Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

Dec 2025, Vol. 4, No. 1
e-ISSN: 3032-6591
pp 202-208

Analisis Kerentanan Siber Kebocoran Data Polri oleh Bjorka

Ilham Indra Mulya[1], Lazarus[2], Muhammad Dewanto Adi Saputra[3], Muhammad Rahmadzani Hidayat[4]
Fakultas Hukum, Universitas Pembangunan Nasional Veteran Jakarta
Email: 2210611071@mahasiswa.upnvj.ac.id, 2210611082@mahasiswa.upnvj.ac.id, 2210611086@mahasiswa.upnvj.acid, 2210611087@mahasiswa.upnvj.ac.id

Abstract: Kasus kebocoran data Polri oleh peretas bernama Bjorka pada tahun 2025 menyoroti lemahnya sistem keamanan siber di Indonesia, khususnya dalam pengelolaan data pribadi oleh lembaga negara. Kebocoran yang melibatkan data identitas personel Polri ini menjadi bukti bahwa kerentanan keamanan digital tidak hanya mengancam individu, tetapi juga institusi strategis negara. Penelitian ini bertujuan untuk menganalisis akar penyebab kebocoran, tanggung jawab hukum Polri sebagai pengendali data pribadi menurut Undang-Undang Perlindungan Data Pribadi (UU PDP), serta urgensi reformasi keamanan siber nasional. Metode yang digunakan adalah pendekatan yuridis normatif melalui analisis peraturan perundang-undangan, literatur akademik, serta penelusuran kasus. Hasil penelitian menunjukkan adanya ketidaksesuaian antara kewajiban normatif perlindungan data dengan implementasi teknis keamanan informasi. Penelitian ini menegaskan bahwa peningkatan keamanan siber membutuhkan pembaruan sistem, kompetensi SDM, dan penegakan hukum yang konsisten agar kejadian serupa tidak terulang dan kepercayaan publik terhadap negara dapat dipulihkan.

Abstract: *Technological development has transformed many aspects of human life and provided innovations that significantly improve efficiency and convenience. However, the rapid digitalization of society has increased the vulnerability of personal data to cyberattacks and unauthorized access. In Indonesia, public concern over data security escalated following a series of massive data breaches in August 2022, allegedly carried out by an anonymous hacker known as Bjorka. One of the most alarming incidents was the leakage of sensitive data belonging to the Indonesian National Police, revealing critical weaknesses in national cybersecurity systems.This case triggered public distrust and highlighted the urgent need for stronger data protection mechanisms at the state level. Although the government enacted Law Number 27 of 2025 on Personal Data Protection as a legal framework for safeguarding citizens' information, enforcement and implementation remain major challenges. This study aims to analyze the cybersecurity vulnerabilities exposed by the Polri data breach and evaluate Indonesia's readiness to respond to increasingly complex cyber threats. The research emphasizes the importance of strengthening cybersecurity infrastructure, improving digital literacy, and enhancing regulatory oversight to build a secure, transparent, and trustworthy digital ecosystem.*

Article History
Received: November 25, 2025
Revised: November 30, 2025
Published: December 5, 2025

Keywords :
Cybersecurity; Data Breach; Bjorka; Indonesian National Police; Personal Data Protection Law.

Kata Kunci:
Keamanan Siber; Kebocoran Data; Bjorka; Polri; Perlindungan Data Pribadi; UU PDP.

https://doi.org/10.5281/zenodo.17850680

PENDAHULUAN

Teknologi berdampak pada banyak aspek kehidupan di seluruh dunia, dan penemuan-penemuan baru yang dihasilkan oleh kemajuan teknis ini akan membuat hidup lebih mudah bagi masyarakat. Dunia maya, atau sekadar "ruang siber", adalah media elektronik yang merupakan bagian dari jaringan komputer global dan sering digunakan untuk komunikasi satu arah dan timbal balik berbasis telepon atau internet.[1] Namun, di balik kemudahan dan efisiensi yang ditawarkan dunia

[1]Ashilah, A. P., & Rahman, R. (2024). FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH BJORKA. *Jurnal Riset Sistem Informasi*, *1*(3), 17-26.

