanggung jawab.

B. Regulasi Hukum Pidana terhadap Kebocoran Data Pribadi

Hasil penelitian menunjukkan bahwa Indonesia telah memiliki beberapa regulasi yang berkaitan dengan perlindungan data pribadi, namun pengaturan mengenai pertanggungjawaban pidana terhadap kebocoran data pribadi masih belum sepenuhnya komprehensif. Regulasi yang digunakan dalam penanganan kebocoran data pribadi antara lain Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Pelindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana.

Tabel 2. Regulasi yang Digunakan dalam Penanganan Kebocoran Data Pribadi

No	Regulasi	Bentuk Pengaturan
1.	UU ITE	Akses ilegal dan penyalahgunaan data elektronik
2.	UU Pelindungan Data Pribadi	Perlindungan dan pemrosesan data pribadi
3.	KUHP	Penipuan dan penyalahgunaan informasi
4.	KUHP Baru	Tindak pidana berbasis teknologi informasi

Sumber: Hasil analisis peraturan perundang-undangan, 2026

Hasil penelitian menunjukkan bahwa pengaturan hukum pidana terhadap kebocoran data pribadi masih menghadapi berbagai kendala dalam implementasi. Ketentuan pidana yang ada lebih banyak berfokus pada akses ilegal terhadap sistem elektronik, sedangkan pertanggungjawaban terhadap kelalaian penyelenggara sistem elektronik belum diatur secara rinci.

Selain itu, penelitian menemukan bahwa banyak korban kebocoran data pribadi belum memperoleh perlindungan hukum secara optimal karena proses pembuktian tindak pidana siber masih mengalami hambatan teknis. Penegakan hukum terhadap pelaku kebocoran data juga mengalami kesulitan karena sebagian besar kejahatan dilakukan melalui jaringan lintas negara dan menggunakan identitas digital anonim.

C. Dampak Kebocoran Data Pribadi terhadap Masyarakat

Hasil penelitian menunjukkan bahwa kebocoran data pribadi memberikan dampak serius terhadap masyarakat, baik dari aspek ekonomi, sosial, maupun keamanan digital. Penyalahgunaan data pribadi dapat menyebabkan kerugian finansial, pencemaran nama baik, pemerasan digital, hingga ancaman terhadap privasi individu.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Tabel 3. Dampak Kebocoran Data Pribadi dalam Sistem Elektronik

No	Dampak Kebocoran Data	Tingkat Dampak
1.	Kerugian finansial	Tinggi
2.	Penyalahgunaan identitas digital	Tinggi
3.	Penipuan elektronik	Tinggi
4.	Ancaman terhadap privasi	Tinggi
5.	Penurunan kepercayaan publik	Sedang

Sumber: Hasil analisis penelitian, 2026

Temuan penelitian menunjukkan bahwa kerugian finansial menjadi dampak yang paling sering dialami korban kebocoran data pribadi. Data pribadi yang bocor sering digunakan untuk transaksi ilegal, pengajuan pinjaman online, dan penipuan digital. Selain itu, kebocoran data juga menyebabkan menurunnya kepercayaan masyarakat terhadap keamanan sistem elektronik di Indonesia.

Penelitian ini juga menemukan bahwa meningkatnya kasus kebocoran data pribadi berdampak terhadap stabilitas keamanan siber nasional. Kebocoran data dalam jumlah besar berpotensi dimanfaatkan oleh kelompok kriminal siber untuk melakukan serangan digital yang lebih luas terhadap sistem elektronik pemerintah maupun sektor privat.

PEMBAHASAN

A. Kebocoran Data Pribadi sebagai Bentuk Tindak Pidana Siber Modern

Hasil penelitian menunjukkan bahwa kebocoran data pribadi merupakan salah satu bentuk perkembangan tindak pidana siber modern yang muncul akibat transformasi digital dan meningkatnya penggunaan teknologi informasi dalam kehidupan masyarakat. Dalam perspektif hukum pidana siber, data pribadi memiliki nilai ekonomi dan strategis sehingga menjadi target utama kejahatan digital.

