Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial dan Politik
Volume. 2 Nomor. 3 Agustus 2025
e-ISSN: 3046-7950; p-ISSN: 3047-101X, Hal. 142-154
DOI: https://doi.org/10.62383/sosial.v2i3.1998
Available online at: https://journal.lpkd.or.id/index.php/Sosial

Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia

Syifa Nurul Sabila[1], Wira Atman[2],
[1,2] Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

Alamat: Jl. Perintis Kemerdekaan Km.10 Tamalanrea, Makassar, Sulawesi Selatan
Korespondensi penulis: syifaalbira30@gmail.com

Abstract. *This study aims to critically analyze the impact of the SIM card data leak by an anonymous actor named Bjorka on the level of public trust in digital security in Indonesia which first appeared in mid-2022, precisely in August 2022. In addition, it evaluates the extent to which the national legal system is able to provide protection for digital service users and examines the social, moral, and ethical responses of society in addressing the incident. This case demonstrates that data breaches are not merely technical issues but also shake the legitimacy of the state in safeguarding citizens' privacy rights, while revealing gaps in regulatory systems and data governance. This research employs a qualitative approach with a descriptive method. Data were collected through literature reviews of scholarly articles, academic journals, policy reports, and relevant opinion pieces. The findings indicate that Bjorka's data breach incident triggered a crisis of public trust in government institutions and digital service providers. The public responded with fear, anger, and disappointment, mainly due to the lack of transparency and accountability from the responsible parties. Moreover, the implementation of Law No. 27 of 2022 on Personal Data Protection is considered ineffective, both in terms of law enforcement and the readiness of technical and institutional infrastructure.*

Keywords: *Data breach, public trust, digital security, Personal Data Protection Law, Bjorka*

Abstrak. Penelitian ini bertujuan untuk menganalisis secara kritis dampak kebocoran data SIM card oleh aktor anonim bernama Bjorka terhadap tingkat kepercayaan publik terhadap keamanan digital di Indonesia yang muncul pertama kali pada pertengahan tahun 2022, tepatnya pada Agustus 2022. Selain itu, studi ini mengevaluasi sejauh mana sistem hukum nasional mampu memberikan perlindungan kepada pengguna layanan digital, serta menelaah respons sosial, moral, dan etika masyarakat dalam menyikapi peristiwa tersebut. Kasus ini menunjukkan bahwa kebocoran data bukan hanya persoalan teknis, tetapi juga mengguncang legitimasi negara dalam menjamin hak privasi warga, sekaligus membuka celah dalam sistem regulasi dan tata kelola data nasional. Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif. Data dikumpulkan melalui studi pustaka terhadap literatur ilmiah, akademik, laporan kebijakan, serta artikel opini yang relevan. Hasil penelitian menunjukkan bahwa insiden kebocoran data oleh Bjorka telah memicu krisis kepercayaan publik terhadap institusi pemerintah dan penyedia layanan digital. Masyarakat menunjukkan respons emosional berupa ketakutan, kemarahan, dan kekecewaan, terutama akibat minimnya transparansi dan akuntabilitas dari pihak-pihak terkait. Di sisi lain, pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dinilai belum efektif, baik dari segi penegakan hukum maupun kesiapan infrastruktur teknis dan kelembagaan.

Kata kunci: Kebocoran data, kepercayaan publik, keamanan digital, UU PDP, Bjorka

1. LATAR BELAKANG

Di era revolusi digital yang berkembang pesat, teknologi informasi dan komunikasi (TIK) adalah pilar utama yang mendukung beragam kegiatan manusia saat ini. Hampir seluruh sektor kehidupan baik sosial, ekonomi, pendidikan, layanan publik, hingga administrasi pemerintahan telah terdigitalisasi, menjadikan interaksi antarmanusia dan sistem berjalan lebih cepat, efisien, dan terhubung lintas batas geografis. Dunia maya, atau *cyberspace*, tidak lagi hanya menjadi sarana komunikasi, tetapi telah bertransformasi menjadi ruang sosial, ekonomi, bahkan politik

Received: Mei 30, 2025; Revised: Juni 10, 2025; Accepted: Juni 18, 2025;
Online Available: Juni 20, 2025;

baru, tempat berlangsungnya pertukaran informasi dan data secara masif, simultan, dan real-time.

Namun, di balik kemudahan dan efisiensi yang ditawarkan dunia 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 *Bjorka* pada Agustus tahun 2022. Salah satu kasus yang paling menyita perhatian adalah bocornya data pelanggan kartu SIM, mengungkap sekitar 1,3 miliar data pengguna Indonesia yang mencakup NIK, nomor telepon, nama operator, dan tanggal registrasi. Data ini diduga diambil secara ilegal dari sistem pemerintah, termasuk Kementerian Komunikasi dan Informatika, dan dijual di forum gelap sebesar USD 50.000. Ukuran file mencapai 87 GB (18 GB setelah dikompresi), dengan sampel valid sekitar 1,5 juta baris. Insiden ini menimbulkan risiko besar terhadap keamanan privasi dan memicu lonjakan penipuan digital serta penyalahgunaan data oleh pihak tidak bertanggung jawab., serta penyedia layanan telekomunikasi swasta (Sukmawan & Setyawan, 2023; Anjani, 2023).