Dec 2025, Vol. 4, No. 1
e-ISSN: 3032-6591
pp 202-208

digital, terdapat tantangan besar yang terus mengancam isu keamanan siber dan perlindungan data pribadi. Seiring dengan meningkatnya ketergantungan masyarakat terhadap sistem digital, potensi kerentanan terhadap kebocoran dan penyalahgunaan data pribadi pun semakin tinggi. Di Indonesia, perhatian publik terhadap isu ini memuncak setelah terjadinya serangkaian kebocoran data besar-besaran yang dilakukan oleh aktor anonim bernama Bjorkapada Agustus tahun 2022. Salah satu kasus yang paling menyita perhatian adalah bocornya data kepolisian republik Indoneia.[2]

Peristiwa tersebut membuka mata publik bahwa bahkan lembaga negara yang memiliki sistem keamanan tinggi pun masih menyimpan celah yang dapat dimanfaatkan oleh peretas. Kebocoran data Polri pada tahun 2025 tidak hanya menimbulkan kekhawatiran mengenai keamanan informasi internal aparat penegak hukum, tetapi juga menimbulkan ketidakpercayaan masyarakat terhadap kemampuan negara dalam melindungi data pribadi warganya. Kasus ini menjadi momentum penting untuk mengevaluasi kesiapan Indonesia dalam menghadapi ancaman siber yang semakin kompleks dan dinamis di era digital.[3] Di tengah perkembangan teknologi yang begitu cepat, perlindungan data pribadi bukan sekadar persoalan teknis, melainkan juga terkait dengan tata kelola, regulasi, dan kesadaran masyarakat.

Pemerintah Indonesia sebenarnya telah merespons melalui penerbitan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), namun implementasi dan pengawasan masih menjadi tantangan besar. Oleh karena itu, diperlukan penguatan sistem keamanan siber yang komprehensif, peningkatan literasi digital, serta komitmen nyata dari pemerintah dan semua pihak untuk menciptakan ekosistem digital yang aman, transparan, dan dapat dipercaya.[4] Melihat berbagai peristiwa kebocoran data yang terjadi, termasuk kasus Bjorka yang menyeret institusi negara seperti Polri, jelas bahwa isu keamanan siber dan perlindungan data pribadi bukan lagi sekadar wacana teknis, melainkan telah menjadi persoalan strategis yang bersentuhan langsung dengan kepercayaan publik dan kedaulatan negara. Kelemahan dalam sistem keamanan digital dapat menimbulkan dampak yang sangat luas, mulai dari penyalahgunaan identitas, gangguan operasional lembaga negara, hingga potensi ancaman terhadap stabilitas nasional. Di tengah era digital yang terus berkembang, ketergantungan terhadap teknologi justru harus diimbangi dengan kesiapan sistem pertahanan siber yang kuat, terukur, dan berkelanjutan agar tidak terus menjadi sasaran kejahatan siber.

Oleh karena itu, penelitian mengenai kebocoran data Polri pada tahun 2025 menjadi sangat relevan untuk dilakukan guna menilai sejauh mana perlindungan data pribadi di Indonesia telah diterapkan dalam praktik, serta mengidentifikasi celah dan hambatan yang masih terjadi meskipun regulasi seperti UU PDP telah diberlakukan. Kajian ini diharapkan tidak hanya memberikan kontribusi teoritis bagi perkembangan ilmu hukum dan keamanan siber, tetapi juga mendorong formulasi kebijakan yang lebih responsif dan implementatif untuk memperkuat sistem keamanan digital lembaga negara. Dengan demikian, penelitian ini diharapkan mampu memberikan panduan strategis bagi pemerintah, institusi publik, maupun masyarakat dalam mewujudkan ekosistem teknologi yang aman, terpercaya, dan berorientasi pada perlindungan hak privasi setiap warga negara.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan yuridis-normatif dan studi kasus. Pendekatan yuridis-normatif digunakan untuk menelaah peraturan terkait keamanan siber dan