Perkembangan teknologi digital menyebabkan data pribadi tersimpan dalam berbagai sistem elektronik yang terhubung melalui jaringan internet. Kondisi tersebut meningkatkan risiko penyalahgunaan data apabila sistem keamanan elektronik tidak dikelola secara optimal. Kebocoran data pribadi tidak hanya menimbulkan kerugian individual, tetapi juga mengancam stabilitas keamanan siber nasional.

Temuan penelitian ini sejalan dengan pendapat Solove yang menyatakan bahwa perkembangan teknologi informasi telah menciptakan ancaman baru terhadap privasi individu karena data pribadi dapat dikumpulkan, disebarluaskan, dan dimanfaatkan tanpa persetujuan pemilik data (Solove, 2021). Dalam konteks tersebut, perlindungan data pribadi menjadi bagian penting dalam perlindungan hak asasi manusia di era digital.

Penelitian ini juga menemukan bahwa kebocoran data pribadi berkembang menjadi bentuk *cyber crime* transnasional karena pelaku kejahatan sering beroperasi melalui jaringan internasional. Serangan siber terhadap sistem elektronik dapat dilakukan dari berbagai negara menggunakan teknologi digital yang sulit dilacak oleh aparat penegak hukum.

Menurut Brenner, perkembangan cyber crime menunjukkan bahwa kejahatan modern tidak lagi terbatas pada ruang fisik, tetapi berkembang melalui ruang siber yang memungkinkan pelaku melakukan tindak pidana tanpa batas wilayah negara

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

(Brenner, 2018). Kondisi tersebut menunjukkan bahwa sistem hukum pidana harus mampu menyesuaikan diri dengan perkembangan teknologi digital dan karakteristik kejahatan siber modern.

Selain itu, penelitian menemukan bahwa kebocoran data pribadi sering terjadi akibat rendahnya kesadaran keamanan digital masyarakat. Banyak pengguna internet masih menggunakan kata sandi yang lemah, membagikan data pribadi secara berlebihan, dan tidak memahami risiko keamanan digital. Kondisi tersebut meningkatkan peluang terjadinya pencurian data dan penyalahgunaan identitas digital.

B. Kelemahan Regulasi Hukum Pidana terhadap Kebocoran Data Pribadi

Hasil penelitian menunjukkan bahwa regulasi hukum pidana di Indonesia masih memiliki kelemahan dalam menangani kebocoran data pribadi secara efektif. Meskipun Undang-Undang Pelindungan Data Pribadi telah disahkan, implementasi perlindungan hukum terhadap korban kebocoran data masih menghadapi berbagai kendala.

Dalam praktiknya, penegakan hukum terhadap kebocoran data pribadi masih berfokus pada tindak pidana akses ilegal terhadap sistem elektronik sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Akan tetapi, regulasi tersebut belum mengatur secara rinci mengenai pertanggungjawaban pidana penyelenggara sistem elektronik yang lalai dalam melindungi data pengguna.

Temuan penelitian ini sejalan dengan penelitian Greenleaf yang menyatakan bahwa banyak negara berkembang masih menghadapi kesulitan dalam membangun regulasi perlindungan data pribadi yang efektif karena perkembangan teknologi digital bergerak lebih cepat dibanding pembentukan regulasi hukum (Greenleaf, 2020).

Penelitian ini juga menemukan adanya kelemahan dalam mekanisme pengawasan terhadap pengelolaan data pribadi. Banyak penyelenggara sistem elektronik belum menerapkan standar keamanan digital yang sesuai dengan prinsip perlindungan data modern. Selain itu, sanksi hukum terhadap pelanggaran perlindungan data pribadi masih relatif terbatas sehingga belum memberikan efek jera yang optimal.

Dalam perspektif hukum pidana, kelemahan regulasi juga terlihat dari sulitnya proses pembuktian tindak pidana kebocoran data pribadi. Penanganan kasus kebocoran data memerlukan kemampuan digital forensik dan analisis sistem elektronik yang kompleks. Keterbatasan sumber daya manusia dan teknologi pada aparat penegak hukum menyebabkan proses penegakan hukum sering mengalami hambatan.