Kebocoran data ini tidak hanya menjadi insiden teknis yang mengganggu sistem informasi nasional, tetapi juga berdampak serius terhadap persepsi publik. Masyarakat mulai mempertanyakan keseriusan dan kompetensi lembaga pemerintah dalam menjamin keamanan data pribadi warga negara. Ketidakpercayaan ini diperkuat oleh analisis sentimen publik di media sosial yang menunjukkan bahwa sebagian besar masyarakat khususnya pengguna aktif internet menyatakan rasa takut, marah, dan kecewa terhadap minimnya perlindungan dan transparansi pemerintah dalam menangani insiden ini (Wijaya et al., 2024). Fenomena ini menandakan bahwa krisis kepercayaan publik bukanlah isu remeh, tetapi menjadi indikator penting bahwa infrastruktur keamanan digital Indonesia berada dalam kondisi yang mengkhawatirkan. Hal ini menyebabkan Bjorka memilih Indonesia sebagai target serangan karena berbagai alasan strategis, mulai dari kelemahan sistem, kelonggaran regulasi, hingga nilai simbolis dari dampaknya. Secara teknis, infrastruktur keamanan siber Indonesia masih relatif rapuh, dengan banyaknya lembaga yang menggunakan sistem yang sudah ketinggalan zaman dan kurang diaudit, sebagaimana tercermin dari skor NCSI-nya yang rendah. Di sisi regulasi, meskipun UU PDP telah disahkan sejak 2022, implementasinya masih belum optimal sehingga masih terdapat celah pelanggaran yang lebar. Selain itu, serangan ini juga diduga bermuatan simbolis, karena menyasar lembaga pemerintah dan data publik sebagai bentuk

kritik terhadap lemahnya perlindungan negara terhadap warga negaranya. Dengan besarnya jumlah pengguna internet dan tingginya paparan media sosial di Indonesia, dampak sosial dan politik dari serangan ini juga semakin luas dan signifikan.

Peristiwa ini juga membuka ruang diskusi yang lebih dalam mengenai perlindungan hukum terhadap data pribadi. Dalam konteks hukum positif di Indonesia, kebocoran data masih berada dalam wilayah yang "abu-abu". Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sudah berlaku, pelaksanaannya belum sepenuhnya optimal. Banyak penyedia layanan, termasuk operator seluler, belum sepenuhnya menerapkan prinsip transparansi, akuntabilitas, dan perlindungan hak konsumen. Dalam kasus Bjorka, hingga kini belum ada pihak yang secara tegas bertanggung jawab atas kebocoran tersebut, dan masyarakat pun tidak diberikan kompensasi atau klarifikasi resmi yang memadai (Anjani, 2023). Hal ini memperlihatkan adanya celah besar dalam sistem regulasi, pengawasan, dan penegakan hukum di bidang perlindungan data digital.

Sementara beberapa penelitian sebelumnya telah membahas aspek hukum dan kebijakan seputar pelindungan data pribadi, kajian yang secara spesifik menyoroti dampak kebocoran data kartu SIM terhadap kepercayaan publik dalam konteks sosial-psikologis dan hukum masih sangat jarang dilakukan. Sebagian besar studi masih terfokus pada aspek teknis atau hukum normatif, tanpa menggali secara mendalam bagaimana kasus-kasus seperti Bjorka membentuk persepsi publik terhadap sistem digital dan otoritas negara. Inilah yang menjadi gap (celah) dalam literatur yang hendak dijembatani oleh penelitian ini.

Penting juga untuk digarisbawahi bahwa kerugian akibat kebocoran data tidak sebatas dalam bentuk kerugian materiil, tetapi juga dalam bentuk kerusakan sosial yang bersifat sistemik yaitu menurunnya rasa percaya masyarakat terhadap institusi negara. Di tengah upaya pemerintah untuk mendorong digitalisasi melalui e-Government, layanan kesehatan digital, dan platform administrasi publik berbasis daring, kepercayaan masyarakat adalah modal utama. Jika kepercayaan ini luntur, maka agenda transformasi digital pun dapat mengalami stagnasi atau bahkan resistensi. Oleh karena itu, penelitian yang mampu menguraikan secara komprehensif hubungan antara insiden kebocoran data dan krisis kepercayaan publik sangatlah mendesak.

Menurut Ashari (2023), dalam ekosistem digital, kepercayaan merupakan elemen krusial yang menentukan keberlangsungan layanan digital itu sendiri. Ketika data pelanggan disalahgunakan atau bocor, kepercayaan tidak hanya hilang terhadap perusahaan penyedia layanan, tetapi juga terhadap institusi pemerintah sebagai regulator. Maka dari itu, urgensi

penelitian ini menjadi semakin tinggi, karena kepercayaan digital bersifat fundamental dalam keberhasilan agenda digitalisasi nasional.