[2] Sabila, S. N., & Atman, W. (2025). Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik*, *2*(3), 142-154
[3] Hacker Berusia 22 Tahun Ditangkap Setelah Retas Data Bank," Pusiknas Bareskrim Polri, diakses 24 November 2025, https://pusiknas.polri.go.id/detail_artikel/hacker_berusia_22_tahun_ditangkap_setelah_retas_data_bank
[4] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

Dec 2025, Vol. 4, No. 1
e-ISSN: 3032-6591
pp 202-208

perlindungan data pribadi, sedangkan studi kasus difokuskan pada kebocoran data Polri tahun 2022 oleh Bjorka. Pengumpulan data dilakukan melalui studi kepustakaan dengan meninjau buku, jurnal, berita daring, dan dokumen resmi. Data dianalisis menggunakan analisis deskriptif-kualitatif untuk menggambarkan kesenjangan antara regulasi dan implementasinya dalam praktik perlindungan data di Indonesia.

HASIL DAN PEMBAHASAN

Bentuk Kebocoran Data POLRI Yang Dilakukan Bjorka

Kebocoran data POLRI yang dilakukan oleh Bjorka merupakan salah satu kasus peretasan data besar-besaran yang mengungkap kerentanan serius dalam pengelolaan keamanan data institusi negara di Indonesia. Bjorka mengklaim telah mengakses dan membocorkan data pribadi sekitar 341 ribu personel Polisi, yang mencakup data nama lengkap, pangkat, satuan tugas, serta kontak pribadi seperti nomor telefon dan email. Pembocoran ini dilakukan dengan mengekstrak data dalam format kompresi yang kemudian disebarluaskan melalui laman pribadi serta forum gelap di dunia maya sebagai bentuk protes atas klaim penangkapan dirinya oleh kepolisian.[5] Kebocoran ini terjadi karena lemahnya sistem keamanan data internal Polri yang seharusnya terlindungi dengan protokol keamanan yang ketat. Pakar keamanan siber menjelaskan bahwa data yang bocor tidaklah sekadar catatan administratif biasa, melainkan menyangkut informasi yang sangat sensitif yang dapat dimanfaatkan untuk tindakan kriminal maupun penyalahgunaan lain yang mengancam privasi dan keamanan individu maupun institusi. Kebocoran ini mencerminkan kegagalan dalam aspek tata kelola keamanan dan pengelolaan data negara.[6]

Dampak kebocoran data tersebut sangat luas, baik dari sisi privasi personel Polri maupun dari segi stabilitas institusi. Privasi individu yang tercermin dalam data yang bocor sangat rentan dieksploitasi oleh pihak tidak bertanggungjawab, sehingga dapat menimbulkan ancaman terhadap keselamatan personel Polri serta menurunkan kepercayaan publik terhadap institusi keamanan negara. Dari sudut pandang hukum, kebocoran ini juga membuka peluang pelanggaran terhadap Undang-Undang Perlindungan Data Pribadi yang wajib ditegakkan untuk menjaga integritas data pribadi.[7]

kebocoran ini mengindikasikan perlunya reformasi teknologi dan regulasi yang mengatur perlindungan data negara. Meski Polri dan institusi terkait mengklaim telah memiliki sistem proteksi data yang ketat, bukti kebocoran menunjukkan bahwa keamanan siber masih belum memadai sehingga memerlukan peningkatan kapasitas teknis dan penguatan regulasi yang mendukung penanganan kejahatan siber. Tindakan responsif dari pemerintah dan institusi terkait sangat penting untuk mencegah kejadian serupa berulang.[8]

