Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025)
Tema/Edisi : Hukum dan Hak Asasi Manusia (Bulan Kedua belas)
https://jhlg.rewangrencang.com/

PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITALISASI DAN TANTANGAN KEAMANAN SIBER DI INDONESIA

PROTECTION OF PERSONAL DATA IN THE DIGITAL ERA AND CYBERSECURITY CHALLENGES IN INDONESIA

Muhammad Rendi, Fristia Berdian Tamza dan Ahmad Irzal Fardiansyah

Magister Ilmu Hukum, Universitas Lampung

Korespondensi Penulis: renndymu@gmail.com, Fristia.berdian@fh.unila.ac.id, Ahmadirzalf@fh.unila.ac.id

Citation Structure Recommendation:

Rendi, Muhammad, Fristia Berdian Tamza dan Ahmad Irzal Fardiansyah. *Perlindungan Data Pribadi dalam Era Digitalisasi dan Tantangan Keamanan Siber di Indonesia*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.6. No.12 (2025).

ABSTRAK

Era digitalisasi telah membawa transformasi mendasar dalam pengelolaan data pribadi di Indonesia, namun juga menghadirkan tantangan keamanan yang semakin kompleks. Insiden kebocoran data 341.000 personel Polri oleh aktor bernama Bjorka pada Oktober 2025 menjadi bukti nyata dari kerentanan infrastruktur keamanan siber nasional dan kegagalan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Penelitian ini menganalisis tidak hanya kelemahan dalam implementasi UU PDP, tetapi juga peran strategis Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai fondasi keamanan sistem informasi elektronik di lembaga pemerintahan. Kedua instrumen hukum ini UU ITE dan UU PDP menciptakan *dual-layer protection system* untuk perlindungan data pribadi yang dikelola oleh lembaga pemerintahan. UU ITE mengatur keamanan sistem informasi elektronik melalui Pasal 28, Pasal 30, dan Pasal 32, yang mewajibkan lembaga pemerintahan sebagai penyelenggara sistem elektronik untuk melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan data pribadi. Sementara itu, UU PDP menyediakan kerangka komprehensif mengenai perlindungan data pribadi dengan mengatur kewajiban pengendali data, hak subjek data pribadi, pembentukan lembaga pengawas independen (Komisi Perlindungan Data Pribadi/KPDP), dan sistem sanksi administratif serta pidana yang terstruktur. Meskipun kerangka hukum telah disahkan, efektivitasnya dalam praktik masih menghadapi berbagai kendala struktural dan implementatif pada ketiga pilar utama sistem hukum Lawrence M. Friedman: (1) struktur institusi yang lemah dengan kapasitas SDM terbatas di KPDP, koordinasi antarlembaga yang kurang efektif, dan mekanisme akuntabilitas yang perlu diperkuat; (2) substansi regulasi yang masih bersifat abstrak dan memerlukan peraturan pelaksana yang lebih konkrit dan operasional; dan (3) budaya keamanan data dan keamanan siber yang belum tertanam dengan kuat di seluruh institusi publik Indonesia. Pencegahan kebocoran data di masa depan memerlukan pendekatan komprehensif yang mengintegrasikan aspek hukum (harmonisasi UU ITE-UU PDP), teknologi (modernisasi infrastruktur

keamanan siber), organisasi (pembentukan tim keamanan siber dan respons insiden yang terlatih), dan budaya (peningkatan kesadaran keamanan data di seluruh lembaga pemerintahan). Rekomendasi kebijakan disusun untuk empat pemangku kepentingan utama, Pemerintah, Polri, Sektor Swasta, dan Masyarakat guna memperkuat tata kelola perlindungan data pribadi dan keamanan siber nasional secara berkelanjutan, dengan penekanan khusus pada penerapan sanksi yang konsisten dan efektif bagi lembaga pemerintahan yang lalai dalam melindungi data pribadi warga negara.

Kata Kunci: Budaya Keamanan Data, *Dual-Layer Protection System*, Keamanan Nasional, Keamanan Siber Pemerintah, Kebocoran Data, Perlindungan Data Pribadi, Sanksi Administratif dan Pidana, Sistem Hukum, UU ITE, UU PDP

ABSTRACT

The era of digitalization has brought fundamental changes in the management of personal data in Indonesia, but it has also presented increasingly complex security challenges. The leak of 341,000 Indonesian National Police personnel data by an actor named Bjorka in October 2025 is clear evidence of the vulnerability of the national cybersecurity infrastructure and the failure to implement Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This study analyzes not only the weaknesses in the implementation of the PDP Law, but also the strategic role of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as the foundation for electronic information system security in government institutions. These two legal instruments, the ITE Law and the PDP Law, create a layered protection system for the protection of personal data managed by government agencies. The ITE Law regulates the security of electronic information systems through Articles 28, 30, and 32, which require government agencies as electronic system operators to protect the availability, integrity, authenticity, confidentiality, and accessibility of personal data. Meanwhile, the PDP Law provides a comprehensive framework for personal data protection by regulating the obligations of data controllers, the rights of personal data subjects, the establishment of an independent supervisory agency (Personal Data Protection Commission/KPDP), and a structured system of administrative and criminal sanctions. Although the legal framework has been passed, its effectiveness in practice still faces various structural and implementation challenges in the three main pillars of Lawrence M. Friedman's legal system: (1) weak institutional structures with limited human resource capacity in the KPDP, ineffective inter-agency coordination, and accountability mechanisms that need to be strengthened; (2) regulatory substance that is still abstract and requires more concrete and operational implementing regulations; and (3) a culture of data security and cybersecurity that is not yet firmly embedded in all Indonesian public institutions. Preventing future data leaks requires a comprehensive approach that integrates legal aspects (harmonization of the ITE Law and PDP Law), technology (modernization of cybersecurity infrastructure), organization (establishment of a trained cybersecurity and incident response team), and culture (increased awareness of data security across government agencies). Policy recommendations are formulated for four key stakeholders the government, the National Police, the private sector, and the public to strengthen the governance of personal data protection and national

cybersecurity in a sustainable manner, with a particular emphasis on the consistent and effective application of sanctions for government agencies that fail to protect citizens' personal data.
Keywords: Data Security Culture, Dual-Layer Protection System, National Security, Government Cybersecurity, Data Breaches, Personal Data Protection, Administrative and Criminal Sanctions, Legal System, ITE Law, PDP Law