Maka dari itu, penelitian ini hadir untuk mengkaji secara kritis konsekuensi dari fenomena kebocoran data kartu SIM oleh Bjorka terhadap tingkat kepercayaan publik terhadap keamanan digital di Indonesia. Selain itu, penelitian ini juga akan mengevaluasi sejauh mana sistem hukum nasional mampu memberikan perlindungan kepada pengguna layanan digital, serta menelaah bagaimana respons sosial, moral, dan etika masyarakat dalam menyikapi peristiwa tersebut. Temuan dari studi ini diharapkan dapat memberikan kontribusi nyata dalam penyusunan kebijakan yang lebih kuat, responsif, dan inklusif dalam menghadapi tantangan keamanan digital di masa mendatang.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif untuk memahami dan menginterpretasikan fenomena kebocoran data SIM card oleh aktor anonim bernama Bjorka serta dampaknya terhadap tingkat kepercayaan publik terhadap keamanan siber di Indonesia. Pendekatan deskriptif dipilih untuk menggambarkan secara sistematis bagaimana insiden tersebut mempengaruhi persepsi masyarakat, serta untuk mengevaluasi respons institusi terkait dari sisi sosial, hukum, dan kebijakan. Penelitian ini tidak berfokus pada pengukuran kuantitatif, melainkan pada penelusuran makna, narasi publik, dan argumentasi normatif dari berbagai sumber yang terkait.

Teknik pengumpulan data yang digunakan dalam penelitian ini yaitu melalui studi pustaka dengan mengkaji literatur ilmiah, jurnal akademik, laporan riset, dokumen kebijakan, serta artikel opini yang relevan dengan topik penelitian. Sumber-sumber tersebut dianalisis secara kualitatif untuk mengidentifikasi pola-pola argumen, posisi kritis, serta dinamika wacana publik terkait isu kebocoran data dan kepercayaan masyarakat terhadap sistem keamanan digital.

3. HASIL DAN PEMBAHASAN

Karakteristik dan Skema Peretasan dalam Kasus Bjorka

Kasus kebocoran data yang dilakukan oleh sosok anonim dengan nama samaran *Bjorka* menjadi salah satu peristiwa paling menggemparkan dalam sejarah keamanan siber di Indonesia. Peristiwa ini menyerang langsung kredibilitas lembaga negara, khususnya instansi pemerintah yang memiliki tanggung jawab besar dalam bidang teknologi dan komunikasi, seperti Kementerian Komunikasi dan Informatika (Kominfo), tepatnya pada Agustus tahun

2022. Dampaknya tidak hanya dirasakan oleh masyarakat sebagai pemilik data, tetapi juga oleh para pelaku industri teknologi yang sangat bergantung pada kepercayaan digital dan integritas sistem informasi. Dunia maya, yang semula menjadi fondasi utama bagi perkembangan industri digital, justru dipertanyakan keamanannya, terutama ketika aktor eksternal mampu menembus sistem informasi sensitif negara.

Karakteristik peretasan yang dilakukan oleh Bjorka tergolong kompleks dan terstruktur. Ia tidak hanya melakukan peretasan untuk mencuri data, tetapi juga menggunakan strategi komunikasi digital untuk menyampaikan pesan politik kepada publik dan pemerintah. Menurut Suciati dan Suciyani (2023), metode yang digunakan Bjorka mencakup pengumpulan data melalui celah keamanan pada sistem internal, pemanfaatan data lama dari kebocoran sebelumnya, dan penyebaran informasi secara strategis melalui forum *Breach* dan kanal Telegram. Target utama dalam aksinya meliputi data registrasi SIM card, informasi warga negara yang tersimpan di sistem Kominfo, dan data internal dari beberapa lembaga negara lainnya. Skema peretasan Bjorka bahkan menunjukkan pola yang sistematis dimulai dari kompromi sistem, eksfiltrasi data, hingga publikasi dan ancaman lanjutan yang menunjukkan bahwa serangan ini bukan sekadar kriminal digital biasa, melainkan sarat muatan simbolik dan kritik terhadap negara. Riset juga mengungkapkan bahwa per tahun 2024, 79.50% atau sekitar 221.563.479 juta jiwa dari total 278.696.200 juta penduduk Indonesia telah menjadi pengguna internet. Hamper setiap pengguna internet ini terhubung ke setidaknya satu *platform* media yang mengumpulkan data pribadi mereka.