Kasus ini juga menjadi refleksi kritis terkait pengawasan dan pengelolaan keamanan data negara yang selama ini mungkin kurang transparan dan belum teruji secara maksimal. Kebocoran oleh Bjorka menjadi tamparan keras terhadap klaim perlindungan data oleh instansi negara. Kritisnya situasi ini menuntut adanya evaluasi menyeluruh terhadap prosedur keamanan data, peningkatan kesadaran

[5] Tim Wartawan, "Hacker Bjorka Bocorkan Data 341 Ribu Personel Polri, Sistem Keamanan Negara Terancam," Suara Utama (7 Oktober 2025), diakses 24 November 2025, dari https://suarautama.id/hacker-bjorka-bocorkan-data-341-ribu-personel-polri-sistem-keamanan-negara-terancam/.
[6] *Tempo*, "Hacker Bjorka Membobol Data Pribadi 341 Ribu Personel Polri," *Tempo.co*, 4 Oktober 2025, diakses 24 November 2025, dari https://www.tempo.co/hukum/hacker-bjorka-membobol-data-pribadi-341-ribu-personel-polri-2076447.
[7] Wuwungan, M. S. S. (2024). PERLINDUNGAN HUKUM TERHADAP PEMILIK DATA PRIBADI PENGGUNA TEKNOLOGI INFORMASI AKIBAT TINDAK PIDANA PERETASAN. LEX PRIVATUM, 13(4). Hal. 8-9.
[8] Kompas.com, "Polisi Usut Dugaan Kebocoran Data 341 Ribu Personel oleh Bjorka," Kompas Megapolitan, 7 Oktober 2025, diakses 24 November 2025, dari https://megapolitan.kompas.com/read/2025/10/07/07492751/polisi-usut-dugaan-kebocoran-data-341-ribu-personel-oleh-bjorka.

Dec 2025, Vol. 4, No. 1
e-ISSN: 3032-6591
pp 202-208

tentang pentingnya keamanan data dalam konteks institusi negara, serta penegakan hukum yang tegas bagi pelaku kejahatan siber.[9]

Bjorka sendiri menggunakan media kebocoran data tersebut sebagai bentuk perlawanan terhadap aparat kepolisian, setelah adanya klaim penangkapan yang diklaimnya tidak sah atau tidak valid. Hal ini mengindikasikan dinamika baru dalam dunia siber, di mana aktor peretas tidak hanya sekadar mencari keuntungan material, tetapi juga mengekspresikan bentuk oposisi atau kritik terhadap institusi negara melalui metode digital. Dalam hal ini, kebocoran data tidak hanya dianggap sebagai kejahatan teknologi, tetapi juga peristiwa yang merefleksikan hubungan antara warga dan negara dalam ranah digital.[10]

Kasus kebocoran ini harus dianalisis tidak hanya dari perspektif teknis keamanan, melainkan juga dari ranah hukum, etika, dan politik teknologi. Aspek hukum terkait perlindungan data pribadi perlu dipertegas dan diperkuat agar pelaku kejahatan siber memiliki konsekuensi hukum yang jelas. Secara etis, institusi negara wajib menjalankan amanah perlindungan data warganya dengan serius, agar tidak menjadikan warga sebagai korban atas kelalaian pengelolaan data. Sementara secara politik, fenomena ini menjadi indikator kebutuhan reformasi kebijakan teknologi informasi dan komunikasi yang responsif terhadap tantangan era digital.[11]

Kasus kebocoran data POLRI yang dilakukan Bjorka menimbulkan dilema antara hak privasi individu dan kebutuhan keamanan nasional. Ketika data sensitif milik personel kepolisian bocor, potensi ancaman terhadap keamanan institusi dan negara menjadi nyata, sehingga penanganan kebocoran harus dilakukan tanpa mengorbankan prinsip-prinsip hak asasi manusia, termasuk hak atas privasi. Oleh karena itu, penanganan kasus ini harus melibatkan berbagai pihak, baik dari aspek teknis, hukum, sosial, hingga kebijakan. [12]

Kebocoran ini juga menjadi momentum penting untuk mendorong pengembangan kapasitas sumber daya manusia di bidang keamanan siber dalam institusi negara. Tidak cukup hanya mengandalkan perangkat teknologi, melainkan keahlian dan kesadaran sumber daya manusia juga harus dimaksimalkan agar risiko kebocoran dapat diminimalkan melalui pengawasan, pelatihan, dan pemantauan berkelanjutan. Hal ini sebagai bagian dari reformasi keamanan siber yang wajib diperhatikan dalam konteks modernisasi institusi negara.