A. PENDAHULUAN

Era digitalisasi telah mengubah lanskap perlindungan data pribadi di Indonesia secara fundamental dan multidimensional.[1] Transformasi digital yang masif di berbagai sektor pemerintahan, swasta, dan layanan publik telah menciptakan kompleksitas baru dalam pengelolaan dan perlindungan informasi personal. Data pribadi kini tersimpan dalam sistem informasi yang terintegrasi, cloud computing, dan infrastruktur digital yang semakin canggih, namun juga semakin rentan terhadap serangan siber.[2]

Dalam tinjauan filosofis privasi merupakan hak asasi manusia yang fundamental dan tidak dapat dipisahkan dari kemanusiaan itu sendiri. Konsep privasi telah berkembang melalui filsafat hukum yang mendalam sejak abad ke-19. Warren dan Brandeis (1890) dalam karya klasik mereka menegaskan bahwa privasi adalah "*right to be alone*" atau hak untuk memiliki kebebasan dan kesendirian dalam hidup.[3] Konsepsi ini menekankan bahwa setiap individu memiliki hak intrinsik untuk mengontrol informasi tentang dirinya sendiri dan melindungi kehidupan pribadinya dari campur tangan pihak lain yang tidak berhak.[4] Teori "*informational self-determination*" yang dikembangkan dalam konteks hukum Jerman menggambarkan privasi sebagai kemampuan fundamental setiap individu untuk mengatur dan mengontrol informasi pribadi mereka.[5] Teori ini menjadi fondasi bagi berbagai legislasi perlindungan data di berbagai negara, GDPR Uni Eropa dan UU PDP Indonesia. Tanpa kemampuan menentuan nasib data pribadi mereka, individu tidak dapat menjaga integritas dan martabat pribadi mereka dalam masyarakat modern yang semakin terhubung secara digital.

---

[1] S. Arifin dkk., *Cyber Security Culture in Indonesian Government Agencies: Challenges and Policy Recommendations*, Indonesian Journal of Cyber Security, Vol.21, No.2 (2023), p.78

[2] *Ibid.,* p.80.

[3] Samuel D. Warren dan Louis D. Brandeis, *The Right to Privacy*, Harvard Law School, Cambridge, 1890, p.5.

[4] O. Notohamidjojo, *Soal-soal Pokok Filsafat Hukum*, Sastra Hudaya, Jakarta, 1974, p.60.

[5] Hans Kelsen, *Teori Hukum Murni: Dasar-dasar Ilmu Hukum Normatif, Cetakan XVI, Terjemahan dari Pure Theory of Law*, Penerbit Nusa Media, Bandung, 2014, p.45.

Respons pemerintah Indonesia terhadap tantangan ini adalah dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai instrumen hukum utama untuk mengatur dan melindungi hak-hak fundamental warga negara atas keamanan dan privasi data pribadi mereka.[6] UU PDP ini merupakan pencapaian signifikan dalam sistem peraturan perundang-undangan Indonesia yang selama bertahun-tahun memerlukan kerangka hukum komprehensif mengenai perlindungan data pribadi.

Namun, efektivitas kerangka hukum ini menghadapi ujian nyata ketika terjadi insiden kebocoran masif data 341.000 personel Polri oleh aktor siber bernama Bjorka pada Oktober 2025.[7] Insiden ini tidak sekadar mengekspos kerentanan teknis sistem keamanan siber di lembaga penegak hukum, tetapi juga menimbulkan pertanyaan mendalam tentang kesiapan Indonesia dalam mengimplementasikan UU PDP secara efektif dan konsisten di tingkat eksekusi.[8] Data yang bocor mencakup informasi sensitif seperti nama lengkap, pangkat/jabatan, nomor ponsel, alamat email, dan dalam beberapa kasus, informasi lokasi personel.[9]

Ironi yang muncul adalah bahwa lembaga yang seharusnya memimpin dalam melindungi data warga negara justru menjadi korban pelanggaran keamanan siber yang masif. Paradoks ini mencerminkan kesenjangan signifikan antara norma hukum yang telah ditetapkan dan kapasitas implementasi di lapangan.[10] Kebocoran data Polri bukan hanya isu privasi individual, tetapi juga isu keamanan nasional yang strategis dengan implikasi jangka panjang bagi kedaulatan informasi nasional.

---

[6] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, UU No. 27 Tahun 2022, LN Tahun 2022 No. 196, TLN No. 6820, Ps.1.

[7] Bangbara.com, *Setelah Polisi Tangkap Bjorka, 341 Ribu Data Anggota Polri Bocor*, diakses dari https://www.bangbara.com/hukum/36916045040/setelah-polisi-tangkap-bjorka-341-ribu-data-anggota-polri-bocor-publik-pertanyakan-siapa-hacker-sebenarnya, diakses pada 29 Desember 2025.

[8] D. Prasetyo, *Legal Consequences of Data Breach for Data Controller under Indonesia's Personal Data Protection Law*, Journal of Indonesian Legal Studies, Vol.7, No.2 (November 2022), p.315.

[9] Jabar Ekspres, *Polisi Klaim Tangkap Bjorka, Tapi 341 Ribu Data Anggota Polri Diobrak-abrik*, diakses dari https://jabarekspres.com/berita/2025/10/07/polisi-klaim-tangkap-bjorka-tapi-341-ribu-data-anggota-polri-diobrak-abrik-tangkap-aku-di-mimpimu/, diakses pada 29 Desember 2025.

[10] A. Satriatama, *Effectiveness of Personal Data Protection Law Implementation in Indonesian Government Sector*, Jurnal Hukum dan Kebijakan Publik, Vol.5, No.1 (Oktober 2022), p.30.

Signifikansi penelitian ini terletak pada urgensi untuk memahami kelemahan sistemik dalam sistem perlindungan data pribadi melalui studi kasus konkret yang memiliki implikasi langsung terhadap keamanan nasional dan kepercayaan publik terhadap institusi negara.[11] Penelitian ini menggunakan pendekatan yuridis normatif dengan fokus pada analisis mendalam terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan studi kasus melalui kerangka teori sistem hukum Lawrence M. Friedman. Berdasarkan latar belakang tersebut, penelitian ini merumuskan tiga permasalahan utama:

1. Bagaimanakah kelemahan struktur kelembagaan perlindungan data pribadi Indonesia berkontribusi terhadap terjadinya kebocoran data personel Polri, dan apa yang menjadi penyebab utama dan faktor-faktor teknis dan organisasional?
2. Sejauh manakah dampak kebocoran data ini mempengaruhi dimensi keamanan nasional, kepercayaan publik terhadap institusi negara, dan legitimasi implementasi UU PDP di level praktis?
3. Bagaimanakah rekomendasi kebijakan dapat dioptimalkan melalui pendekatan hukum, kelembagaan, dan budaya keamanan data yang komprehensif untuk mencegah terulangnya insiden serupa?