Dampak dari serangan ini begitu luas dan menciptakan efek domino terhadap kepercayaan masyarakat dan dunia usaha. Keamanan siber yang semestinya menjadi elemen fundamental dalam bisnis digital kini justru menjadi titik rawan. Tanpa sistem perlindungan yang kuat, perusahaan teknologi kehilangan fondasi penting untuk membangun hubungan kepercayaan dengan pelanggan. Oleh karena itu, negara memiliki kewajiban untuk memberikan perlindungan yang tidak hanya bersifat teknis, tetapi juga regulatif dan kelembagaan. Pemerintah perlu merancang instrumen hukum yang spesifik dan adaptif terhadap dinamika serangan digital, serta membangun institusi yang mampu merespons ancaman siber secara cepat dan tegas.

Dalam perspektif normatif, hak atas perlindungan data sebagai bagian dari perlindungan hukum tidak hanya termuat dalam hukum positif, tetapi juga diakui dalam ajaran Islam melalui prinsip maqāṣid al-syarīʿah. Sebagaimana dijelaskan oleh Amir Syarifuddin yang merujuk pada pemikiran Imam Asy-Syatibi, maqashid syariah menekankan pentingnya menjaga lima hal pokok dalam kehidupan manusia termasuk harta dan kehormatan yang dalam konteks

digital dapat diterjemahkan sebagai data pribadi dan integritas informasi. Meskipun tidak secara eksplisit membahas tindakan *hacking*, prinsip-prinsip maqashid dapat dijadikan dasar untuk mengevaluasi kejahatan digital sebagai bentuk pelanggaran terhadap maslahat umat yang memerlukan ijtihad baru dari para ahli hukum Islam.

Dengan demikian, kasus Bjorka menunjukkan bahwa peretasan di era digital bukan lagi sekadar pelanggaran teknis, melainkan fenomena sosial, politik, dan etika yang menuntut respons hukum dan kebijakan yang multidimensional. Baik dari sisi perlindungan negara, dunia usaha, maupun norma sosial keagamaan, kejahatan siber semacam ini menuntut mekanisme mitigasi yang jauh lebih adaptif dan responsif dibanding pendekatan tradisional terhadap kejahatan konvensional.

Dampak Sosial terhadap Kepercayaan Publik

Pencurian data pribadi kini menjadi isu krusial dalam wacana keamanan siber global. Menurut Reynolds (2023), pencurian identitas salah satu bentuk pencurian data pribadi berdampak pada hampir 1 dari 10 orang dewasa setiap tahunnya, menunjukkan betapa serius dan meluasnya permasalahan ini. Berdasarkan Laporan *National Cyber Security Index* (NCSI) tahun 2022, Indonesia mencatatkan skor keamanan digital sejumlah 38,96 dari total 100 poin. Dengan capaian tersebut, Indonesia menempati posisi ketiga terbawah di antara negara-negara anggota G20 dalam hal kesiapan keamanan siber.

Lebih dari sekadar mendapatkan informasi individu, pencurian data telah menjadi sarana eksploitasi dan penghasilan dalam ekonomi digital ilegal. Para pelaku kejahatan semacam ini umumnya memiliki kompetensi teknis yang tinggi, memungkinkan mereka untuk menyamarkan aktivitasnya dan menghindari sistem deteksi keamanan. Bahkan, mereka mampu menganalisis risiko secara cermat dan memanfaatkan berbagai celah dalam infrastruktur keamanan yang ada (Reynolds, 2023). Hal ini memperlihatkan kompleksitas serta kecanggihan metode yang digunakan dalam kejahatan siber, yang kini tidak hanya menyasar perorangan, melainkan juga institusi besar seperti lembaga pemerintah dan perusahaan swasta

Di Indonesia, kebocoran data yang terjadi pada aplikasi MyPertamina pada tahun 2023 menjadi ilustrasi nyata dari ancaman tersebut. Dalam insiden tersebut, sekitar 21 juta data pengguna terekspos, memperlihatkan lemahnya sistem perlindungan data yang ada. Dampaknya sangat besar, tidak hanya pada sisi kepercayaan publik terhadap penyelenggara layanan digital, tetapi juga pada aspek ekonomi yang terdampak akibat kebocoran tersebut. Peristiwa ini sekaligus menandai bagaimana celah dalam pengelolaan data bisa dimanfaatkan oleh pelaku siber untuk melancarkan aksinya, dan menegaskan perlunya pembenahan sistem perlindungan data secara menyeluruh di Indonesia.

Penelitian ini akan difokuskan pada tiga persoalan utama yang berkaitan dengan insiden kebocoran data MyPertamina pada Mei 2023. Pertama, kajian ini bertujuan untuk mengungkap karakteristik serta pola kejahatan siber dalam kasus tersebut, sekaligus menganalisis bagaimana hal itu mencerminkan perkembangan ancaman digital di Indonesia. Kedua, penelitian akan menilai sejauh mana efektivitas regulasi dan kebijakan nasional dalam merespons dinamika ancaman keamanan siber yang terus berubah. Ketiga, studi ini akan mengkaji dampak jangka panjang kebocoran data terhadap tingkat kepercayaan masyarakat serta stabilitas sektor ekonomi digital nasional.