Tanggung Jawab Hukum POLRI Sebagai Pengendali Data

Sebagai lembaga negara yang mengumpulkan, menyimpan, dan memproses data dalam jumlah besar, POLRI memiliki kewajiban hukum yang jelas sebagai Pengendali Data Pribadi.[13] Status ini secara tegas diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), di mana Pasal 1 angka 4 mendefinisikan Pengendali Data sebagai pihak yang menentukan tujuan dan kendali pemrosesan data pribadi. Dengan demikian, setiap tindakan POLRI terkait pengelolaan data personel maupun data masyarakat berada dalam kerangka tanggung jawab hukum UU PDP dan regulasi terkait lainnya. Dalam kerangka UU PDP, POLRI wajib menerapkan prinsip-prinsip perlindungan data pribadi sebagaimana tertuang dalam Pasal 3. Prinsip tersebut mencakup legalitas, kehati-hatian, transparansi, pembatasan tujuan, akurasi, keamanan, dan akuntabilitas. Setiap kebocoran

[9] Wuwungan, M. S. S. (2024). *Op.cit.* Hal. 9.
[10] Kompas.com, "Polisi Ungkap Bjorka Simpan 5 GB Data Termasuk Milik Pemerintah Asing," Kompas Megapolitan, 3 November 2025, diakses 24 November 2025, dari https://megapolitan.kompas.com/read/2025/11/03/13235001/polisi-ungkap-bjorka-simpan-5-gb-data-termasuk-milik-pemerintah-asing.
[11] Wuwungan, M. S. S. (2024). *Op.cit.* Hal. 10.
[12] Kompas.com, *Op.cit.* https://megapolitan.kompas.com/read/2025/10/07/07492751/polisi-usut-dugaan-kebocoran-data-341-ribu-personel-oleh-bjorka.
[13] Wira Prayatna. *Pemanfaatan Big Data Untuk Keamanan Publik: Paradigma Baru POLRI*. Yogyakarta: Deepublish Digital. (2025). hlm. 81.

Dec 2025, Vol. 4, No. 1
e-ISSN: 3032-6591
pp 202-208

data pada dasarnya mencerminkan kegagalan memenuhi prinsip keamanan (security principle) yang menuntut pengendali data menjaga kerahasiaan, integritas, dan ketersediaan data pribadi.[14] Apabila kebocoran data POLRI benar terjadi, hal ini menunjukkan adanya pelanggaran pada pemenuhan prinsip keamanan dan akuntabilitas, pengendali data bertanggung jawab atas seluruh pengelolaan data pribadi di bawah kendalinya.

Selanjutnya, UU PDP secara khusus mengatur kewajiban teknis dan organisasional pengendali data dalam Pasal 35 ayat (1), yaitu memastikan perlindungan data melalui pengamanan yang layak terhadap risiko kehilangan, penyalahgunaan, akses tidak sah, gangguan, dan penghancuran.[15] Pengamanan ini harus dilakukan melalui metode yang sesuai standar, seperti enkripsi, pengendalian akses, dan pemutakhiran sistem. Dalam kebocoran data POLRI, jika insiden tersebut terjadi akibat kelemahan infrastruktur keamanan atau kelalaian pemeliharaan sistem, maka terdapat indikasi pelanggaran terhadap kewajiban Pasal 35. Termasuk dalam kewajiban tersebut adalah memastikan seluruh sistem aktif maupun arsip (legacy systems) memiliki tingkat perlindungan yang memadai. UU PDP juga mengatur kewajiban notifikasi insiden dalam Pasal 46 ayat (2), di mana pengendali data wajib memberitahukan subjek data dan lembaga terkait sejak diketahuinya kegagalan perlindungan data. Notifikasi ini bukan sekadar formalitas, melainkan mekanisme transparansi untuk memastikan bahwa subjek data mengetahui risiko yang berpotensi timbul atas kebocoran tersebut. Hingga saat ini belum terdapat informasi publik yang jelas menunjukkan pelaksanaan kewajiban notifikasi oleh POLRI, sehingga aspek akuntabilitas institusional masih menjadi pertanyaan besar.[16]