B. PEMBAHASAN

1. Kerangka Teori Sistem Hukum Lawrence M. Friedman dan Aplikasinya

Lawrence M. Friedman mengembangkan model sistem hukum yang komprehensif melalui analisis mendalam terhadap dinamika hukum dalam masyarakat modern dan kompleks.[12] Menurut Friedman, sistem hukum terdiri dari tiga pilar utama yang saling terkait dan interdependen: struktur institusi, substansi norma hukum, dan budaya hukum.[13]

---

[11] Lawrence M. Friedman, *The Legal System: A Social Science Perspective*, Russell Sage Foundation, New York, 1975, p.15.
[12] Lawrence M. Friedman, *The Legal System: A Social Science Perspective*, p.20
[13] *Ibid.,* p.22.

Ketiga pilar ini berfungsi secara sinergis dalam menciptakan, menegakkan, dan mengimplementasikan hukum di dalam masyarakat, sehingga kelemahan pada salah satu pilar dapat mempengaruhi efektivitas seluruh sistem hukum.[14]

Pertama, struktur institusi mencakup lembaga-lembaga yang bertanggung jawab untuk membentuk, menegakkan, dan mengawasi pelaksanaan hukum. Dalam konteks perlindungan data pribadi Indonesia, struktur institusi meliputi Komisi Perlindungan Data Pribadi (KPDP), Kementerian Komunikasi dan Informatika, Badan Siber dan Sandi Negara (BSSN), Kepolisian Negara Republik Indonesia (Polri), Kejaksaan Agung, Pengadilan Negeri, dan berbagai lembaga sektoral yang mengelola data pribadi.[15] Efektivitas struktur ini bergantung pada kapasitas SDM, koordinasi antar lembaga, ketersediaan sumber daya, dan mekanisme akuntabilitas yang jelas.

Kedua, substansi norma hukum mencakup aturan-aturan, prinsip-prinsip, dan ketentuan-ketentuan yang mengatur perilaku dan hubungan hukum. Dalam perlindungan data pribadi, substansi meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah tentang Penyelenggaraan Keamanan Siber, dan berbagai regulasi sektoral yang mengatur keamanan dan pengelolaan data.[16] Substansi regulasi harus jelas, konkrit, dan spesifik untuk memandu implementasi di lapangan.

Ketiga, budaya hukum mencerminkan nilai-nilai, sikap, kesadaran, dan kebiasaan yang berkembang dalam masyarakat luas dan di kalangan aparatur pemerintah dalam menjalankan kewajiban hukum. Dalam konteks perlindungan data pribadi, budaya hukum meliputi tingkat kesadaran publik tentang pentingnya keamanan data, kepatuhan terhadap regulasi, adopsi praktik-praktik terbaik (*best practices*) dalam pengelolaan data, serta mindset dan komitmen aparatur negara terhadap keamanan siber nasional.[17]

---

[14] Hans Kelsen, *Pure Theory of Law*, University of California Press, Berkeley, 1967, p.45.

[15] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, UU No. 27 Tahun 2022, Ps.1 angka 5.

[16] Indonesia, *Undang-Undang tentang Informasi dan Transaksi Elektronik*, UU No. 11 Tahun 2008, LN No. 58, TLN No. 4843, Ps.28.

[17] S. Arifin, dkk., *Cyber Security Culture in Indonesian Government Agencies: Challenges and Policy Recommendations*, p.95.

2. Kronologi Kebocoran Data Polri dan Data Pemerintah

Peristiwa kebocoran data Polri dimulai dengan penangkapan pertama oleh Polda Metro Jaya terhadap pemuda berinisial WFT pada tanggal 23 September 2025 di Minahasa, Sulawesi Utara.[18] Tersangka diduga melakukan akses ilegal terhadap sistem perbankan dan infrastruktur digital milik entitas lain. Namun, kurang dari dua minggu setelah penangkapan, pada tanggal 4-5 Oktober 2025, data 341.000 personel Polri mulai beredar di forum-forum gelap internet (*dark web*) dengan menggunakan akun bernama "Bjorka".[19]

Data yang bocor mencakup informasi sensitif dengan tingkat kerahasiaan tinggi, meliputi nama lengkap personel, pangkat/jabatan, nomor ponsel aktif, alamat email, dan dalam beberapa kasus, informasi tentang penempatan dan unit tugas.[20] Verifikasi dilakukan oleh spesialis keamanan siber independen Alfons Tanujaya yang mengkonfirmasi bahwa data yang dibagikan merupakan data valid dan autentik, meskipun merupakan data historis dari periode 2016-2017.[21]

Adapun Kasus Kebocoran Data Platform Pemerintah Indonesia lainnya yaitu:

a. Kebocoran Data Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan
   Pada bulan Mei 2021, situs Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan mengalami peretasan yang mengakibatkan data pribadi 279 juta orang Indonesia dibocorkan dan dijual di forum online Raid Forums dengan harga 0,15 Bitcoin atau setara 230 juta Rupiah kurs Desember 2025.[22] Insiden ini menunjukan beberapa poin kritis yakni:

---

[18] Pusiknas Polri, *Hacker Berusia 22 Tahun Ditangkap*, diakses dari https://pusiknas.polri.go.id/detail_artikel/hacker_berusia_22_tahun_ditangkap_setelah_retas_data_bank, diakses pada 26 November 2025.

[19] Bangbara.com, *Setelah Polisi Tangkap Bjorka, 341 Ribu Data Anggota Polri Bocor.*

[20] Jawa Pos, *Bjorka Klaim Belum Ditangkap Polisi, Kini Bocorkan 341 Ribu Data Personel Polri*, diakses dari https://www.jawapos.com/kasuistika/016664349/bjorka-klaim-belum-ditangkap-polisi-kini-bocorkan-341-ribu-data-personel-polri, diakses pada 26 November 2025.