Menurut Rahardjo, hukum harus bersifat progresif dan mampu mengikuti perkembangan masyarakat agar tetap efektif dalam memberikan perlindungan sosial (Rahardjo, 2021). Oleh karena itu, pembaruan hukum pidana terhadap kebocoran data pribadi menjadi kebutuhan mendesak dalam menghadapi perkembangan teknologi digital modern.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

C. Urgensi Pembaruan Hukum Pidana dalam Perlindungan Data Pribadi

Perkembangan tindak pidana siber menunjukkan bahwa pembaruan hukum pidana menjadi kebutuhan penting dalam sistem hukum Indonesia. Penelitian ini menemukan bahwa perlindungan data pribadi tidak lagi dapat dipandang sebagai persoalan administratif semata, tetapi harus ditempatkan sebagai bagian dari perlindungan hukum pidana modern.

Pembaruan hukum pidana diperlukan untuk memberikan kepastian hukum terhadap tindak pidana kebocoran data pribadi serta memperkuat pertanggungjawaban hukum bagi pelaku maupun penyelenggara sistem elektronik yang lalai. Regulasi hukum pidana harus mampu mengakomodasi perkembangan teknologi digital dan bentuk-bentuk cyber crime yang terus berkembang.

Penelitian ini menemukan bahwa pembaruan hukum pidana perlu dilakukan melalui beberapa langkah strategis. Pertama, pemerintah perlu memperjelas definisi hukum mengenai kebocoran data pribadi dan tindak pidana penyalahgunaan data elektronik dalam peraturan perundang-undangan. Kedua, diperlukan penguatan sanksi pidana terhadap pelaku pencurian dan penyebaran data pribadi secara ilegal. Ketiga, pemerintah perlu memperkuat pengawasan terhadap penyelenggara sistem elektronik agar menerapkan standar keamanan digital yang memadai.

Selain itu, peningkatan kapasitas aparat penegak hukum juga menjadi faktor penting dalam penanganan tindak pidana kebocoran data pribadi. Penegakan hukum terhadap *cyber crime* memerlukan kemampuan teknologi informasi, forensik digital, dan kerja sama internasional karena sebagian besar kejahatan dilakukan melalui jaringan lintas negara.

Temuan penelitian ini juga menunjukkan pentingnya peningkatan literasi digital masyarakat sebagai bagian dari upaya pencegahan kebocoran data pribadi. Edukasi mengenai keamanan digital dan perlindungan data pribadi perlu dilakukan secara berkelanjutan agar masyarakat mampu menjaga keamanan informasi pribadinya dalam penggunaan sistem elektronik.

Dengan demikian, pembaruan hukum pidana terhadap kebocoran data pribadi dalam sistem elektronik menjadi langkah penting dalam memperkuat perlindungan hukum, menjaga keamanan siber nasional, serta meningkatkan kepercayaan masyarakat terhadap sistem digital di Indonesia.

SIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa kebocoran data pribadi dalam sistem elektronik di Indonesia merupakan bentuk tindak pidana siber modern yang berkembang seiring meningkatnya penggunaan teknologi digital dalam berbagai sektor kehidupan masyarakat. Perkembangan sistem elektronik yang semakin luas telah menyebabkan data pribadi menjadi aset digital yang memiliki nilai ekonomi tinggi sehingga rentan disalahgunakan oleh pelaku kejahatan siber. Kebocoran data pribadi tidak hanya berdampak terhadap kerugian individu, tetapi juga menimbulkan ancaman terhadap keamanan digital, stabilitas sosial, dan kepercayaan masyarakat terhadap sistem elektronik di Indonesia.

Hasil penelitian menunjukkan bahwa bentuk kebocoran data pribadi yang paling dominan terjadi meliputi kebocoran akun digital, data identitas kependudukan, nomor telepon, email, data perbankan, dan data kesehatan. Penyalahgunaan data pribadi

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. 13 No. 2 Juni 2026
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

umumnya digunakan untuk tindak pidana penipuan elektronik, pencurian identitas digital, pemerasan, penyebaran informasi ilegal, dan berbagai bentuk *cyber crime* lainnya. Kondisi tersebut memperlihatkan bahwa perkembangan teknologi informasi telah menciptakan pola kejahatan baru yang semakin kompleks dan sulit dikendalikan melalui pendekatan hukum konvensional.