Evaluasi Perlindungan Data Pribadi dalam Perspektif Hukum Indonesia

Salah satu langkah atau evaluasi untuk mengantisipasi dan mencegah ancaman di dunia siber adalah dengan memperkuat regulasi mengenai pencurian data pribadi. Pemerintah Indonesia juga dapat mendorong kerja sama yang lebih erat di bidang keamanan siber, baik melalui hubungan bilateral maupun multilateral dengan negara lain. Selain itu, sinergi antara pemerintah dan sektor swasta perlu ditingkatkan untuk memperkuat pertumbuhan sektor ekonomi dan teknologi keamanan digital. Di tingkat individu, pencegahan bisa dilakukan dengan meningkatkan kewaspadaan terhadap informasi yang beredar di media sosial, khususnya dari sumber yang tidak jelas atau orang asing. Tidak sembarangan membuka tautan atau mempercayai informasi dari sumber tak dikenal menjadi bentuk kehati-hatian yang penting.

Hingga saat ini, insiden kebocoran data pribadi yang marak terjadi di Indonesia belum ditangani secara serius. Mayoritas kasus hanya berakhir pada teguran atau sanksi administratif, tanpa penyelesaian hukum yang kuat. Hal ini dikarenakan Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) belum diberlakukan secara menyeluruh. Berdasarkan Pasal 74, implementasi sanksi berupa denda terhadap pihak yang lalai baru akan berjalan efektif dua tahun setelah undang-undang tersebut resmi diundangkan. Masa transisi ini dimaksudkan agar para pengelola data pribadi memiliki waktu untuk menyesuaikan diri dengan ketentuan yang ada.

Dalam kondisi seperti ini, pemerintah memanfaatkan berbagai insiden kebocoran data sebagai alat untuk mempercepat pembentukan regulasi perlindungan data. Proses pembahasan undang-undang di parlemen pun berlangsung relatif cepat. Sementara itu, masyarakat sebagai pihak yang terdampak menunjukkan reaksi yang beragam ada yang mendukung langkah pemerintah, ada pula yang mengkritisi, bahkan sebagian bersimpati pada para pelaku peretasan. Ragam respons ini mencerminkan adanya tekanan publik agar negara segera memperkuat perlindungan atas data digital warganya.

Dinamika antara para pemangku kepentingan dalam isu ini kemudian membentuk suatu pemahaman moral kolektif, yang menekankan urgensi regulasi perlindungan data pribadi sebuah kebijakan yang telah lama dinantikan. Dalam konteks ini, narasi kebijakan memegang peran penting dalam membentuk opini publik agar sejalan dengan arah kebijakan yang ditetapkan oleh para pengambil keputusan.

Oleh karena itu, keberadaan UU Perlindungan Data Pribadi dipandang sebagai jawaban terhadap kekhawatiran masyarakat atas meningkatnya kebocoran data dan menurunnya kepercayaan publik terhadap kemampuan negara dalam melindungi keamanan digital. Penelitian ini memberikan sumbangsih dalam kajian kebijakan publik, terutama dengan menggunakan pendekatan Narrative Policy Framework (NPF) yang memungkinkan analisis kebijakan dilakukan secara lebih komprehensif tidak hanya berfokus pada hasil atau pelaksanaan kebijakan, tetapi juga pada narasi dan konteks sosial yang melatarbelakanginya.

Kesenjangan dan Tantangan dalam Sistem Keamanan Siber Nasional

Tantangan besar dalam keamanan siber di Indonesia adalah keterbatasan infrastruktur teknologi dan kurangnya tenaga ahli keamanan siber. Oleh karena itu, investasi besar dalam pengembangan teknologi keamanan siber, serta pelatihan dan peningkatan kapasitas tenaga kerja di bidang ini, sangat diperlukan. Penerapan *NIST Cybersecurity Framework (CSF)* di Indonesia menghadapi sejumlah tantangan besar, terutama yang berkaitan dengan kondisi infrastruktur teknologi yang belum memadai, hal ini disebut tidak memadai karena keterbatasan penguasaan terhadap teknologi keamanan siber, serta kurangnya sumber daya manusia yang memiliki keahlian di bidang tersebut. Banyak organisasi, khususnya yang berada di sektor pemerintahan dan usaha kecil menengah (UMKM), masih belum memiliki sistem teknologi informasi yang cukup andal. Misalnya, belum tersedia jaringan yang aman, sistem pemantauan ancaman, maupun pemanfaatan layanan cloud yang sesuai dengan standar keamanan internasional. Padahal, untuk bisa menerapkan NIST secara menyeluruh, diperlukan infrastruktur yang memenuhi standar seperti ISO/IEC 27001, NIST SP 800-53, hingga IEC 62443. Sayangnya, tidak sedikit organisasi yang masih mengandalkan sistem lama dan hanya mengandalkan perangkat lunak keamanan dasar seperti antivirus dan firewall, yang belum cukup untuk menangani ancaman siber modern.