[21] Katadata, *Ahli IT Sebut Data 341 Ribu Personel Polri Valid*, diakses dari https://katadata.co.id/digital/teknologi/68e35760e5acf/ahli-it-sebut-data-341-ribu-personel-polri-yang-disebar-bjorka-valid, diakses pada 26 November 2025.

[22] Tempo, *3 Kasus Kebocoran Data Aplikasi atau Situs Milik Pemerintah*, diakses dari https://www.tempo.co/digital/3-kasus-kebocoran-data-aplikasi-atau-situs-milik-pemerintah-477847, diakses pada 26 November 2025.

1) Skala Dampak Masif: Data yang bocor mencakup hampir seluruh populasi Indonesia, termasuk data orang yang sudah meninggal, menunjukkan ketiadaan mekanisme data *cleansing* dan *quality control* yang memadai.
2) Inisiatif Respons: Kementerian Komunikasi dan Informatika kemudian memblokir situs Raid Forums, tetapi tindakan ini bersifat reaktif setelah kebocoran sudah terjadi, bukan preventif.
3) Implikasi Hukum: Insiden BPJS menunjukkan bahwa meskipun pada saat itu UU PDP belum disahkan (diundangkan Oktober 2022), ketiadaan regulasi yang komprehensif tidak menjadi penghalang bagi lembaga untuk kelalaian dalam menjaga keamanan data.[23]

b. Kebocoran Data Daftar Pemilih Tetap (DPT) dan Data Kependudukan

Pada 21 Mei 2020, pemilik akun @underthebreach mengungkapkan temuan kebocoran Data Pemilih Tetap KPU 2014, di mana 2,3 juta data kependudukan milik warga Indonesia dilaporkan bocor dan dibagikan lewat forum komunitas hacker dalam bentuk file berformat PDF.[24] Data yang terekspos meliputi:

1) Nama lengkap
2) Nomor Kartu Keluarga (KK)
3) Nomor Induk Kependudukan (NIK)
4) Tempat dan tanggal lahir
5) Alamat rumah
6) Berbagai data pribadi lainnya

Lebih mengkhawatirkan lagi, hacker dalam kasus ini mengklaim masih memiliki sebanyak 200 juta data warga Indonesia yang akan dibocorkan di forum tersebut. Insiden ini mengungkapkan bahwa infrastruktur penyimpanan data nasional rentan terhadap akses tidak sah, dan data historis dari proses pemilihan yang sudah selesai masih tersimpan tanpa protokol penghapusan yang jelas.

---

[23] Indonesia, *Undang-Undang tentang Informasi dan Transaksi Elektronik*, UU No. 11 Tahun 2008, LN Tahun 2008 No. 58, TLN No. 4843, Ps.28.

[24] BINUS, *Kebocoran Data Nasional Sebanyak 210 Instansi Kena Bobol*, diakses dari https://sis.binus.ac.id/2024/11/12/kebocoran-data-nasional-sebanyak-210-instansi-kena-bobol/, diakses pada 26 November 2025.

c. Kebocoran Data Direktorat Jenderal Pajak

Pada September 2024, Indonesia mengalami insiden signifikan di mana data pribadi sekitar 6 juta wajib pajak terekspos, termasuk data Presiden Joko Widodo.20 Informasi yang bocor mencakup:

1) Nomor Pokok Wajib Pajak (NPWP)

2) Nomor Induk Kependudukan (NIK)

3) Informasi akun bank dan transaksi finansial

4) Data penghasilan dan profil ekonomi

Dengan terbukanya data pajak, risiko serangan phishing dan penipuan identitas meningkat secara signifikan. Penyerang dapat menggunakan kombinasi NIK dan NPWP untuk melakukan fraud finansial, membuka akun kredit atas nama korban, atau melakukan rekayasa sosial yang lebih rumit.[25]

d. Kebocoran Data Pemilih Pemilu 2024 - Oktober 2024

Semua bermula saat peretas anonim bernama "Jimbo" mengaku telah meretas situs KPU dan mendapatkan data pemilih. Dalam unggahannya, diungkapkan bahwa dari 252 juta data yang diperoleh, beberapa terduplikasi. Penyaringan menghasilkan 204.807.203 data unik. Angka tersebut hampir sama dengan jumlah pemilih dalam daftar pemilih tetap KPU, yang mencapai 204.807.222 pemilih dari 514 kabupaten dan kota di Indonesia serta 128 negara perwakilan (liputan6.com, 30 November 2023)

Data pemilih yang bocor ini berpotensi disalahgunakan untuk: Iklan yang ditargetkan dan manipulasi kampanye politik untuk keperluan Pengumpulan intelijen Kampanye rekayasa sosial dengan presisi tinggi pelecehan dan intimidasi terhadap kelompok pemilih tertentu.[26]

---

[25] A. R. Hakim, dkk., *A Novel Digital Forensic Framework for Data Breach Investigation: Application in Enterprise Security*, IEEE Access, Vol.11, (April 2023), p.42655.

[26] S. Arifin, dkk., *Cyber Security Culture in Indonesian Government Agencies: Challenges and Policy Recommendations*, p.100-110.

3. Analisis Faktor-Faktor Teknis Penyebab Kebocoran Data

a) Infrastruktur Teknologi *Legacy* dan Tidak Terupdate

Sistem informasi Polri menggunakan infrastruktur teknologi lama yang tidak kompatibel dengan standar keamanan siber modern dan *best practices* internasional.[27] Arsitektur sistem yang usang membuat sistem rentan terhadap eksploitasi kerentanan yang sudah diketahui luas. Upgrade infrastruktur memerlukan investasi finansial yang besar, sehingga banyak lembaga pemerintah menunda modernisasi dan terus menggunakan sistem yang sudah berusia puluhan tahun.[28] Kombinasi faktor usia sistem dan ketiadaan update keamanan menciptakan kondisi ideal bagi penyerang untuk memanfaatkan celah keamanan.

b) Manajemen Patch dan Update Keamanan Tidak Optimal

Penerapan patch keamanan dan update keamanan dilakukan secara tidak konsisten dan sering tertinggal dari rilis update terbaru dari vendor penyedia teknologi.[29] Gap ini menciptakan jendela peluang bagi penyerang untuk memanfaatkan kelemahan yang sudah diketahui. Adapun yang menyebabkan ini adalah Kurangnya budget untuk maintenance dan keterbatasan SDM yang terlatih dalam *patch management* menjadi alasan utama lambatnya penerapan update keamanan.

c) Segmentasi Jaringan dan Kontrol Akses Lemah

Database personel tidak tersegmentasi dengan baik dari sistem lainnya, memungkinkan penyerang yang berhasil menembus pertahanan awal untuk melakukan *lateral movement* ke seluruh infrastruktur jaringan.[30] Kontrol akses tidak menerapkan prinsip "*least privilege*" secara konsisten, di mana setiap user diberikan akses lebih luas dari yang sebenarnya diperlukan.

d) Monitoring dan Deteksi Ancaman Tidak Memadai

Sistem monitoring keamanan jaringan (SIEM) tak memiliki kapabilitas deteksi dini yang memadai terhadap aktivitas mencurigakan atau eksploitasi kelemahan.[31]

---

[27] *Ibid.*, p.102.