Selain UU PDP, kewajiban hukum POLRI sebagai pengendali data juga bersandar pada regulasi keamanan siber lainnya, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Pasal 14 PP PSTE mewajibkan penyelenggara sistem elektronik menerapkan manajemen keamanan informasi yang berstandar internasional, termasuk identifikasi risiko, perlindungan, pendeteksian serangan, dan pemulihan pasca insiden. Apabila kebocoran data terjadi akibat lemahnya penerapan manajemen risiko, POLRI dapat dinilai tidak memenuhi ketentuan PP PSTE. Lebih lanjut, Permenkominfo No. 4 Tahun 2016 tentang Manajemen Keamanan Informasi juga menegaskan kewajiban instansi pemerintah untuk menerapkan Information Security Management System (ISMS).[17]

SIMPULAN

Kasus kebocoran data Polri oleh Bjorka pada tahun 202 menunjukkan bahwa ancaman keamanan siber di Indonesia telah berkembang ke tingkat yang sangat serius dan menyasar institusi strategis negara. Kebocoran data yang melibatkan lebih dari ratusan ribu identitas personel Polri bukan hanya menggambarkan lemahnya sistem keamanan digital, tetapi juga mengindikasikan bahwa tata kelola pengelolaan data negara belum sepenuhnya sejalan dengan standar perlindungan data pribadi. Peristiwa ini turut memperkuat kekhawatiran bahwa kehadiran regulasi seperti UU PDP belum menjamin implementasi perlindungan data secara efektif apabila tidak dibarengi dengan pengawasan, kesiapan infrastruktur, dan kompetensi teknis yang memadai.

[14] Andrew A. D., Alya N., Nabilatul A. P., Nabilah N. (2025). *PERTANGGUNGJAWABAN HUKUM PEMERINTAH DALAM KEBOCORAN DATA PRIBADI PADA PENYELENGGARAAN PUSAT DATA NASIONAL*. Jurnal Hukum Samudra Keadilan Vol. 20, No. 1, 109-124.
[15] Pricillia Alvionita Yusuf. (2024). *Tanggung Jawab Keamanan Data Digital Oleh Penyelenggara Sistem Elektronik*. Lex Privatum Vol. 13, No. 5.
[16] Marsya I. E. R., Sinta D. R., Amelia C. (2025). *Perbandingan Penerapan Prinsip Transparansi Antara Indonesia dengan Irlandia dalam Hal Terjadinya Kegagalan Pelindungan Data Pribadi*. Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara Vol. 3, No. 2), 51-71.
[17] Wenderlin Koswara. (2022). *Implementasi Aturan Perlindungan Data Pribadi Oleh Penyelenggara Sistem Elektronik Dikaitkan Dengan Teori Keadilan Dan Kepastian Hukum*. Jurnal Paradigma Hukum Pembangunan Vol. 7, No. 2, 86-103.

Dec 2025, Vol. 4, No. 1
e-ISSN: 3032-6591
pp 202-208

Polri sebagai Pengendali Data Pribadi memiliki tanggung jawab penuh atas pengelolaan dan keamanan data yang berada di bawah kendalinya. Kewajiban tersebut mencakup pemenuhan prinsip keamanan, penerapan sistem pengamanan informasi yang sesuai standar, serta pemberitahuan kepada subjek data jika terjadi insiden kebocoran. Fakta kebocoran data ini menegaskan adanya ketidaksesuaian antara kewajiban normatif yang diatur dalam UU PDP dengan pelaksanaan perlindungan data dalam praktik. Dengan kata lain, Polri belum sepenuhnya menunjukkan akuntabilitas dan kepatuhan yang menjadi tuntutan hukum sebagai pengendali data.