Di samping itu, adopsi teknologi keamanan yang lebih canggih seperti SIEM, EDR, arsitektur Zero Trust, dan sistem intelijen ancaman juga masih sangat terbatas. Kondisi ini membuat banyak organisasi kesulitan dalam membangun sistem keamanan yang tangguh dan dapat beradaptasi dengan dinamika serangan siber. Tantangan lain yang tak kalah penting adalah minimnya jumlah tenaga profesional di bidang keamanan siber. Meskipun permintaan

akan ahli yang bersertifikasi dan memiliki kemampuan teknis semakin meningkat, pasokan dari lembaga pendidikan maupun pelatihan belum mencukupi. Masalah ini diperburuk oleh rendahnya kesadaran dari banyak organisasi terhadap pentingnya keamanan digital. Hal ini tampak dari alokasi anggaran yang masih minim, ketiadaan kebijakan keamanan internal yang jelas, hingga tidak adanya posisi strategis seperti Chief Information Security Officer (CISO) dalam struktur organisasi.

Hambatan lainnya adalah soal pendanaan. Untuk bisa mengadopsi framework NIST secara serius, dibutuhkan investasi yang tidak sedikit baik dalam bentuk pembangunan infrastruktur, pengembangan SDM, maupun kegiatan audit keamanan secara rutin. Sayangnya, masih banyak organisasi yang memandang keamanan siber sebagai beban biaya, bukan sebagai bentuk investasi untuk perlindungan jangka panjang. Oleh karena itu, diperlukan upaya yang lebih terstruktur dari pemerintah dan pemangku kepentingan lain, seperti pelaksanaan audit berdasarkan standar global, peningkatan anggaran keamanan TI, serta pemberian insentif bagi organisasi yang mau berkomitmen membangun sistem keamanan yang kokoh. Strategi ini menjadi krusial agar Indonesia lebih siap dalam menghadapi ancaman siber yang terus berkembang dan semakin kompleks. Pemerintah, dengan dukungan sektor swasta, harus berinvestasi dalam pendidikan dan pelatihan keamanan siber, sehingga dapat menutup kesenjangan keahlian yang ada.

Menggunakan hukum positif tradisional untuk memerangi kejahatan cyber sangatlah besar. Hal ini disebabkan oleh fakta bahwa kejahatan ini melibatkan beberapa faktor yang saling berhubungan, yaitu korban, pelaku, hukum, dan respons sosial, terhadap kejahatan tersebut. Meskipun hukum berperan vital untuk mencegah dan memberantas kejahatan, menyusun peraturan atau undang-undang yang dapat mengikuti perkembangan pesat teknologi informasi saat ini seringkali sulit. Akibatnya, aturan hukum kerap kali tertinggal zaman ketika mengatur ranah yang terus berkembang pesat seperti teknologi informasi, alhasil memicu kekososongan regulasi. Fenomena ini nampaknya terjadi pula dalam penanganan tindak kejahatan di dunia maya atau *cybercrime*.

Masalah pokok dalam upaya melindungi data pribadi di Indonesia terletak pada masih lemahnya aturan hukum yang berlaku serta minimnya penegakan hukum yang tegas dalam menghadapi kasus kebocoran data di tengah perkembangan era big data saat ini. Tantangan utama dalam penerapan NIST di Indonesia adalah kurangnya infrastruktur teknologi yang memadai dan kesadaran yang masih rendah di banyak organisasi. Salah satu kendala lainnya dalam penerapan NIST Cybersecurity Framework di Indonesia adalah belum optimalnya dukungan infrastruktur teknologi. Banyak fasilitas data center yang masih tersebar dan belum

memenuhi standar keamanan internasional secara menyeluruh. Selain itu, pemanfaatan sistem deteksi dan pencegahan ancaman secara otomatis masih terbatas, terutama di sektor pemerintahan dan usaha kecil menengah. Keterbatasan akses internet, terutama di luar wilayah perkotaan, turut menghambat penerapan teknologi keamanan digital berbasis cloud. Selain itu, pemanfaatan teknologi enkripsi dan sistem autentikasi berlapis seperti MFA dan PKI belum banyak diterapkan. Namun, telah ada perkembangan positif seperti pembentukan Pusat Operasi Keamanan Siber Nasional oleh BSSN, pengesahan Undang-Undang Perlindungan Data Pribadi, dan inisiatif pembangunan data center nasional berbasis cloud. Tumbuhnya ekosistem startup di bidang keamanan digital dan pelatihan Incident Response Team (CSIRT) di berbagai lembaga menjadi indikasi langkah konkret peningkatan ketahanan siber nasional. Kasus kebocoran data di e-HAC Kemenkes dan POLRI menunjukkan bahwa masih banyak lembaga yang belum memiliki sistem deteksi dan respon yang efektif terhadap ancaman siber. Selain itu, kekurangan tenaga ahli keamanan siber di Indonesia juga merupakan hambatan yang signifikan, meningkatnya mengingat frekuensi kompleksitas serangan siber.