[28] Ridho Aminullah dan Devi Purnama, *Manajemen Risiko Keamanan Siber bagi Institusi Pemerintah: Framework dan Best Practices*, Penerbit Universitas Airlangga, Surabaya, 2023, p.89-95.

[29] *Ibid.*, p.104.

[30] *Ibid.*, p.106.

[31] National Institute of Standards and Technology, *NIST Cybersecurity Framework Version 1.1*, NIST, Gaithersburg, MD, 2018, p.25.

Dalam banyak kasus kebocoran data baru diketahui beberapa bulan atau bahkan bertahun-tahun setelah penyerang berhasil menembus sistem. Respons terhadap insiden keamanan juga terlambat karena ketiadaan respon insiden tim yang terlatih dan terstruktur.[32] Lembaga pemerintah sering tidak memiliki prosedur yang jelas untuk menangani insiden keamanan, sehingga ketika kebocoran terdeteksi waktu terbuang untuk memahami *scope* dan dampak insiden.

e) Budaya Keamanan Siber Lemah di Seluruh Organisasi

Budaya keamanan siber belum menjadi prioritas utama dalam organisasi Polri, dengan rendahnya kesadaran personel terhadap pentingnya keamanan data dan keamanan informasi.[33] Pelatihan keamanan siber yang terbatas dan tidak berkelanjutan menyebabkan personel tidak terlatih dalam mengenali dan mengatasi ancaman keamanan siber. Ketiadaan budaya "*security awareness*" yang kuat menjadikan manusia sebagai titik lemah dalam keamanan siber organisasi.

f) Celah Keamanan Aplikasi dan Protokol Transmisi Data

Banyak aplikasi pemerintah yang dikembangkan tanpa menerapkan secure coding practices dan security testing yang memadai.[34] Celah keamanan aplikasi seperti SQL *injection*, *cross-site scripting* (XSS), dan *weak authentication mechanisms* sering tidak diidentifikasi sebelum aplikasi di-*deploy* ke *production environment*. Transmisi data antara sistem juga sering tidak menggunakan enkripsi yang kuat atau protokol yang aman.[35] Penggunaan HTTP (bukan HTTPS) untuk transmisi data sensitif masih ditemukan di beberapa aplikasi pemerintah, memungkinkan penyerang untuk melakukan serangan dan penyadapan data.

4. Analisis Normatif: Kewajiban Pengelola Data Berdasarkan UU PDP dan UU ITE

Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, setiap lembaga pemerintah pengelola data pribadi, termasuk Polri,

---

[32] Bambang Susanto, dan Sigit Priyanto, *Forensik Digital dan Investigasi Cybercrime: Studi Kasus dan Praktik Terbaik di Indonesia*, PT Penerbit Elex Media Komputindo, Jakarta, 2023, p.267-275

[33] S. Arifin, dkk., *Cyber Security Culture in Indonesian Government Agencies: Challenges and Policy Recommendations*, p.110.

[34] Agus Purwono, *Cyber Law: Aspek Data Privasi Edisi Revisi*, Refika Editama, Jakarta, 2022, p.145-156.

[35] DLAPiper, *Data Protection Laws in Indonesia*, diakses dari https://www.dlapiperdataprotection.com, p.35.

BPJS, KPU, Direktorat Jenderal Pajak, dan lembaga pemerintah lainnya memiliki status hukum sebagai Pengendali Data Pribadi (*Data Controller*) dengan kewajiban-kewajiban yuridis yang spesifik dan dapat dipaksakan secara hukum. Pemerintah yang lalai dalam mengelola data pribadi akan dikenakan sanksi berdasarkan UU PDP, berupa Sanksi Administratif bagi institusi dan potensi Sanksi Pidana bagi pejabat yang bertanggung jawab, serta kewajiban untuk membayar Ganti Rugi kepada korban. Pasal 12 ayat (1) UU PDP secara jelas memberikan hak kepada Subjek Data Pribadi: "Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan." Meskipun UU PDP tidak merinci jenis kerugian yang dapat dituntut, frasa "ganti rugi" dalam hukum perdata Indonesia (KUHPerdata) sudah mencakup kerugian materiil dan imateriil. Hal ini memastikan bahwa korban dapat menuntut kompensasi atas segala bentuk dampak buruk yang dialami, baik yang berbentuk uang maupun yang bersifat mental/psikologis, akibat kelalaian Pengendali Data Pribadi (termasuk pemerintah).

a. Kewajiban Keamanan Data (Pasal 5 huruf d dan Pasal 54 UU PDP dan UU ITE Pasal 30 Ayat (1)

Polri harus menjamin keamanan, integritas, dan kerahasiaan data pribadi melalui implementasi teknis dan organisasional yang memadai.[36] Kewajiban ini mencakup pengimplementasian enkripsi, *access control*, *audit trails*, dan mekanisme keamanan lainnya yang sesuai dengan standar industri dan regulasi yang berlaku. Analisis Terhadap Kasus Kebocoran Pasal 54 UU PDP mewajibkan pengendali data untuk "menyelenggarakan sistem pengamanan Data Pribadi yang menggunakan teknologi terkini."[37] Penggunaan sistem *legacy* yang usang oleh Polri jelas melanggar ketentuan ini. Standar keamanan internasional seperti ISO/IEC 27001:2013 dan *NIST Cybersecurity Framework* secara eksplisit mengharuskan penggunaan teknologi keamanan yang *up-to-date* dan sesuai dengan *risk profile* organisasi. [38]

---

[36] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, UU No. 27 Tahun 2022, Ps. 5 huruf d.