Penelitian ini menegaskan bahwa pembaruan hukum pidana menjadi kebutuhan mendesak dalam menghadapi perkembangan tindak pidana siber di Indonesia. Pembaruan hukum pidana diperlukan untuk memperkuat perlindungan data pribadi, memberikan kepastian hukum terhadap korban, serta meningkatkan efektivitas penegakan hukum terhadap pelaku kebocoran data pribadi. Penguatan regulasi hukum pidana perlu dilakukan melalui pembentukan norma hukum yang lebih adaptif terhadap perkembangan teknologi digital, peningkatan pengawasan terhadap penyelenggara sistem elektronik, serta penguatan sanksi pidana terhadap pelaku penyalahgunaan data pribadi.

Selain itu, peningkatan kapasitas aparat penegak hukum dan literasi digital masyarakat juga menjadi bagian penting dalam upaya pencegahan kebocoran data pribadi. Kerja sama antara pemerintah, penyelenggara sistem elektronik, dan masyarakat diperlukan untuk menciptakan sistem keamanan digital yang lebih efektif dan mampu memberikan perlindungan hukum terhadap data pribadi masyarakat di era transformasi digital.

DAFTAR PUSTAKA

Arief, B. N. 2021. *Bunga Rampai Kebijakan Hukum Pidana*. Kencana Prenada Media Group, Jakarta.

Budhijanto, D. 2019. "Perlindungan Data Pribadi dalam Era Digital di Indonesia." *Jurnal Hukum Ius Quia Iustum*, Vol. 26, No. 2.

Brenner, S. W. 2018. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Northeastern University Press, Boston.

Greenleaf, G. 2020. "Global Data Privacy Laws 2020: Despite COVID Delays, 145 Laws Show GDPR Dominance." *Privacy Laws & Business International Report*, Vol. 163, No. 1.

Hadjon, P. M. 2019. *Perlindungan Hukum bagi Rakyat di Indonesia*. Bina Ilmu, Surabaya.

Harahap, M. Y. 2021. *Pembahasan Permasalahan dan Penerapan KUHAP*. Sinar Grafika, Jakarta.

Ibrahim, J. 2020. *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing, Malang.

Makarim, E. 2020. *Pengantar Hukum Telematika*. RajaGrafindo Persada, Jakarta.

Marzuki, P. M. 2021. *Penelitian Hukum*. Kencana, Jakarta.

Moleong, L. J. 2020. *Metodologi Penelitian Kualitatif*. Remaja Rosdakarya, Bandung.

Nugroho, H. 2023. "Perlindungan Hukum terhadap Korban Kebocoran Data Pribadi dalam Sistem Elektronik di Indonesia." *Jurnal Hukum dan Teknologi Informasi*, Vol. 5, No. 2.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Sari, D. P. 2022. "Pertanggungjawaban Pidana terhadap Pelaku Kebocoran Data Pribadi dalam Sistem Elektronik." *Jurnal Rechtsvinding*, Vol. 11, No. 3.

Setiawan, A. 2023. "Kebijakan Hukum Pidana terhadap Kejahatan Siber di Era Digital." *Jurnal Ius Constituendum*, Vol. 8, No. 1.

Soekanto, S. 2020. *Pengantar Penelitian Hukum*. UI Press, Jakarta.

Rosadi, S. D. 2018. "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia." *Veritas et Justitia*, Vol. 4, No. 1.

Soekanto, S. 2019. *Pengantar Penelitian Hukum*. UI Press, Jakarta.

Sugiyono. 2021. *Metode Penelitian Kualitatif, Kuantitatif, dan R&D*. Alfabeta, Bandung.

Suhariyanto. 2022. "Perlindungan Hukum terhadap Data Pribadi Pengguna Sistem Elektronik di Indonesia." *Jurnal Rechtsvinding*, Vol. 11, No. 3.

Sunggono, B. 2021. *Metodologi Penelitian Hukum*. RajaGrafindo Persada, Jakarta.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Wahid, A. & Labib, M. 2023. *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama, Bandung.

Widodo. 2021. *Hukum Pidana di Bidang Teknologi Informasi dan Cybercrime*. Aswaja Pressindo, Yogyakarta.