Urgensi Penguatan Kebijakan dan Edukasi Digital Berbasis Kepercayaan Publik

Upaya untuk mewujudkan sistem perlindungan data pribadi yang efektif di Indonesia memerlukan strategi yang tidak dapat berjalan secara sepihak. Diperlukan pendekatan kolaboratif yang bersifat inklusif, melibatkan berbagai pemangku kepentingan secara aktif dan berkelanjutan. Pemerintah, sebagai aktor utama dalam pembentukan regulasi dan penegakan hukum, dituntut untuk menciptakan mekanisme partisipatif yang lebih terbuka, di mana masyarakat sipil, pakar teknologi, dan pengguna layanan digital memiliki ruang untuk menyampaikan pandangan, kebutuhan, dan kekhawatiran mereka. Hal ini penting agar kebijakan yang lahir tidak hanya bersifat top-down, tetapi juga mencerminkan aspirasi dan kepentingan public

Di sisi lain, sektor industri, baik swasta maupun BUMN, memegang peran penting dalam memastikan bahwa pengelolaan data dilakukan secara bertanggung jawab. Perlindungan data pribadi seharusnya tidak lagi dilihat sekadar sebagai kewajiban hukum yang harus dipenuhi, melainkan sebagai bagian dari komitmen etis terhadap konsumen. Perusahaan perlu mengintegrasikan prinsip-prinsip privasi dan keamanan sejak tahap perancangan layanan (*privacy by design*) dan menjadikan transparansi sebagai bagian dari standar operasional mereka.

Sementara itu, keberadaan Lembaga Swadaya Masyarakat (LSM) dan kelompok advokasi digital menjadi elemen penting dalam menjaga akuntabilitas. LSM harus terus diberdayakan melalui perlindungan hukum, akses terhadap informasi, dan dukungan sumber daya agar dapat

menjalankan fungsi kontrol sosial secara independen dan kritis. Mereka berperan sebagai jembatan antara masyarakat dengan pemerintah dan industri, sekaligus sebagai penjaga agar kepentingan publik tetap menjadi pusat perhatian dalam diskursus kebijakan data.

Salah satu langkah hukum yang ditempuh pemerintah Indonesia untuk melindungi data pribadi dan membangun kepercayaan publik lagi adalah dengan menetapkan regulasi yang menegaskan kewajiban menjaga setiap tahap siklus data, mulai dari pengumpulan hingga pemusnahan, sesuai dengan prinsip perlindungan yang berlaku. Sebagai perbandingan, Uni Eropa melalui GDPR (2016) menetapkan tujuh prinsip dasar, antara lain pemrosesan data harus dilakukan secara sah, adil, dan transparan; sesuai dengan tujuan awal pengumpulan; terbatas pada data yang relevan; akurat dan diperbarui; disimpan dalam jangka waktu yang wajar; dijaga kerahasiaannya; serta diawasi melalui mekanisme pertanggungjawaban yang jelas.

Jika prinsip-prinsip tersebut dijadikan acuan, maka pemrosesan data pribadi baru dapat dilakukan jika terdapat dasar hukum yang sah, seperti adanya persetujuan dari pemilik data, kepentingan kontraktual, kewajiban hukum, perlindungan kepentingan vital, tugas yang dijalankan untuk kepentingan publik, atau kepentingan sah pihak pengendali data maupun pihak ketiga. Pendekatan ini bertujuan menciptakan sistem pengelolaan data yang aman dan transparan, sekaligus menjaga hak-hak individu atas informasi pribadinya.

Hanya dengan sinergi dan komitmen dari ketiga pilar utama tersebut negara, sektor swasta, dan masyarakat sipil Indonesia dapat membangun sistem perlindungan data pribadi yang tidak hanya responsif terhadap tantangan teknologi, tetapi juga berpihak pada keadilan sosial. Sebuah sistem yang berorientasi jangka panjang, mampu menjamin keberlanjutan, dan benar-benar melindungi hak-hak digital masyarakat di era informasi ini.

Pemerintah telah mengambil langkah nyata untuk memerangi dan mencegah penyalahgunaan data pribadi masyarakat dengan meluncurkan sebuah sistem yang dikenal sebagai Indonesian Data Protection System (IDPS). Sistem ini dirancang khusus guna menekan angka kejahatan di ranah digital, terutama yang terkait dengan penyalahgunaan informasi dan data individu. IDPS berfungsi krusial dalam mengamankan data pribadi yang tersimpan di pusat-pusat data atau lokasi pengumpulan informasi.

Tidak sebatas itu sistem ini juga memastikan agar proses pengelolaan data dan informasi pribadi dilakukan secara tepat, melalui koordinasi internal yang telah ditetapkan. Secara administratif, IDPS berada di bawah pengawasan Kementerian Komunikasi dan Informatika (Kominfo). Dalam pelaksanaannya, IDPS terdiri dari dua komponen utama, yakni otoritas atau pusat data dan petugas data. Tugas otoritas data yaitu mengumpulkan sekaligus melindungi

informasi pribadi yang telah dikirimkan oleh petugas data, sehingga koordinasi terkait data yang dimiliki oleh individu dapat dilakukan secara lebih efektif dan terpusat.