[37] *Ibid.,* Ps.5 huruf d dan Ps.54.

[38] ISO/IEC, *Information Security Management Systems - Requirements (ISO/IEC 27001:2022)*, ISO dan IEC, Geneva, 2022, p.42-48.

Pasal 30 ayat (1) UU ITE mengatur larangan akses ilegal terhadap sistem elektronik, yaitu "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun", dengan ancaman pidana penjara maksimal 6 tahun dan/atau denda Rp600 juta (Pasal 46 ayat (1)). Intinya, pasal ini melarang peretasan atau pembobolan sistem elektronik milik orang lain tanpa izin, seperti mencuri data atau informasi.

b. Kewajiban Akuntabilitas (Pasal 5 huruf f UU PDP dan UU ITE Pasal 32)

Polri harus dapat membuktikan dan mendemonstrasikan bahwa telah melakukan pemrosesan data pribadi sesuai dengan prinsip-prinsip yang diatur dalam UU PDP.[39] Akuntabilitas ini mencakup dokumentasi mengenai dasar hukum pemrosesan, tujuan pemrosesan, kategori emilik data, dan mekanisme perlindungan yang diimplementasikan.

Analisis Terhadap Kasus Kebocoran: Respon Polri yang cenderung defensif dan kurang transparan pasca kebocoran data, seperti menyebutkan bahwa "data yang bocor adalah data lama dari 2017" bertentangan dengan semangat akuntabilitas ini.[40] Dalam perspektif hukum perlindungan data, konsep "data lama" tidak meringankan tanggung jawab selama data tersebut masih merupakan data pribadi. Sejalan dengan prinsip GDPR yang juga diadopsi UU PDP, kewajiban untuk melindunginya tetap berlaku dengan sepenuhnya, terlepas dari kapan data tersebut dikumpulkan.[41]

Prinsip akuntabilitas dalam Pasal 5 huruf f mengharuskan setiap pengendali data untuk memiliki dokumentasi yang jelas tentang:

1) Inventaris data pribadi yang dimiliki
2) Sistem penyimpanan dan lokasi data
3) Mekanisme keamanan yang diterapkan
4) Riwayat akses data
5) Insiden keamanan yang telah terjadi

---

[39] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, UU No. 27 Tahun 2022, Ps. 5 huruf f.

[40] D. Prasetyo, *Op.Cit.,* p.325-330.

[41] Hardi Sudarsono, *GDPR dan Implementasinya: Perlindungan Data Pribadi dalam Era Digital*, Penerbit Deepublish, Yogyakarta, 2022, p.102-107

Ketiadaan dokumentasi yang memadai tentang kebocoran data Polri menunjukkan kegagalan dalam menerapkan prinsip akuntabilitas ini.[42]

Pasal 32 UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) mengatur larangan bagi setiap orang untuk mengubah, menambah, mengurangi, merusak, menghilangkan, memindahkan, atau menyembunyikan Informasi Elektronik (IE) dan/atau Dokumen Elektronik (DE) milik orang lain atau publik secara sengaja, tanpa hak, atau melawan hukum, serta larangan memindahkan data ke sistem orang lain yang tidak berhak, dengan ancaman pidana penjara hingga 10 tahun dan/atau denda hingga Rp5 miliar untuk pelanggaran ayat (3). Pasal ini penting untuk melindungi privasi dan keamanan data pribadi di ranah digital.

c. Kewajiban Notifikasi Pelanggaran Data (Pasal 46 UU PDP)

Dalam hal terjadi pelanggaran keamanan data, Polri wajib memberitahukan kepada setiap Pemilik Data Pribadi yang terdampak dalam waktu paling lama 72 (tujuh puluh dua) jam setelah kebocoran diketahui.[43] Notifikasi harus memuat informasi mengenai jenis data yang bocor, mekanisme kebocoran, dampak potensial, dan langkah-langkah remedial yang sedang dilakukan.

1) Analisis terhadap Kasus Kebocoran:

Dalam kasus kebocoran data Polri, notifikasi kepada 341.000 personel terdampak lambat dan tidak transparan. Beberapa personel bahkan mengetahui tentang kebocoran data mereka melalui media massa daripada melalui komunikasi resmi dari Polri. Hal ini jelas melanggar kewajiban dalam Pasal 46 yang mengharuskan notifikasi dalam *window* waktu 72 jam.

Notifikasi yang transparan dan cepat adalah kewajiban mandatori yang tidak dapat dikurangi atau ditawar-tawar. Keterlambatan dalam memberitahu data subjek tentang kebocoran mencegah mereka mengambil tindakan preventif untuk melindungi diri mereka dari potensi penyalahgunaan data (seperti *fraud*, *phishing*, atau *identity theft*).

---

[42] A. Satriatama, *Effectiveness of Personal Data Protection Law Implementation in Indonesian Government Sector*, p.330-335.

[43] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi*, UU No. 27 Tahun 2022, Ps.46.

d. Kewajiban Pemeliharaan dan Pencegahan (Pasal 5 Umum dan Pasal 54 PDP dan UU ITE Pasal 32)

Substansi Normatif: Menurut Pasal 34 UU PDP, penilaian dampak perlindungan data pribadi dilakukan untuk mengevaluasi potensi risiko yang timbul dari suatu pemrosesan data pribadi serta upaya atau langkah yang harus dilakukan untuk memitigasi risiko.[44] Data personel Polri, mengingat sifatnya yang sensitif dan berpotensi risiko tinggi (*high-risk processing*), seharusnya telah melalui DPIA yang komprehensif. DPIA yang baik harus mengidentifikasi: Jenis data pribadi yang diproses (sensitif, biometric, lokasi, dll) Teknologi yang digunakan untuk menyimpan dan memproses data Potensi risiko kepada data subjek (*privacy violation*, *discrimination*, dll) Kesalahan sistem yang dapat terjadi dampak potensial terhadap keamanan nasional atau keamanan publik Mitigasi risiko yang diperlukan Ketiadaan atau ketidakadekuatan DPIA merupakan indikasi bahwa Polri tidak sepenuhnya memahami dan mengimplementasikan kewajiban-kewajiban yang diatur dalam UU PDP.[45] Pasal 34 mengharuskan bahwa sebelum pemrosesan data berisiko tinggi dimulai, DPIA harus sudah dilakukan dan dokumentasi harus tersedia untuk keperluan akuntabilitas.[46] Adapun kewajiban Penyelenggara Sistem elektronik yaitu diatur dalam pasal 28 ayat 3 mewajibkan perlindungan lima aspek keamanan yaitu 1) Ketersediaan: Sistem dan data dapat diakses oleh pemilik atau pihak berwenang kapan pun diperlukan tanpa gangguan yang tidak direncanakan, 2) keutuhan: Data pribadi tidak mengalami perubahan, penghapusan, atau modifikasi yang tidak sah selama disimpan atau ditransmisikan, 3) Keotentikan: Verifikasi bahwa data berasal dari sumber yang *legitimate* dan identitas pengguna dapat terverifikasi dengan akurat, 4). Kerahasiaan: Proteksi data pribadi dari akses tidak sah melalui enkripsi, kontrol akses, dan mekanisme keamanan lainnya, dan 5) Keteraksesan: Jaminan bahwa data pribadi dapat diakses oleh pemilik dalam format yang dapat dipahami sesuai hak-hak dalam UU PDP. Berdasarkan UU ITE Pasal 32 berkaaitan dengan sanksi terhadap modifikasi dan perubahan data yang dilakukan oleh setiap orang