REFERENSI

Wira Prayatna. Pemanfaatan Big Data Untuk Keamanan Publik: Paradigma Baru POLRI. Yogyakarta: Deepublish Digital. (2025). hlm. 81.

Andrew A. D., Alya N., Nabilatul A. P., Nabilah N. (2025). PERTANGGUNGJAWABAN HUKUM PEMERINTAH DALAM KEBOCORAN DATA PRIBADI PADA PENYELENGGARAAN PUSAT DATA NASIONAL. Jurnal Hukum Samudra Keadilan Vol. 20, No. 1, 109-124.

Ashilah, A. P., & Rahman, R. (2024). FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH BJORKA. *Jurnal Riset Sistem Informasi*, *1*(3), 17-26.

Marsya I. E. R., Sinta D. R., Amelia C. (2025). Perbandingan Penerapan Prinsip Transparansi Antara Indonesia dengan Irlandia dalam Hal Terjadinya Kegagalan Pelindungan Data Pribadi. Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara Vol. 3, No. 2), 51-71

Pricillia Alvionita Yusuf. (2024). Tanggung Jawab Keamanan Data Digital Oleh Penyelenggara Sistem Elektronik. Lex Privatum Vol. 13, No. 5.

Sabila, S. N., & Atman, W. (2025). Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik*, *2*(3), 142-154.

Wenderlin Koswara. (2022). Implementasi Aturan Perlindungan Data Pribadi Oleh Penyelenggara Sistem Elektronik Dikaitkan Dengan Teori Keadilan Dan Kepastian Hukum. Jurnal Paradigma Hukum Pembangunan Vol. 7, No. 2, 86-103.

Wuwungan, M. S. S. (2024). PERLINDUNGAN HUKUM TERHADAP PEMILIK DATA PRIBADI PENGGUNA TEKNOLOGI INFORMASI AKIBAT TINDAK PIDANA PERETASAN. LEX PRIVATUM, 13(4). Hal. 8-9.

Hacker Berusia 22 Tahun Ditangkap Setelah Retas Data Bank," Pusiknas Bareskrim Polri, diakses 24 November 2025, https://pusiknas.polri.go.id/detail_artikel/hacker_berusia_22_tahun_ditangkap_setelah_retas_data_bank

Tim Wartawan, "Hacker Bjorka Bocorkan Data 341 Ribu Personel Polri, Sistem Keamanan Negara Terancam," Suara Utama (7 Oktober 2025), diakses 24 November 2025, dari https://suarautama.id/hacker-bjorka-bocorkan-data-341-ribu-personel-polri-sistem-keamanan-negara-terancam/.

Tempo, "Hacker Bjorka Membobol Data Pribadi 341 Ribu Personel Polri," *Tempo.co*, 4 Oktober 2025, diakses 24 November 2025, dari https://www.tempo.co/hukum/hacker-bjorka-membobol-data-pribadi-341-ribu-personel-polri-2076447.

Tempo, "Polda Metro Jaya Dalami Dugaan Pembobolan Data Pribadi 341 Ribu Personel Polri," Tempo.co, 6 Oktober 2025, diakses 25 November 2025, dari Tempo. tempo.co/hukum/polda-metro-jaya-dalami-dugaan-pembobolan-data-pribadi-341-ribu-personel-polri-2076778.

Kompas.com, "Polisi Usut Dugaan Kebocoran Data 341 Ribu Personel oleh Bjorka," Kompas Megapolitan, 7 Oktober 2025, diakses 24 November 2025, dari https://megapolitan.kompas.com/read/2025/10/07/07492751/polisi-usut-dugaan-kebocoran-data-341-ribu-personel-oleh-bjorka.