4. KESIMPULAN DAN SARAN

Kasus kebocoran data oleh Bjorka mengungkap kerentanan serius dalam sistem keamanan siber Indonesia, yang berdampak langsung pada menurunnya kepercayaan masyarakat terhadap negara. Insiden ini tidak sekadar menunjukkan lemahnya perlindungan data secara teknis, tetapi juga menyoroti kurangnya kesiapan institusi, lemahnya regulasi, serta minimnya tanggung jawab dalam penanganan kasus. Peretasan yang menyasar data publik dan institusi negara menyampaikan pesan simbolik tentang rapuhnya legitimasi negara dalam menjaga hak digital warganya. Situasi ini diperparah dengan belum optimalnya implementasi UU PDP, serta kurangnya tenaga ahli dan infrastruktur pendukung.

Untuk itu, diperlukan langkah bersama dari semua pihak. Pemerintah perlu memperkuat pengawasan dan membuka ruang partisipatif dalam pembuatan kebijakan, sementara pelaku industri harus menempatkan keamanan data sebagai prioritas utama. Di sisi lain, masyarakat sipil harus diberdayakan agar dapat mengawal kebijakan dan memperjuangkan hak-hak digital warga. Prinsip perlindungan data yang adil, baik dari standar internasional seperti GDPR maupun nilai lokal seperti maqāṣid al-syarī‘ah, bisa menjadi dasar membangun sistem yang lebih adaptif dan berkeadilan. Membangun kembali kepercayaan publik tidak cukup melalui janji, tetapi melalui tindakan konkret dan sistem yang benar-benar melindungi kepentingan masyarakat.

DAFTAR REFERENSI

Anjani, A. N. (2025). Perlindungan Hukum Terhadap Kebocoran Data Pada Registrasi Ualang Kartu Prabayar di PT.Telkomsel.

Atara, I., Harapan, U. P., Pelita, U., Raffi, H., & Haksoro, A. B. (2025). ANALISIS KRIMINOLOGI TERHADAP PENCURIAN DATA PRIBADI DI ERA DIGITAL: STUDI KASUS KEBOCORAN DATA PENGGUNA APLIKASI MYPERTAMINA TAHUN 2023. Jurnal Ilmiah Penelitian Mahasiswa, 3(2), 129–140. https://doi.org/10.61722/jipm.v3i2.787

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia. GANESHA LAW REVIEW, 5. https://doi.org/10.31316/jk.v6i1.2657

Ghazawneh, A., & Henfridsson, O. (2015). A paradigmatic analysis of digital application marketplaces. Journal of Information Technology, 30(3), 198–208. https://doi.org/10.1057/jit.2015.16

Hukom, S., Humi, N., & Lukman, I. (2025). The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era. Hakim: Jurnal Ilmu Hukum Dan Sosial, 3(1), 974–992. https://doi.org/10.51903/hakim.v3i1.2291

Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data Zaki Rizaldi, A. M., Dwi Putra, R., Ul Hosnah, A., & Zaki Rizaldi, M. (n.d.). Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data. http://jurnal.um-tapsel.ac.id/index.php/justitia

Lubis, A. J., Cempaka, F. G., & Suhirwan. (2025). Perang Cyber Sebagai Bentuk Peperagan Asimetris: Perspektif Filsafat Kamanan Digital dan Nist Cybersecurity Framework.

Nurhana, A., & Indawati, Y. (2023). Perlindungan Hukum atas Data Pribadi Pengguna SIM Card Telepon Seluler. Amnesti: Jurnal Hukum, 5(1), 66–82. https://doi.org/10.37729/amnesti.v5i1.2706

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. http://ejournal.upi.edu/index.php/TELNECT/

Pelaksanaan Perlindungan Data Pribadi, K., Sitorus, R., Zaman Felix Saragih, J., & Banke, R. (2025). Kendala Pelaksanaan Perlindungan Data Pribadi. https://doi.org/10.56128/jkih.v5i1.438 PERLINDUNGAN HUKUM PERUSAHAAN TEKNOLOGI TERHADAP. (n.d.).

Prawira, Y., & Yola, L. (2023). Analisis Narrative Policy Framework (NPF) dalam Kebijakan Undang-undang Pelindungan Data Pribadi (UU PDP). Jurnal Transformative, 9(2), 204–226. https://doi.org/10.21776/ub.transformative.2023.009.02.5

Sukmawan, D. I., & Setyawan, D. P. (n.d.). Hacker, Fear, and Harm: Data Breaches and National Security.

Yudistira, M., & Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo. 5(4). https://doi.org/10.31933/unesrev.v5i4