[44] Indonesia, *Undang-Undang tentang Perlindungan Data Pribadi, UU No. 27 Tahun 2022*, Ps. 34.

[45] *Ibid.*

[46] ISO/IEC, *Information Security Management Systems - Requirements (ISO/IEC 27001:2022),* p.22-28.

dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi elektronik milik orang lain atau publik dikenakan Sanksi Pidana penjara paling lama 8 (delapan) tahun atau denda paling banyak 800 juta.

5. Implikasi Keamanan Nasional dan Dampak Multidimensional

Kebocoran data Polri dan data Pemerintah melampaui permasalahan privasi individual dan berkembang menjadi isu keamanan nasional yang strategis dengan implikasi jangka panjang. Data personel polisi yang bocor memiliki nilai intelijen tinggi bagi berbagai aktor ancaman.[47] Adapun ini sebagai bukti kelemahan sektor perlindungan data pribadi yang ada di Indonesia yang menyebabkan kepercayaan publik terhadap lembaga pemerintahan menurun drastis sehingga memerlukan transformasi digital pemerintah secara keseluruhan guna memperbaiki citra kepercayaan masyarakat terhadap keamanan dan integritas sistem digital pemerintah.

6. Rekomendasi Kebijakan dan Strategi Pencegahan Komprehensif

Untuk mencegah terulangnya insiden kebocoran data serupa dan memperkuat sistem perlindungan data pribadi nasional, diperlukan strategi pencegahan yang komprehensif mencakup ketiga pilar sistem hukum Lawrence M. Friedman yaitu Struktur, Subtansi, dan Budaya.

Analisis terhadap kasus-kasus kebocoran data yang telah menimpa institusi pemerintah Indonesia seperti kebocoran data BPJS Kesehatan (279 juta *records* pada 2021), Direktorat Jenderal Pajak (6 juta records pada 2024), dan Polri (341 ribu personel pada 2025) menunjukkan bahwa Indonesia memiliki kelemahan sistemik pada ketiga pilar secara simultan: struktur kelembagaan yang fragmentasi, substansi norma hukum yang abstrak, dan budaya hukum yang belum matang.

Sebagai saran dari pilar struktur : Mungkin bisa melakukan pembentukan Komisi Perlindungan Data Pribadi (KPDP) yang mandiri dan berwenang untuk melakukan investigasi serta menjatuhkan sanksi administratif hingga Rp100 miliar kepada *data controller* yang melanggar kewajiban perlindungan data,

[47] BSSN, *Lanskap Keamanan Siber Indonesia 2024: Tren Ancaman dan Strategi Respons*, BSSN, Jakarta, 2024, p.68-75.

dengan independensi penuh dari eksekutif dan reporting langsung kepada Presiden.

Sebagai saran dari pilar substansi : Penyusunan Peraturan Pemerintah dan Peraturan Menteri per sektor (Kepolisian, Kesehatan, Keuangan, Pendidikan) yang mengoperasionalisasi *security standards* sektor-spesifik. Ketiga, harmonisasi regulasi lintas sektor untuk menciptakan kohesi dalam definisi data pribadi, standar keamanan, dan mekanisme *breach notification* di berbagai undang-undang sektor.

Sebagai saran dari pilar budaya : Program kesadaran keamanan siber dari diri sendiri sehingga kita lebih *awareness* terhadap data pribadi, dan pelaporan insiden jika memang ada indikasi bahwa data pribadi disalahgunakan atau diretas oleh pihak lain, adanya konsekuensi terhadap lembaga yang lalai atas perlindungan data pribadi.

C. PENUTUP

Berdasarkan analisis komprehensif menggunakan kerangka teori sistem hukum Lawrence M. Friedman, penelitian ini menyimpulkan bahwa sistem perlindungan data pribadi Indonesia mengalami kelemahan sistemik yang multidimensional dan memerlukan *respons integrated*. Kelemahan tersebut menyentuh ketiga pilar sistem hukum secara simultan: Pertama, struktur kelembagaan perlindungan data pribadi masih belum optimal dengan kapasitas SDM yang terbatas, koordinasi antarlembaga yang kurang efektif, dan mekanisme akuntabilitas yang perlu diperkuat. Kedua, substansi regulasi UU PDP masih bersifat abstrak dan memerlukan peraturan pelaksana yang lebih konkrit, spesifik, dan operasional untuk membimbing implementasi di lapangan. Ketiga, budaya keamanan data dan keamanan siber belum tertanam dengan kuat di seluruh institusi publik Indonesia, dengan tingkat kesadaran yang masih rendah tentang pentingnya keamanan informasi.

Kasus kebocoran data Polri dan data Pemerintah telah mendemonstrasikan dengan jelas bahwa meskipun UU PDP telah disahkan dan memberikan kerangka hukum yang komprehensif, efektivitasnya dalam praktik masih jauh dari optimal.

Insiden ini mengungkapkan gap yang signifikan antara norma hukum yang telah ditetapkan dengan implementasi praktis di lapangan, yang disebabkan oleh kombinasi faktor: keterbatasan kapasitas institusi dan SDM, ketiadaan peraturan pelaksana yang spesifik dan operasional, infrastruktur teknologi yang usang dan tidak terbarui, serta budaya organisasi yang belum sepenuhnya mengadopsi keamanan siber sebagai prioritas strategis.

Pencegahan terhadap kebocoran data di masa depan dan penguatan perlindungan data pribadi nasional harus bersifat komprehensif dan mencakup aspek hukum, teknologi, organisasi, dan budaya secara terintegrasi. Solusinya yaitu melibatkan komitmen kepemimpinan yang kuat, investasi sumber daya yang berkelanjutan dan terukur, serta perubahan budaya organisasi yang mendalam di seluruh lembaga publik dan swasta yang mengelola data pribadi serta sanksi yang jelas terhadap lembaga publik yang lalai mengelola data pribadi masyarakat.

Diharapkan penelitian ini dapat memberikan kontribusi yang bermakna dalam pengembangan tata kelola perlindungan data pribadi dan keamanan siber nasional yang lebih kuat, efektif, dan berkelanjutan ke depan.

DAFTAR PUSTAKA

Buku

Aminullah, Ridho dan Devi Purnama. 2023. *Manajemen Risiko Keamanan Siber bagi Institusi Pemerintah: Framework dan Best Practices*. (Surabaya: Penerbit Universitas Airlangga).

BSSN. 2024. *Lanskap Keamanan Siber Indonesia 2024: Tren Ancaman dan Strategi Respons*. (Jakarta: BSSN).

Friedman, Lawrence M.. 1975. *The Legal System: A Social Science Perspective*. (New York: Russell Sage Foundation).

ISO/IEC. 2022. *Information Security Management Systems - Requirements (ISO/IEC 27001:2022).* (Geneva: International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC)).

Kalsen, Hans. 2014. *Teori Hukum Murni: Dasar-dasar Ilmu Hukum Normatif, Cetakan XVI, Terjemahan dari Pure Theory of Law*. (Bandung: Penerbit Nusa Media).

Kelsen, Hans. 1967. *Pure Theory of Law.* (Berkeley: University of California Press).

National Institute of Standards and Technology. 2018. *NIST Cybersecurity Framework Version 1.1*. (Gaithersburg, MD: NIST).

Notohamidjojo, O. 1974. *Soal-soal Pokok Filsafat Hukum*. (Jakarta: Sastra Hudaya).

Purwono, Agus. 2022. *Cyber Law: Aspek Data Privasi Edisi Revisi*. (Jakarta: Refika Editama).

Sudarsono, Hardi. 2022. *GDPR dan Implementasinya: Perlindungan Data Pribadi dalam Era Digital*. (Yogyakarta: Penerbit Deepublish).

Susanto, Bambang dan Sigit Priyanto. 2023. *Forensik Digital dan Investigasi Cybercrime: Studi Kasus dan Praktik Terbaik di Indonesia*. (Jakarta: PT Penerbit Elex Media Komputindo).

Warren, Samuel D. dan Louis D. Brandeis. 1890. *The Right to Privacy*. (Cambridge: Harvard Law School).

Publikasi

A. Satriatama, *Effectiveness of Personal Data Protection Law Implementation in Indonesian Government Sector.* Jurnal Hukum dan Kebijakan Publik. Vol.5, No.1 (2022), p.330-335.

Arifin, S. dkk.. *Cyber Security Culture in Indonesian Government Agencies: Challenges and Policy Recommendations*. Indonesian Journal of Cyber Security. Vol.21. No.2 (2023).

Hakim, A. R., dkk.. *A Novel Digital Forensic Framework for Data Breach Investigation: Application in Enterprise Security.* IEEE Access. Vol.11. (April 2023),

Prasetyo, D.. *Legal Consequences of Data Breach for Data Controller under Indonesia's Personal Data Protection Law*. Journal of Indonesian Legal Studies. Vol.7. No.2 (November 2022).

Satriatama, A.. *Effectiveness of Personal Data Protection Law Implementation in Indonesian Government Sector*. Jurnal Hukum dan Kebijakan Publik. Vol.5. No.1 (Oktober 2022).

Website

Bangbara.com. *Setelah Polisi Tangkap Bjorka, 341 Ribu Data Anggota Polri Bocor*. diakses dari https://www.bangbara.com/hukum/36916045040/setelah-polisi-tangkap-bjorka-341-ribu-data-anggota-polri-bocor-publik-pertanyakan-siapa-hacker-sebenarnya. diakses pada 26 November 2025.

BINUS. *Kebocoran Data Nasional Sebanyak 210 Instansi Kena Bobol.* diakses dari https://sis.binus.ac.id/2024/11/12/kebocoran-data-nasional-sebanyak-210-instansi-kena-bobol/. diakses pada 26 November 2025.

DLAPiper. *Data Protection Laws in Indonesia*. diakses dari https://www.dlapiperdataprotection.com. diakses pada 26 November 2025.

Jabar Ekspres. *Polisi Klaim Tangkap Bjorka, Tapi 341 Ribu Data Anggota Polri Diobrak-abrik.* diakses dari https://jabarekspres.com/berita/2025/10/07/polisi-klaim-tangkap-bjorka-tapi-341-ribu-data-anggota-polri-diobrak-abrik-tangkap-aku-di-mimpimu/. diakses pada 26 November 2025.

Jawa Pos. *Bjorka Klaim Belum Ditangkap Polisi, Kini Bocorkan 341 Ribu Data Personel Polri.* diakses dari https://www.jawapos.com/kasuistika/016664349/bjorka-klaim-belum-ditangkap-polisi-kini-bocorkan-341-ribu-data-personel-polri. diakses pada 26 November 2025.

Katadata. *Ahli IT Sebut Data 341 Ribu Personel Polri Valid*. diakses dari https://katadata.co.id/digital/teknologi/68e35760e5acf/ahli-it-sebut-data-341-ribu-personel-polri-yang-disebar-bjorka-valid. diakses pada 26 November 2025.

Pusiknas Polri. *Hacker Berusia 22 Tahun Ditangkap*, diakses dari https://pusiknas.polri.go.id/detail_artikel/hacker_berusia_22_tahun_ditangkap_setelah_retas_data_bank. diakses pada 26 November 2025.

Tempo. *3 Kasus Kebocoran Data Aplikasi atau Situs Milik Pemerintah*, diakses dari https://www.tempo.co/digital/3-kasus-kebocoran-data-aplikasi-atau-situs-milik-pemerintah-477847. diakses pada 26 November 2025.

Sumber Hukum

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.